(Cool title needed!) Building a Liquid Options Protocol

Zubin Koticha
Opyn
WORKING DRAFT

November 1, 2019 DRAFT

Abstract

In this paper, we propose a generalized noncustodial options protocol on Ethereum. This peer to contract design lets options buyers to obtain protection against both technical and financial risks that DeFi users face and also allows options sellers to earn premiums on idle cryptoassets through these vanilla put options. The two initial use cases of focus are deposit insurance (e.g. protecting users of money markets like Compound against hacks and liquidity crises), and options markets letting people to hedge risk against events like DAI breaking its peg. These products will enable people to earn premiums on their ETH collateral by providing insurance through options selling. This framework also allows for the primitive of fungible, freely tradable ERC20 option contracts. These primitives can serve functions such as allowing people to hedge risks, create leverage, buy insurance, and make bets on volatility. This framework makes it possible for option sellers to offer synthetic protection by specifying a different collateral type (such as ETH) than the asset the strike price is denominated in. Further, we propose

1 Introduction

1.1 Decentralized Finance

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 is accelerating. Users have been drawn to DeFi for a number of reasons. Some, including those without access to the US Dollar in fiat, have been lending out DAI or USDC on money market protocols like Compound or dYdX to simulate a USD savings account. Many other users have been attracted to the high USD-denominated yields offered by Compound, 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].

1.2 Motivation

Risk factors include smart contract platforms getting hacked, flash crashes in the value of collateral, and liquidity crises in DeFi. Current solutions like Nexus Mutual are oversubscribed and difficult to scale given that Nexus is a single underwriter, meaning that there are severe limits to the amount of insurance they can offer, and Nexus requires human involvement for claim assessment. In addition, Nexus Mutual only protects against smart contract hacks; its Compound insurance provides no recourse against liquidity crises on Compound, for example.

We propose an options marketplace to The advantages with an options marketplace for insurance include the following: it supports many underwriters (options sellers), it incentivizes

options buyers to exercise only when it is profitable to them (i.e. when their options are in the money), eliminating the need for human claim assessors, and it protects against both technical and financial risks. That is why buying put options is one of the most commonly used strategies for financial insurance in traditional finance.

1.3 Options

True derivatives markets are missing in Decentralized Finance. Such markets are extremely important in traditional finance for reasons including hedging, leverage, and financial insurance.

Options are amongst the most widely traded instruments in traditional finance, with a yearly exchange volume of more than $635 trillion (not including OTC options trading). Some of the key uses of these options are hedging and financial insurance.

The two initial use cases we'll focus on are deposit insurance (e.g. protecting users against Compound getting hacked or having liquidity crises), and options markets allowing people to hedge risk against events like DAI breaking its peg. Our framework allows for the primitive of fungible, exchange tradable ERC20 option contracts in DeFi.

1.3.1 How plain vanilla options work:

Let's begin with Alice, who will be the options seller for the rest of the paper, and Bob, the options buyer.

Scenario 1: Bob wants the right, but not obligation to sell 1 DAI for 1 USDC at 11:59 PM on December 31, 2019. Alice is willing to take on the obligation to purchase 1 DAI from Bob for 1 USDC at 11:59 PM on December 31, 2019. For Bob to gain this right to be able to obligate Alice, he pays her .10 USDC. Fast forward to 11:59 PM on December 31, 2019. Say Bob wants to sell his 1 DAI, then Alice must purchase it for 1 USDC. In the case that Bob does not want to sell his 1 DAI, Alice will just keep her 1 USDC.

Let's break scenario 1 down, to understand some basic options terminology.

- Bob is called the option *owner* (or buyer)
- Alice is called the option *writer* (or seller)
- DAI, the asset that Bob wants the right to sell, is called the *underlying asset*
- 1 USDC, the price at which Bob wants to sell DAI, is called the *strike price*
- .10 USDC, the price Bob pays Alice to purchase the option, is called the *premium*
- The process of Bob selling his 1 DAI to Alice for 1 USDC on 11:59 PM on December 31, 2019, is known as *exercise*
- USDC, the asset that Bob receives if he exercises, is called the *strike asset*
- Because Bob can only exercise his option exactly at the time of expiry, and not before or after that time, this type of option is an *European option*
- Because Bob has the right to *sell* DAI, this is called a *put option*
- 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.
- The specification of all the above parameters together create a unique option *series*.

