A composable margin trading and lending protocol

Version 2.0
November 15, 2022

Overview

In this document, we will explore Dolomite's technical infrastructure. Dolomite is a decentralized exchange (DEX) that allows for trustless trade settlement and overcollateralized loans, never assumes custody of its users' funds, offers margin trading using spot settlement of assets, and provides on-chain liquidity through use of automated market maker (AMM) pools.

Introduction

Dolomite's infrastructure is centered around a suite of smart contracts that are written in Solidity and are deployed to the Arbitrum Ethereum layer 2 for public, transparent settlement. Solidity smart contracts offer the benefit of being publicly auditable, meaning the code and rules for a system can be seen and analyzed by anyone, at any time. Moreover, the state of any system that uses these smart contracts can be analyzed at any point in time to ensure the soundness of a system throughout its entire history. In an environment where trust is earned by remaining transparent and access to a system is fairly distributed, a system built around smart contracts is most certainly the way of the future.

The basis for these smart contracts were forked from dYdX, another company in the cryptocurrency industry, with minor changes (written in more detail here) made to the core system that greatly enhance its prior featureset. Meaning, audits of the protocol by Open Zeppelin and Bramah Systems should still be applicable. The changes that were made to the core and the new modules that hook into the system are described below, and have been audited by SECBIT in August of 2021. Some additional changes to the system were added after SECBIT's security audit, but those additional changes, including the rest of the system, have 100% test and branch coverage.

The goal of this infrastructure and system is to enable easy and unstoppable access to spot trading, margin trading, passive liquidity provisioning, and other financial instruments through nothing more than a cryptocurrency wallet. It is important that systems that are fragile to price movements are incapable of going down and minimize any centralized points of failure. Dolomite intends to be amongst the first decentralized exchanges to tie major trends in decentralized finance (DeFi) into a uniform, sleek, and capital-efficient system that users can access at any time, from any type of device.

Over time, the protocol's ownership will be democratized, to be owned by an on-chain DAO. Such a DAO would only be able to flourish and be decentralized if the protocol it governs is built purely on-chain, with ownership distributed amongst a wide variety of users, stakeholders, and others.

Note, all numeric figures reflect the state of the protocol to be deployed at the time of publication.

How the Base Protocol Works

The suite of smart contracts acts as its own ecosystem, which dictates which markets are supported, how interest accrues, ownership of the protocol, risk parameters of the global ecosystem, and risk parameters that are unique to individual assets. The base smart contracts are *not upgradeable* and all base logic cannot be changed. Modules (called *Operators*) can be added or removed from the protocol, which allows aspects or certain interactions to change. However, base-layer rules, like how ownership is defined, risk limitations (how high or low certain protocol terms can go and be set), math regarding interest rate accrual, math regarding collateralization, the need to stay collateralized, and the need to spot settle all transactions cannot change. The only way to change these rules would be forking the protocol, deploying a new one, and for users to opt into moving to the new one by explicitly migrating their crypto. To start their interaction with the system, users must deposit any supported crypto. For the sake of example, we will use ETH and DAI (a stablecoin that is pegged to 1 USD) throughout this document.

Performing a deposit increments the user's internal balance in the protocol. Balances in the protocol are pooled amongst all users, so if user A deposits 100 DAI and user B deposits 200 DAI, the protocol's aggregate ERC20 balance is 300 DAI. Each user's internal balance is 100 DAI and 200 DAI respectively. Users may withdraw at any time, and there are no fees for depositing or withdrawing outside of ordinary network (gas) fees. Through use of cryptography, users opt into all transactions, and the owners of the protocol never assume custody of the user's crypto, at any point. After performing a deposit, each user's funds are immediately made available, in a pooled manner, for lending, allowing a counterparty to use the aggregate balance for borrowing (in this case, 300 DAI).

Trading from within the Dolomite ecosystem can occur in one of two ways. The first way is through internal transfers, in which one user's balance is exchanged with another user. In such an event, the aggregate balance of the protocol does not change. Rather, the internal balances amongst the two users would have changed. This is how most trading will be done, and it is the only way the Dolomite interface will support. The second way to trade is from one user to an external protocol. A user could, for example, perform a trade with a Uniswap pool (another on-chain DEX), exchanging funds with the pool. The user's internal balance would reflect the trade's terms, and the aggregate balance of the protocol would change too, to reflect the crypto that left and entered the system.

