DefiHedge: A Marketplace for Fixed Rate Defi Lending and Interest-Rate Derivatives

Draft 0.1.0

Julian Traversa
JulianT@nescience.io
Nescience Software & Capital

William Hsieh
whsu2012@gmail.com
The Raytheon Company

March 8, 2020 (Deprecated With Current Build)

1 Introduction

Since Ethereum's inception, its ecosystem of decentralized financial applications has steadily progressed towards providing the financial infrastructure necessary to avoid traditional centralized financial services. Today, nearly $1 Billion are locked into decentralized protocols, a number which peaked at $1.22 Billion in February of 2020[1].

Unfortunately, while this market has seen significant adoption, the decentralized & trust-less market lacks the financial infrastructure to provide fixed-rate lending and/or interest-rate derivative markets.

Further, while the available variable-rate lending services (e.g. Compound, DyDx, Fulcrum) allow those with surplus assets to put them to use, and those without assets to utilize the time value of said surplus, only those with a high risk tolerance find the volatile rates that these services offer to be acceptable.

Users who do not accept this volatility are then left with blockchain assets that are deflationary/stagnant. These users are forced to adopt a number of centralized blockchain lending services in order to utilize their assets. Centralized lending services however carry the risk of all centralized & trust based blockchain services. One must trust the exchange not to be hacked, make errors with your lending position, or exit scam, in addition to the centralized pay-to-play process behind asset selection.

Alternatively, users who find these potentially volatile rates within their risk tolerance are limited in terms of their exposure to these rates. Without the existence of decentralized interest-rate derivative markets/interest rate swaps, one can only benefit from an 8% rate to the extent that they can extend their capital.

In this paper we introduce a unique, trust-less decentralized protocol which enables the offering of fixed-rate peer-to-peer loans in addition to derivative interest-rate markets. In doing so we enable users to hedge against the volatility of decentralized finance while giving others the ability to leverage their capital through access to derivative interest-rate markets.

2 The DefiHedge Protocol

DefiHedge is a decentralized protocol & exchange built on the Ethereum blockchain, utilizing the Compound Protocol. DefiHedge establishes an infrastructure for the creation of algorithmically defined fixed-rate lending contracts & swaps through the use of strictly defined smart contracts.

Offerers are able to interact with our lending market to create a fixed-rate loan contract for any Ethereum token (offered by Compound). Takers are then able to fill the offer's terms, locking in both the maker and taker's funds until the term is complete.

Each offer/lending contract is a unique smart contract and as such provides a transparent and publicly available ledger which records all contract terms and events.

2.1 Fixed-Side Offer Contracts

Unlike the Compound Protocol, DefiHedge does not currently aggregate contracts into a single fungible pool. Similar to a traditional exchange, DefiHedge's infrastructure involves standard market participants in the form of offer makers and offer takers. While this infrastructure limits automatic rate arbitration, such a system is necessary in order to uniquely define the terms of each contract.

In order to ensure liquidity and organizational structure, the available markets are defined by fixed time periods (e.g. 1 week, 3 month, 1 year). Limiting offers to specific term lengths results in increased activity in the given defined markets, therefore increasing the efficiency of rate arbitration across the protocol and improving the experience of the user.

2.1.1 Use Cases

Individuals with long-term investments in Ethereum based assets may find that an excessive, yet highly variable rate (e.g. DAI: 3-12%) offers significantly more risk than a high fixed-rate. For those with a sensitive risk tolerance, DefiHedge provides the ability to hedge their investment and reduce their risk profile through an interest rate swap.

Given the exchange structure, users are provided the opportunity to arbitrage fixed-rates and speculate on fixed-rates within DefiHedge. Provided multiple term markets for a single asset, and significant DeFi rate volatility, users can easily arbitrage across available term periods and lock in additional rate profit by filling rates lower than their own fixed rate.

In traditional finance, companies with very high credit ratings are able to issue bonds at rates low enough to arbitrage the fixed rate they are receiving. Depending on the regulatory environment DefiHedge expands the range of companies that can find similar activities profitable. Should the DeFiHedge fixed yield considerably beat market rates, companies with a wider range of credit ratings would be able to issue high rate bonds and still find profit without significant risk.

2.2 Floating-Side Offer Contracts

Once a lending offer has been created, DefiHedge allows users to easily select and fill a given lending contract, locking both the taker and maker's capital into the DefiHedge lending contract for the agreed upon term.

Using the DefiHedge user interface/exchange, users can quickly identify current market rates and analyze DeFi trends. Once an offer is created, it is treated similar to an order on a traditional exchange.

Those with capital who wish to lock in a fixed rate are able to create an offer above market price (rate) or are able to fill a floating-side offer at the current market price.

Those users with the collateral to cover a fixed-rate offering and desire to speculate on the variable/fixed spread are able to create an offer below market price (rate) or are able to fill a fixed-side offer at the current market price.