Scenario 2: Let's take scenario 1 and adjust it slightly to create a new series. Bob wants the right, but not obligation to buy 1 DAI for 1 USDC by 11:59 PM on December 31, 2019. Alice is willing to take on the obligation to sell 1 DAI to Bob for 1 USDC by 11:59 PM on December 31, 2019. For Bob to gain this right to be able to obligate Alice, he pays her .10 USDC. Fast forward to at 11:00 AM on November 20, 2019. Say Bob wants to buy 1 DAI, then Alice must sell it for 1 USDC. In the case that Bob does not want to buy his 1 DAI, Alice will just keep her 1 USDC.

There are two key differences between scenario 1 and scenario 2, which will allow us to understand two more key options concepts.

- Because Bob can only exercise his option anytime before or on 11:59 PM on December 31, 2019, this type of option is an *American option*
- Because Bob has the right to buy DAI, this is called a *call option*

Now let's explore some common terminology around strike prices. Let's consider scenario 1, where Bob holds a put option with a strike price of 1 DAI.

- If the price of 1 DAI falls below 1 USDC, the put option is called *in-the-money*, since it is profitable for Bob to exercise his option
- If the price of 1 DAI is exactly 1 USDC, the put option is called *at-the-money*, where it does not make a difference to Bob whether or not he exercises his option
- If the price of 1 DAI is greater than 1 USDC, the put option is called *out-of-the-money*, since it is not profitable for Bob to exercise his option

1.4 Volatility

Most cryptocurrencies are so volatile that the resulting cryptocurrency options are very expensive and there may not be as much demand for options at a fair price. In addition, the 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 could 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.

1.5 Complexity

The problem with options in DeFi is that there are many variables to select when creating an options contract. Thus, when one mints new options, they run the risk creating a contract that does not have very high liquidity or fungibility.

Here are some of the important variables:

- Variable 1: Expiry time
- Variable 2: European vs American
- Variable 3: Underlying asset
- Variable 4: Strike Price
- Variable 5: Strike asset
- Variable 6: Collateral / margin requirement
- Variable 7: Collateral / margin type

- Variable 8: Call or Put

We call a specific option with the above parameters defined an option *series*. That is, the option we described in scenario 1, that gives Bob the right to sell 1 DAI for 1 USDC at 11:59 PM on December 31, 2019 a particular series. Options contracts within any particular series are fungible, but options are not fungible with options from a different series. Given so many possible expiries, underlying:strike asset pairs, and strike prices, etc. liquidity can't immediately form around any one 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, won't be too expensive, will have strike prices that are always near-the-money, or will have strike prices that are always desirable for buyers and sellers, and will not vary too much on the other above criteria.

From the above, you can see that options contracts are extremely useful tools in traditional finance, allowing users to do engage in hedging, insurance, and leverage. They are vital primitives for DeFi to have. However, as important as they are, it is difficult to deliver even plain vanilla option markets in DeFi given that the cryptoasset volatility and option contract complexity both negatively affect liquidity. This means that additional work is required for options to be viable in DeFi.

1.6 An Approach to Liquid Options

The above implies that, in order to create a liquidity options marketplace, one must address the dual goals of reducing volatility and decreasing options complexity.

One way we can try to fulfill our dual aims of reducing volatility and options complexity, while still fulfilling user demand for puts, 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 follow:

- 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.
- 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. What's important to note here is that stablecoins, such as DAI, should always trade 1:1 with the USD in theory. Similarly, cUSDC should only be slowly increasing in value relative to USD in theory.

In addition, since these put options solve pressing user pain points in DeFi (they can protect DAI holders from DAI breaking its peg or cUSDC holders from a hack on Compound), we can expect significant buyer demand.

So, how do we create something that resembles a put option on cTokens or DAI but has a high degree of fungibility in DeFi? Let's explore in the following sections.