Position values are marked in USD using prices that are written on-chain by Chainlink oracles. Chainlink is an immensely important aspect of maintaining the health and security of the system. Whenever the price of a supported asset deviates by a slight percentage, or after an expiry window, Chainlink oracles post new prices on-chain in a timely manner, making them consumable by the margin protocol. In deploying Dolomite to a layer-2 solution, Chainlink will be able to post more granular and even more timely price data whenever the price of a crypto asset changes (compared to layer-1 Ethereum). This will further reduce the likelihood of black swan events in which a base layer-1 blockchain is too congested to process price updates.

When a user wishes to borrow from the protocol, it must be done in an overcollateralized manner such that the value of collateral held in the user's internal balance is greater than the value borrowed, plus the minimum collateralization threshold. When a user borrows crypto, their internal balance goes negative. A balance of -100 DAI indicates the user borrowed 100 DAI. Any user that borrows crypto must pay an algorithmically-determined interest rate to the pooled balance of the protocol, in exchange for borrowing crypto. There are currently no origination fees for borrowing crypto from the system.

Interest rates in the protocol are represented as APR and are determined by the utilization rate of that specific crypto's balance. Meaning, if there is 300 DAI available in the pool and 100 DAI being borrowed, the utilization rate is said to be 33% (100 / 300). As the utilization rate increases, the interest rate paid by borrowers increases to a maximum (at the time of writing) of 100%. Lenders receive a fraction, currently 90%, of what the borrowers pay (called the *Earnings Rate*). This 10% delta becomes one of the ways the protocol earns revenue. Meaning, if the protocol has 100,000,000 DAI being borrowed and a borrow rate of 10% APR, the protocol would earn 1% APR, equal to about 1,000,000 DAI per year. The remaining 9% APR goes to the lenders, who deposited the DAI into the system. However, the 9% APR (9,000,000 DAI per year) would be distributed to all DAI depositors, which, at a utilization rate of, say, 60%, is 166,666,666 DAI. That would make the DAI lending interest rate 9,000,000 DAI per year / 166,666,666 DAI deposited equal to 5.4%. Keep in mind, these interest rates and utilization numbers are used for the sake of example and they differ from the deployed parameters.

Upon trading with borrowed funds through method two (mentioned above), in which crypto leaves the protocol to be traded with an external system, there may be a shortage of that borrowed crypto available for the lender to process a withdrawal. In this scenario, the interest rate would move toward the maximum allowable value (presently 100% APR),

because the utilization rate would have to be really high for this to happen. Economic theory would suggest the user would not want to withdraw if the APR were that high. However, more importantly, it would entice more lenders to provide liquidity, arbitraging other rates in the industry, lowering the rates back to a normal level.

An extremely important aspect of any margin protocol is maintaining solvency. If the value of the user's collateral drops to be worth less than 115% (at the time of writing; this figure may change in the future or for specific collateral types) of the user's borrowed crypto, the account will be subject to liquidation. Liquidations forcefully repay any debt that is owed by a borrower by transferring an equivalent amount of collateral from the borrower to the liquidator, plus a liquidation penalty of 5% (this figure may change in the future). In an example, if a user borrows 2000 DAI, holds 2 ETH as collateral, and the value of ETH drops below 1,150 DAI per ETH, the liquidator would receive -2000 DAI and ~+1.8261 ETH (2,000 DAI in debt * penalty of 5% / 1,150 DAI per ETH). Presumably, the liquidator would then proceed to sell the ETH for 2000 DAI on the market, leaving approximately ~0.0869 ETH left as a reward (excluding any potential trading fees) for performing the liquidation. It is intended that over time the liquidation penalty and minimum collateralization goes down, as Dolomite markets increase in liquidity, reducing the need for such large buffers. Moreover, the deployment to an Ethereum layer 2 system increases transaction throughput and speed, reducing the risk that latency or network congestion can affect the health of the system.