As an alternative to using the DefiHedge interface/exchange, at any point after a lending contract has been created users can easily access the parameters of the contract and lock it in through basic web3 calls.

2.2.1 Use Cases

For those with a high risk tolerance and those wishing to take a long position on DeFi rates, DefiHedge provides the ability to extend their investment significantly and offers users the ability to take leveraged positions on DeFi rates through a process similar to a traditional interest rate swap.

For example, a user wants to long the current 8% DAI rate. Using DeFi hedge, with only $50, this user could cover a theoretical fixed rate 5% APR bond for one year. Should the DAI rate remain at 8%, the user would stand to gain $31.50, a 63% year over year gain, a yield nearly 8x that of the 8% DAI rate that the $50 would have otherwise been accumulating.

In traditional finance, this strategy is usually employed by companies with a high enough credit rating to issue bonds at a low fixed rate. With DefiHedge, this opportunity is expanded such that any user can employ similar high yield strategies.

2.3 Potential Developments

DefiHedge provides the initial infrastructure for a number of interest rate derivates. Future implementations could include Caps, Floors & Swaptions. The Bank for International Settlements estimated the notional value of all OTC derivates to be $524 Trillion at the end of June-2019. DefiHedge intends to be the first to bridge the gap between the growing decentralized finance industry and the established interest rate derivative market.

3 Implementation

DefiHedge's initial implementation is based around an initial smart contract which has the ability to create additional smart contracts, given certain parameters are met. This results in a system which allows any Ethereum user to trustlessly issue binding lending contracts. At this time the protocol is easily accessable on the Ropsten network for use by dApp's, institutions, and individuals.

3.1 Broker Contract

The core of the DefiHedge protocol is the Broker Contract. Using the Broker Contract users can specify the currency they wish to offer, the length of the bond, the amount of currency, and the rate they are offering. Once a user has determined these parameters, the contract both deploys a unique offer contract and ensures the correct funding has been sent between the user and the newly deployed contract.

Functions	Parameters & Description
	uint value, *uint* duration, *uint* rate
offerEthFloatingSide	Creates an offer to fill a fixed rate Eth swap at the given duration and rate. The value parameter is taken as the value sent with the transaction.
	uint tokenNumber, *address* tokenAddress, *uint* duration, *uint* rate
offerErcFloatingSide	Creates an offer to fill a fixed rate ERC swap for the given token, duration and rate. The offer contract first must be approved to move the ERC tokens.
	uint value, *uint* duration, *uint* rate
offerEthFixedSide	Creates an offer for a fixed rate Eth swap at the given duration and rate. The value parameter is taken as the value sent with the transaction.
	uint tokenNumber, *address* tokenAddress, *uint* duration, *uint* rate
offerErcFixedSide	Creates an offer for a fixed rate ERC swap for the given token, duration and rate. The offer contract first must be approved to move the ERC tokens.

3.2 Floating-Side Offer Contracts

Once a floating-side offer contract has been created, all of the initial offerer's funds are transferred to the contract address and it can either be confirmed/locked in, or aborted.

Should the offerer wish to change the terms of the loan or cancel their offer, they can do so easily with the abort() function so long as the network is able to process the abort call before another user locks in the contract.

Alternatively, other users can confirm the floating-side offer contract by agreeing to its terms and taking the opposing fixed-side position. In taking the opposing fixed-side position, one would be agreeing to provide the correct notional capital needed to meet the fixed-side offer's position size. Once the offer has been confirmed, funds are pooled together in the contract and are turned into the appropriate interest bearing compound cToken using the mint() function.

For example, if a user created a floating-side offer contract with a position size (interest) of \$50 at 5% APR, the corrosponding fixed-side user would need to provide \$1000 in notional value to the contract. Once confirmed, the \$1050 are immediately supplied to the compound protocol and turned into cTokens.

Once the contracts terms have been completed, either user can trigger the bondRelease() function which returns the fixed-side user their initial capital + interest,

while returning the floating-side user the remainder of the capital. This can be done automatically with future DefiHedge implementations.

3.3 Fixed-Side Offer Contracts

Similar to a floating-side offer contract, once a fixed-side offer contract has been created, all the offerer's funds are transferred to the contract and the given functions can then be called to either lock in, or abort, the fixed-side offer contract.

Should the offerer wish to change the terms or cancel the offer, he/she can do so with a low cost abort() call to the contract. So long as your transaction is processed before it is locked in, the offerer's funds are immediately and seamlessly returned.

Should another user find the terms of the offer agreeable, he/she can lock in the offer by calling the takeOffer() function and agreeing to cover the opposing float-side position. In doing so, the taker agrees to provide the capital to cover the entire fixed rate bond up front. This ensures that the terms of the bond are enforceable without the need for credit approval and without the possibility of the taker absconding with their capital. Once the contract is locked in, the funds are pooled, supplied to the Compound Protocol and minted into cTokens.