1.7 Protective Puts

One way to hedge positions using derivatives is through protective put options. That is, in traditional finance, owners of an asset who want to be protected against some downside risk often hedge 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 get rid of this asset at a certain predetermined price. This allows them to cap the loss on said position. For example, if they bought a stock for $50 a share and wanted to cap their loss at $10, they could purchase a put option with a strike price of $40, which would 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 goes up: they get to keep all their gains but are exposed only to $10 of loss.

1.8 Prior Work

The most notable prior attempt for options in Decentralized Finance is dYdX. The original dYdX whitepaper considered ERC20 options markets [1]. However, 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 signficant barrier to liquidity [7] (it would not have been possible for sellers to write and sell their options Unsiwap, for example) İn addition, dYdX placed a number of restrictions on sellers that have been addressed in this paper. The protocol 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, and did not allow sellers to get out their positions before expiry. Further, it does 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 collateral types also prevented many strike assets de to their high interest rates.

Work from Maker, UMA, and Yield Protocol have made considerable strides in ETH-collateralized synthetics and as such are significant inspirations to the ideas put forth in this paper, especially in informing this paper's ideas of repo collateralization, token fungibility, and liquidation.

2 Mechanism

As in all options markets, the two key actors in the protocol are those who want to sell put options, and those who want to buy put options. In this example, as before, Alice sells puts and Bob buys puts.

Those who want to sell put options are analogous to those who mint DAI using CDPs in the Maker system, or those who mint yTokens in the Yield Protocol. In Maker, someone who mints and sells DAI is said to be short DAI. In Yield Protocol, someone who mints and sells yTokens is said to be short yTokens. Similarly, someone who mints and sells put options on our platform is said to be short put options. Note that in all the above protocols (Maker, Yield, Options), it makes no sense to mint the aforementioned tokens without the intent to immediately sell them. Further, those who buy and hold puts are like those who buy and hold DAI on exchanges.

Alice, the options seller, mints these put options and attempts to find a buyer. Meanwhile, Bob wants to protect himself against DAI breaking its peg. As a result, Bob buys the put options from Alice, and pays her a premium for purchasing the options. For Bob, he gains protection. Alice, on the other hand gets a premium in response for writing these options and selling them to Bob. This agreement between Alice and Bob, as outlined above, is known as an options contract, aptly named because it gives the buyer, Bob, the option, but not the obligation, to sell his asset to Alice.

Let's look at the option properties from the point of view of Bob, the option Buyer. He makes the most possible money for his option when his DAI becomes worthless; his option in that case would allow him to sell a worthless asset for a whole dollar, and thus he is essentially getting a dollar from Alice in exchange for sending her a token that is worth nothing. Note that the maximum payout of a put option is its strike price, thus maximum value of a put option is also its strike price. Since the strike price is the maximum amount that Alice will ever need to pay Bob if he exercises the option, that is the amount of collateral Alice must post in order to keep herself fully collateralized.

Now let's consider the point of view of Alice, the option seller. While Bob is given an option, Alice is given an obligation to buy the asset from Bob at his discretion. This has a few implications: first, Alice is required to post collateral but Bob is not. Alice knows that Bob will only exercise his put option when it is profitable for him to do so, and to exercise it, he will have to send DAI, so he will send DAI.

Of course, Bob will only exercise the option when it is profitable for him to do so. The reverse also holds true: Bob will only exercise when it is unprofitable for Alice. Since this contract is an obligation for her, the only way she will enter into the contract is if Bob pays her for the option! In fact, he must pay her an amount which makes her feel comfortable with this risk. The amount that Bob pays to buy the options contract from Alice is called the price of the option, or the option premium.

2.1 Participant Motivation

Let's take a look at an example. As before, Alice sells puts and Bob buys puts.

2.1.1 Buyer motivation:

Imagine that Bob, the option buyer, holds a substantial amount of DAI. However, Bob is scared of DAI losing its peg, which could cause him to lose money. Therefore, Bob wants to be protected against DAI's peg breaking, so that if DAI crashes below, say, $0.99, he doesn't lose any of his money. Bob would clearly be willing to pay some money to Alice if Alice could protect him against DAI going down in price below $0.99. In this case, as in traditional finance, Bob could hedge out his DAI risk by buying put options from Alice.