Most importantly, the role of being a liquidator is permissionless, allowing anyone to participate in this process and reap the reward. This is important in decentralizing all aspects of the system, asserting fairness and transparency in when liquidations can occur to a user's position. Over time, liquidations will be triggered via Chainlink oracles, who will get paid a slight premium in LINK for executing this job, and the DAO will receive the reward. Over time, the DAO's protocol-owned liquidity can serve as a backstop in case of a black swan event, in which collateral cannot be liquidated fast enough. Thus the reward from liquidations would be socialized to DAO participants. Interestingly, a DAO member that is liquidated, but owns a stake in the DAO, would not really be paying the full 5% liquidation penalty since the penalty would be effectively paid to themselves, as a DAO participant.

The base margin protocol allows users to execute arbitrary action(s), upon interaction. For the sake of simplicity for the user and other integrators, most interaction is done through *Operators* that string together the appropriate actions with the requested parameters. The

supported actions are *Deposit*, *Withdraw*, *Transfer*, *Buy*, *Sell*, *Trade*, *Liquidate*, *Vaporize*, and *Call*. *Trade* is for exchanging internal balances amongst two protocol users, while *Buy* and *Sell* are for exchanging with external protocols. At the end of a sequence of actions, basic checks are done, like if the user is collateralized. This means users are able to execute more complex actions like *flash loans*, in which capital is borrowed from the system, but must be repaid before the checks are done at the end of a sequence of actions. In DeFi, this is typically used to close arbitrage opportunities and perform other types of rebalancing transactions. *Vaporize* is a step beyond liquidation that occurs if a user's account is completely insolvent - the debt outweighs the assets of the account. Recalling mention of the DAO as a liquidity backstop, this is one instance where it could be used to process necessary vaporizations to maintain solvency.

Changes to the dYdX Base Protocol

In an effort to reduce redundancy of maintaining this document and the README on GitHub, please refer to this bullet point list that highlights all changes. As a team, we are most notably proud of the changes made to the system that allow the protocol to list tons of markets without cratering the protocol. This will be one of the first times a DeFi lending protocol is able to list all assets in a non-isolated, pooled manner, without compromising the risk profile of the pool nor DOSing itself by maintenance gas costs that scale linearly with each new asset that's supported. Most importantly, all capital will be able to be efficiently shared without partitioning funds throughout many isolated pools.

Capital Efficiency with Integrated AMM Pools

One major feature that was built directly into protocol as a new *Global Operator* is AMM pools. The overall logic was originally written by the Uniswap team (using Uniswap v2), but was altered heavily to mesh well with the margin protocol as a base. In doing so, AMMs are able to maintain exposure to the interest that is paid to them by borrowers. Moreover, the funds pooled in this AMM manner are able to be borrowed by users too. This means a pool with, for example, 1,000 DAI and 1 ETH may contain 1,100 DAI and 1.05 ETH at the end of 1 year from lending interest rates alone, excluding any swap fees that are collected. Technically, these pools are owned by the users that provide liquidity to them, and trades with these pools do not change the aggregate balance of the protocol, since they are done internally between the user and the AMM pool.

One major change to the Uniswap v2 logic is the removal of executing arbitrary code during a swap. As a team, we thought this feature was no longer needed, since it could already be done within dYdX's core architecture, and would potentially expose the protocol to more complex attack vectors. See *Flash Swaps* to learn more about this feature in the original Uniswap v2.

These AMM pools charge the user a static 0.3% fee for executing any trades against them. Presently, all 0.3% goes to liquidity providers. Once the DAO is created, the trade fees will be split 0.20% to liquidity providers and 0.10% to the DAO participants. Upon transitioning to the DAO, this will be another method through which revenue could be accrued. Over time, these static fees can be lowered to (near) 0% once the LP tokens are added to the protocol as a collateral and borrowable asset. Reason being, users will be able to borrow the LP tokens and break them into their two underlying assets, allowing traders to speculate on the impermanent loss of a specific AMM pool on the platform. Thus, converting any impermanent loss (IL) into an *impermanent gain* for effectively going "long volatility" for that specific LP token. Instead, LP participants would be more accurately compensated for their risk by users taking the other side of the trade (LPs are effectively short volatility because they preserve capital when prices don't diverge from their entry).