For example, if a user created a fixed-side offer contract with a position size of $1000 at 5% APR, a user would need to provide $50 up front to the contract. In doing so, it ensures that the fixed-side user always receives their fixed rate. Once confirmed, the pooled $1050 are seamlessly minted into cTokens, receiving interest on the Compound Protocol.

As with floating-side offer contracts, the bondRelease() function can only be called once the bond term has expired. Once called, the contract immediately redeem's the available Compound cTokens and returns the fixed-side user their initial capital + interest, and the floating-side user the remaining capital available in the contract.

Public Functions	Modifiers & Description
abort()	Can only be executed by offerer.
	Aborts the contract and returns funds to the offerer.
takeOffer()	Requires contract approval before ERC-20 offers can be confirmed. Requires appropriate capital.
	Locks in the terms of the contract, in the process pooling funds and supplying them to the compound protocol.
bondRelease()	Either party can call the bondRelease() function once the timeLock time has passed.
	Redeem's cTokens and immediately returns a fixed rate to one party and the remaining funds to the other.
Events: Aborted() OfferConfirmed() termEnded()	Events Emit: Aborted(): (*address* contractAddress) OfferConfirmed(): (*address* contractAddress, ..., *uint* rate, *uint* lockTime) termEnded(): (*address* contractAddress)

3.4 Exchange Architecture

In order to access the DefiHedge protocol, users can either interact directly using a smart contract, implement their own web3 interface/exchange, or utilize the DefiHedge exchange.

The DefiHedge exchange will resemble most other contemporary decentralized exchanges. There is a given selection of assets/markets available for users to select. Assets in DefiHedge will be unique markets determined by asset+term duration.

For example, the first two assets likely to be offered by the protocol will be ETH and DAI. The theoretical DefiHedge markets offered then consist of:

ETH1MONTH	DAI1MONTH
ETH3MONTH	DAI3MONTH
ETH6MONTH	DAI6MONTH

Rates are arbitrated similar to price on a normal exchange, organized with fixed/float side offers meeting at a market rate. In kind, order size would equate to the nominational value (size) of the position.

Unlike most current DEX dApps, the initial MVP implementation will store orders (offers) on-chain. Given potential issues with such a design under high congestion, this exchange design will be depreciated by an alternative, likely similar to current 0x architecture. While most users will transition, the on-chain protocol will continue to operate for those who wish for complete decentralization or those users under restrictive governments.

Proposed are two primary research designs:

- 0x design: The transition to on-chain transactions off-chain order matching is relatively intuitive, technically less challenging than other potential implementations, and relies much less on consistent liquidity providers.

  This involves launching DefiHedge as an initial relayer while providing the infrastructure for additional relayers to add liquidity to the protocol. Some issues are presented with an 0x based design, however most are ameliorated with further improvements in Ethereum main chain scalability, layer 2 child-chains, or extension contracts.

- Kyber design: While a path to efficient implementation may not be immediately apparent, a Kyberesque system may also be possible.

  A design based on the Kyber Network requires a large network/community of liquidity providers which itself requires significant investment (time/capital) to acquire. Further, while the slippage seen on the Kyber Network may be acceptable for those accepting the terms of a trade, rate slippage would be seen as a critical issue preventing adoption of a lending system.

In addition to exchange architecture design/research, we are tracking technologies such as optimistic rollups (e.g. loopring), STARK's (e.g. 0x STARKDex) and general Eth 2.0/sharding which each significantly reduce the possibility of attack vectors found in both on-chain or 0x-based exchanges:

- DDOS attacks
- Sybil attacks
- Race condition attacks/frontrunning
- fee loss

Such technologies would significantly reduce the issues apparent in both on-chain order designs and 0x based designs, and as such must be considered in our decision making process.

3.5 Governance

As with similar protocols, DefiHedge will initially retain centralized control of the protocol and, over time, transition to decentralized governance. Fundamentally, this involves ensuring that the primary stakeholders and the community as a whole are granted proportional governmental control. Should the exchange feature an 0x-based design, the DefiHedge exchange will remain a portal to access the DefiHedge protocol and forfeit any disproportionate voting/governance power. Future governance includes:

- The addition/approval of available Compound cToken markets.
- The removal/halting of approved markets
- The ability to delegate a new admin, allowing continuous democratic processes
- The addition of further derivative markets
- The addition of relayer/exchange incentivization
- The ability to implement an opt-in contract recovery protocol

4 Summary

- The DefiHedge protocol provides the infrastructure to create functioning, trustless interest-rate derivative markets (swaps).
- The DefiHedge exchange provides an interface to access the DefiHedge protocol, and is structured similar to most exchanges.
- As with other exchanges, users can create offers, and/or take offers, while arbitrating an acceptable market rate.
- Using DefiHedge, users can quickly and safely accept the terms of a trustless peer-to-peer fixed-rate bond or take a leveraged position on current DeFi interest rates.