2.1.2 Seller motivation:

On the other hand, imagine that Alice, the option seller, has conviction that the DAI peg is secure and thus DAI price volatility will be very low in the future. Then, Alice should sell put options on DAI as Bob won't exercise unless the value of DAI crashes to below $0.99. Since Bob pays an option premium to Alice in return for her protection, Alice is making a profit unless DAI crashes.

Bob feels protected by Alice even though he doesn't know her because Alice has put down sufficient collateral, or margin, to protect Bob in the case that Bob needs the protection.

2.2 Selling Options

How does Alice sell options to Bob that she doesn't yet own? She can mint them from the protocol itself! Sellers, like Alice, who want to mint and sell options have to put down collateral in a margin account that we will call a "repo", which is extremely similar to a "repo" in Yield Protocol or a CDP in Maker.

Selling the contract obligates Alice to give up some amount of her collateral in the repo later if Bob wants to exercise (though she'll get another asset in return). For example if the collateral asset is ETH, Alice might have to give up some amount of ETH at (European option) or before (American option) the exercise date IN exchange for Bob's cUSDC or DAI only if Bob exercises the options contract.

It is key to note that if minters on this platform don't sell options tokens that they mint, they gain no benefit at all from minting tokens. This is because, unless the minter can sell those tokens, the tokens aren't doing anything, and the minter is in a neutral position. So, they will try to find some market on which to sell these options contracts. Minting options would only done by a party that has an interest in selling options tokens.

Some properties of these minted options are as follows:

- Put option tokens for any specific series are completely fungible
- Put option tokens are ERC20s
- Those buying and selling put options contracts will converge around some market price for the options contract.

2.3 Margin Requirement:

For now, assume that Alice must be fully collateralized: that is, her margin must be greater than or equal to the strike price, as that is the exact amount that she will send to Bob upon exercise (in return for Bob's underlying asset). It would be ideal for Alice to sell option contracts while being only partly collateralized: we will discuss capital efficiency in greater depth in the future work section.

Note that both the maximum payout, and the maximum value of a put option is its strike price, and thus, the strike price is the maximum value of the put option and the maximum amount of collateral required.

2.3.1 An Example: DAI Price Hedge

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

In order to mint the above token, if Alice wants to sell exactly one token of the above put series, she puts down exactly 0.99 USDC as collateral in a repo and specifies the above as parameters and as a result, new put option tokens are minted to her address. She can subsequently sell those options wherever and to whomever she wants (e.g. on Uniswap), which is how she collects her option premium.

Imagine that Alice sells the options contract to Bob at the market rate of 0.10 USDC (in truth, the purchase currency is irrelevant). This premium that Bob pays Alice is immediate revenue for Alice. As long as Bob holds the options contract that he had bought, the put option token gives him the right to exchange 1 DAI for 0.99 USDC on (before) 11:59 PM on December 31, 2019 with Alice (or any other seller who opened a repo for this series, to be precise).

Then later (but still before December 31st), imagine that the price of 1 DAI falls drastically to 0.50 USDC, which is far below 0.99 USDC (i.e. the put is in the money). If Bob were to try to sell his 1 DAI on a DEX, he would only get 0.50 USDC for it. However, because he bought and owns the put option, he can exercise it to sell his 1 DAI to Alice for 0.99 USDC. If he exercises, he has only lost one cent (due to a strike price of 0.99 USDC rather than 1 USDC).

2.3.2 An Example: Compound Deposit Insurance

If you deposit funds on Compound, you get a receipt, which is a interest bearing ERC20 asset called a cToken that represents your loan balance. That allows you to come later and redeem your deposited funds.

Let's say Bob has deposited USDC on Compound and gotten cUSDC in return. Bob fears that if Compound gets hacked, his $100 worth of cUSDC won't be redeemable for 100 USDC, or if the utilization ratio on Compound is 100%, and there isn't any liquidity left on Compound. 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.

Now we modify the put option in the previous example so that the underlying is cUSDC rather than DAI. As before, Alice mints and sells a put option to Bob, where Bob's put option token gives him the right to exchange $1 worth of cUSDC for 0.99 USDC before 11:59 PM on December 31, 2019 with Alice.

Then later (but still before December 31st), imagine that there is a hack or liquidity crisis on Compound and thus the amount of USDC redeemable for $1 worth of cUSDC falls drastically to 0 USDC, which is far below 0.99 USDC (i.e. the put is in the money). Therefore, Bob has the right to exercise his option to sell his 1 DAI to Alice for 0.99 USDC.

3 Ensuring Liquidity

Alice has a strong incentive to only mint tokens that she believes will be highly liquid. This is because,

1. so that she can find a buyer in a quick amount of time who will pay her a reasonable premium.
2. after selling her contract, if she wants to exit her position (in a process called unwinding which we discuss later), she would have to buy exactly as many puts as she sold, and therefore, she would want a liquid market where she could buy back the same option she sold!

3.1 Choosing Appropriate Strike Prices and Expiry Dates:

One thing that would prevent the options from becoming liquid is if there were too many types of options for Bob to choose from and thus liquidity was fragmented amongst these options, preventing a liquid market from forming around any particular series. If we limit the number of strike prices and expiry dates that valid options can have (and thus limit the number of "options series"), that would ostensibly give the options the highest chance of being liquid. We maximize liquidity by limiting the number of different types of options Alice can make. We can decide to have only one strike price and expiry date that trades at any time for every token pair. For example, at any one time, for both DAI and cUSDC insurance, only the options that expire at the end of the current quarter are actively trading. Therefore, if there are fewer different types of options trading, liquidity should be concentrated around these option types. Each put options token has its own ERC20 token contract.

3.1.1 Strike Price

We should generally choose options contracts that are at the money or slightly out of the money, as these are the most liquid in traditional finance [8], since it is in the incentive of the options holder to just exercise an in the money option.

3.1.2 Expiry

In order to encourage liquidity, we want to have as few expiry dates as possible. For example, perhaps just put options that expire at the end of the quarter are tradable. (In the last month of the current quarter, we can introduce also the option expiring at the end of the following quarter to the marketplace.) This centralizes liquidity around a few different puts.

4 Settlement

4.1 Physical Settlement and Cash Settlement

There are two main ways in which settlement occurs after Bob exercises his options:

For physically settled options, Bob must supply the underlying asset in order to exercise, but in cash settled options, Bob just needs to submit an exercise transaction, after which Alice sends him the difference between the strike price and price of the underlying asset.

4.1.1 Physical Settlement Example:

In this, 1 DAI is sent from Bob's repo account to Alice's repo account, and 0.99 USDC is transferred from Alice's repo account to Bob's repo account. (Bob is left with 0.99 USDC, while Alice is left with 1 DAI.)

4.1.2 Cash Settlement Example:

For this, we need a price oracle. Let's say that, at expiry, the price oracle says that 1 DAI is worth 0.65 USDC. Then, Bob's option is in the money by 0.34 USDC. (0.99 - 0.65). Then, if Bob exercises his option, 0.34 USDC (the net value of the option) is transferred from Alice's repo account to Bob's repo account. (Alice is left with 0.65 USDC, while Bob is left with 1 DAI plus 0.34 USDC.)

4.1.3 Benefits of Physical Settlement over Cash Settlement:

- Buyers tend to prefer physical settlement given that they receive their desired asset and feel safe given the security from 1:1 collateralization. Cash settlement opens up risks with ETH for buyers since buyers will have to convert their ETH to USDC if it's a DAI:USDC option, so buyers are exposed to a little bit of risk right after expiry.
- With fully physically settled options where the strike asset and underlying asset are the same, we can create physically settled options without a single oracle. With cash settlement, there is more dependency on oracles from needing to understand the price of the underlying relative to the collateral type in order to do settlement. In addition, in the event of a severe hack, it is unclear that oracles will be able to properly price assets like cTokens, making physical settlement better in such a case. For example, cash settlement seems to be really hard for cUSDC:USDC options as it is unlikely that there is any reliable oracle that would know the price of cUSDC in such a case.

4.1.4 Benefits of Physical Settlement over Cash Settlment:

- Buyers don't need to send the underlying asset to exercise, just an exercise transaction, meaning that buyers can trade these options without ever obtaining the underlying asset.
- Cash settlement is more capital efficient, since sellers only need to post the expected difference between the underlying and and strike price as collateral, rather than the entirety of the strike price. A more capital efficient system, all else being equal, is more likely to develop liquidity and will be far more attractive sellers. Physically settled options on the other han need to be fully collateralized and thus are less capital efficient (see Capital Efficiency section for further explanation)

5 Exercise

Bob can exercise his option in two ways:

5.1 Exercising American Options

In an option with American exercise, Bob just exercises whenever he wants to as long as his exercise transaction is received before or at expiry, at which point he sends his underlying (in physical settlement) and gets the appropriate amount of seller collateral. Essentially, he will automatically exercise on whichever repo he chooses, ideally the contract will the lowest collateralization ratio. This is the simplest form of exercise.

5.2 Exercising European Options

European exercise means that Bob can only exercise at the exact time of expiry. This creates some complication due to the nature of the blockchain. If expiry is approaching on a specific block, there's 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's effectively the same as extending expiry to a later block, and we seem to have the same problem as before.

Imagine Bob's option is sufficiently in-the-money and so he wishes to exercise, but there are 5 hours left until expiry. Bob fears that he's exercising too early: if the underlying and strike asset prices end up moving against him in the next 5 hours, he could end up exercising an out-of-the-money options come expiry and thus lose a lot 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, that means he lost money too!

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

5.2.1 American at the end

The options contract becomes American just for the final few days (or final x number of blocks). This decreases Bob's stress because he knows he has a sufficiently long time period to exercise for. However, this still is not ideal because it means that Bob gives up the time-value of his options contract in order to exercise; he is necessarily getting shortchanged by exercising early.

Theoretically speaking, the only case in which it would make sense to exercise an American option early is if it is a call option sufficiently in-the-money, and where the strike asset is higher yielding than the underlying asset. In fact, the yield he earns from today until the expiry date of the contract must be greater than the price he would get for just telling the contract today (gaining the benefits of the remaining time value), for exercising to be worthwhile. Say Bob has an option on DAI, and the price of DAI goes to .9 USDC. Then Bob's option is sufficiently in the money and he can exercise his option to get 1 USDC. However, in this case the yield on DAI is strictly better than that on USDC (from rates we've seen in DeFi to date), meaning that Bob should earn more by selling his option rather than exercising it early.

For the above, when Bob exercises, in the case of physical settlement, he sends the exercise transaction along with his underlying (say, 1 DAI) at some point during the final "American period." The exercise transaction sends all of Alice's collateral (0.99 USDC) to Bob, and sends his 1 DAI to Alice. In such a case of physical settlement, no reliance on oracles is required!

5.2.2 Using an Exercise Oracle

Using an exercise oracle allows Bob to exercise exactly on expiry. Bob sends his 1 DAI to his repo account, along with an instruction. The instruction can take one of the following two values:

- "Exercise." If this is the instruction, or, if there is no instruction accompanying the 1 DAI in Bob's repo account, then, at expiry, the 1 DAI is transferred automatically (by the exercise oracle) from Bob's repo account to Alice's repo account, while 0.99 USDC is transferred in the opposite direction.
- "Exercise if the Price oracle has a price for DAI less than x USDC." If this is the instruction, then the exercise oracle checks the price oracle for the price of DAI vs USDC, and if DAI is worth less than x USDC, then 1 DAI is transferred from Bob's repo account to Alice's, and 0.99 USDC goes in the opposite direction.

Note that if Bob doesn't want to exercise, he simply doesn't send the 1 DAI to his own repo account.

Of course, Bob can cancel his signal transaction as long as he does it ahead of time. With physically-settled options, Bob's before-expiry signal message would require Bob to transfer his DAI (note that this doesn't happen when cash settled) to the same margin account that Alice has her ETH in. Upon expiry, if the oracle determines that the put token is in the money, it allows Alice's ETH value up to the strike price to be collected by Bob (when he comes to get it), and it allows Bob's DAI, and Alice's extra "over" collateral in ETH to be collected by Alice. If the oracle determines the contract is out of the money, it merely allows Bob's DAI to be collected by Bob (if he comes to collect it) and it allows Alice to collect all of her ETH collateral (if she comes to collect it).

However, Bob does not need to do this for a cash-settled option, he could just send a before-expiry signal message to the platform. For the above, cash-settled is better.

Note that both 2 above can also be used with American options for greater comfort for Bob.

5.3 Pros and Cons of American and European Options

American options give more optionality to the buyer and thus are strictly better for the buyer. The main thing is that, for a low level of options liquidity, 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 can exercise rather than having to sell the options contract.

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 obtain options.

6 Strike Asset differs from Collateral Asset

Minting and selling the put option token obligates Alice to 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 and only 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 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 our protocol 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 on our protocol 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'd never enter into this agreement (yes, we are aware there's a difference between floating and fixed rates - we need to rewrite this part using NPVs and such).

However, imagine that Alice gets more in premiums from Bob than owning cUSDC would have yielded her. This means that Bob is essentially earning a negative interest rate on his cUSDC! It is unlikely that he would ever put his money in Compound in this case (unless of course he is not using Compound for savings, but for leverage).

Therefore, a collateral type with a high interest rate (or at least with a higher possible interest rate than the underlying) cannot be supplied as collateral by Alice because there is a large opportunity cost to doing so. Luckily, Ether fits this profile.

What we do know though is that many possible Alices 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; you basically get no interest from putting ETH down on Compound. So, if Alice puts down a bunch of ETH as margin/collateral and sells the above put option, she would get an option premium for doing so.

Let's look at an example where Alice has her margin denominated in ETH. 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 runs the risk of getting liquidated, which we discuss further in the following section.

7 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. Alice's collateral could go below some minimum collateral ratio (judging by an ETH:USDC oracle), so anyone in the system could automatically liquidate her. In order to liquidate her, someone must burn the exactly number of tokens as her repo backs. Whoever liquidates this repo should get exactly as much ETH as the strike price of those put tokens, and the rest should go back to Alice, minus a penalty, of which some goes to the liquidator and some could potentially go to the protocol creators. Alice also has the ability to add collateral and to remove collateral up to the collateral requirement.

Note that since all options in a series are fungible, the protocol contains liquidity from repos other than Alice's, allowing Bob to exercise, so he will not be bothered by Alice getting liquidated. If Bob and Alice are the only two players in the marketplace, then of course no one can liquidate Alice except for Bob himself.

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 in European options.

At any time, Alice can completely exit her short position in a process called unwinding. To unwind her own repo, she can buy any of the tokens of the previous series that she sold, and then burn them to release collateral. If she burns as many tokens as she has minted and sold, then she can completely exit her short put position (and thus unlock the entirety of her collateral). If she burns fewer tokens 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 min collateral requirement for her now smaller position size).

For Bob to unwind his position, he should just sell (on a DEX or another exchange) the options contract that he's bought. For example, if he's sold his DAI and thus doesn't want any DAI insurance any longer, he can sell his DAI puts on Uniswap. Note that, although Bob would be selling options, unlike Alice, he doesn't have a short options position because he is just selling the options he previously bought, he is not selling options that he never previously owned.

9 Capital Efficiency

The first thing to note is that 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.

Note that 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 margin requirement of an options contract is a function of implied volatility, the price of the underlying asset, the time until expiry, and the first three variables as per Black-Scholes. That is to say, Alice must have as much margin 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's a recruse problem, requiring the option to exist in the first place) so it makes it harder.

In such a scheme, under normal currencies, the capital efficiency of the protocol is lower 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 max 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.

(in the above, explain how adding collateral and liquidations work)

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 doesn't 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.

10 Helping Alice sell puts

By definition, it would be difficult for users to use the platform until the put tokens had liquidity. As we expressed above, Alice only mints puts if she feels reasonably certain that she can sell them quickly for a fair price.

Thus far, we have assumed the existence of DEXes that can handle the level of options liquidity that Alice requires. However, we can help Alice out a little bit. The first way is by creating the equivalent of Oasis.DEX for put tokens: the first DEX specifically designed for trading options tokens. The features of such a DEX are unclear, but a specialized DEX just for DAI seemed to work quite well for Maker.

Note that the above are in no way necessary for the system to operate smoothly.

11 Extending the Protocol to Call Options

Though we have referred to these put options for the entirety of the paper, since they're 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 .95 USDC, this is the same as a call option that gives him the right to buy .95 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.

12 Future Work

In order to make this protocol more attractive to sellers like Alice, we might want to work on collateral rehypothecation: yTokens as collateral!

12.1 Reverse Dutch Auctions Option Sales

Additionally, we could implement a reverse dutch auction for options sales as well. This means that, after Alice mints the option, a reverse dutch auction is started whereby the protocol attempts to sell the option for Alice. Beginning at the maximum price of the put option (which is for some amount until the strike price, the protocol offers up the option for sale, and reduces the offer price until there is a buyer.

12.2 Perpetual Options

Intuitively, if these options could be perpetual / always provide cover to whoever holds the tokenized long side, then we would significantly increase fungibility because all options would have the same expiry date (time infinity). Of course, in traditional finance, options must expire in order to have a finite value. (not 100% sure that's true actually, will have to work it out).

One way in order to create a perpetual option of this type is through a rollover: by stringing together an infinite number of options of finite expiry, we can create a single options contract with infinite expiry. The difficulty is creating some kind of structure that allows a user to get perpetual insurance without having to periodically buy a new fixed term options. Some researchers (i.e. Dan Robinson at Paradigm) are working on the aforementioned.

So, can we make these options have a subscription value? (the payment model still makes no sense), capital efficiency, more collateral types, off-chain stuff as well!

If these options are perpetual, then they must be American (the notion of exercising only on expiry, like in a European option, makes no sense if there is no expiry).

So, if we want these puts to be perfectly fungible and perpetual for Compound Deposits we can't have a finite strike price because as the value of cUSDC increases relative to USDC, the strike price should be steadily increasing to reflect this fact. Therefore, our strike price must be formulaic. Imagine the strike price is constant * max cUSDC:USDC ratio ever. If the constant was 1, then we'd be able to sell our cUSDC for exactly the best ratio that Compound has seen thus far.

Alice is the one who would need to continue paying Bob for this to be perpetual. This is the hard part. A floating rate taken once a week could be something, which means that essentially this token never expires, however, the rate could be decided in a Compound like style and based on the pool of buyers and sellers. The problem is that Bob shouldn't feel scared that his premium will arbitrarily increase; he's buying protection!

12.3 Compound-style

In the Compound style model, insurance purchasers need to continually pay interest to the sellers of insurance, kind of like a CDS. They put their cUSDC into our contract, and some of the interest gets paid to the other side of the trade. The amount of interest that's paid is determined formulaically by supply and demand for insurance.

How do we determine how much collateral Alice needs to post?

12.4 Multi-Collateral

Like Maker, our protocol would benefit from having multiple uncorrelated collateral assets.

12.5 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. The biggest distinction between Yield and unlike Maker. Another large distinction between Yield and our protocol is that, compared to Yield, options contracts, in expectation, decrease in value over time, which should imply more sell-side demand.

12.6 Peer To Contract

Like Maker, this is a peer to contract system. In the maker system, if you were the first person ever to mint DAI, you're going to have difficulty finding someone to sell it to. However, once there is a liquid market for DAI, you can take your minted DAI and immediately use it or sell it (for more ETH, for example). The exact same is true of our put tokens. Peer to Contract systems tend to have more liquidity, are easier for users, allow for easier application composability, are better suited to the liveness properties of the blockchain, and have been more empirically successful than their peer to peer counterparts in DeFi [7].

Acknowledgments

This paper is heavily based on a number of conversations the author had with Robert Leshner of Compound and Dan Robinson of Paradigm who remained extremely helpful throughout the writing of the paper. Really appreciated feedback from Allison Lu, Fred Ehrsam, Matt Huang, Arjun Balaji, Tom Schmidt, Cyrus Younessi, Roderik van der Graaf, Tina Zhen on their thoughts and feedback on the contents of this paper.

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

References

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

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

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

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

[5] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin - Open Source P2P Money, 2008.

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

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

[8] 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