Over time, the team thinks this model for executing trades could be improved to also use ranged orders (similar to Uniswap V3), that can close as ranged limit orders or limit orders at static prices. This is a key area in which the team would like to improve the trading experience, while fully meshing it into the margin protocol.

Aside from allowing users to "long volatility" by supplying their LP tokens to shorts, they can also borrow (for example, USDC) against the value of their LP tokens to yield farm elsewhere, create their own hedges against impermanent loss, and much more. The possibilities and new alpha this will unlock for LPs are expansive.

Admin Rights

At the time of launch, the protocol will be managed by a multi-signature wallet that is owned by Dolomite's executive team. The company behind Dolomite is Leavitt Innovations, Inc. - a Delaware corporation. Any administrative action is time-gated by 48 hours, and will ramp up to 1 week over time, to protect users from quick and unexpected changes. Once the DAO takes control of the protocol, this multi-signature wallet will be replaced by the DAO's governance contracts (most likely Compound's Governor Bravo or something

similar). The DAO's physical entity will likely be an offshore foundation, which, at the time of writing, is still in the process of being established. The implications of these administrative rights include the ability to make the following changes and perform the following actions on the protocol:

- Withdrawing excess tokens that accrue from the delta between what borrowers pay and what lenders receive
- Withdrawing unsupported tokens that are sent to the protocol (likely accidentally)
- Adding new markets, represented as ERC-20 tokens
- Closing old markets, which only disables borrowing. It does not remove a market completely
- Recycling any markets that are marked as *recyclable*, allowing their internal IDs to be reused, for efficiency's sake
- Changing the price oracle for a market
- Changing the interest accrual method for a market
- Changing the margin premium for a market, requiring users maintain a higher collateralization to avoid collateralization for this particular market
- Changing the reward premium for a market, rewarding liquidators with a larger reward upon liquidating this particular market
- Changing the global margin ratio, below which users may be liquidated. This value is capped at a maximum of 200%
- Changing the global liquidation reward, which is given to liquidators for maintaining the system's solvency. This value is capped at a maximum of 50%
- Changing the earnings rate, which dictates how much of the borrowers' accrued interest should be paid to lenders. This value is capped at 100%
- Changing the minimum borrowed value, which restricts borrowers from having an out-standing debt of less than this value. This value is currently 0
- Adding and removing *Global Operators*, which are allowed to perform actions on behalf of on any account. This is intended for smart contracts, which implement their own logic regarding permissioned access

Transition to a DAO

Over time, the goal of this on-chain ecosystem is to hand control to the users that help add to its value. Liquidity providers, traders, lenders, builders, and other community members all comprise an important backbone in curating a strong ecosystem from what is originally a business-ran product. To minimize points of failure, align incentives, and remove unilateral control over the protocol's ownership, transitioning to a DAO is extremely

important. It is expected to occur in late 2022 or early 2023, occurring in a few short phases. Upon doing so, all administrative rights, revenue to be earned by the protocol through trading fees, the interest spread, liquidations, and more would be transferred to the DAO.

Protocol Risks and Their Mitigation

With running an on-chain margin and trading system, there are plenty of risks of which to be aware, and this list may not contain them all. Smart contracts are still considered to be an experimental technology. Although security audits have been performed by top firms on the technology and there are hundreds of tests written that contain 100% code/branch coverage, there is still the possibility of bugs being uncovered that result in funds being locked in or stolen from the system. If the base layer-2 system on which the protocol runs is halted or otherwise compromised, it could result in positions going underwater or other negative effects that are unknown at the time of writing.

If the keys to the wallets that control the administrator's multi-signature wallet are compromised, it can have detrimental effects on the system. For example, adding a *Global Operator* that is able to steal funds from users. To mitigate this risk in the short term, the time delay of 48 hours enables the team and users to monitor the state of the system and broadcast any changes that are going to occur. In doing so, our hope is users will have the time to react accordingly if the system is ever hijacked. With the system transitioning to a DAO, a few wallets being hijacked would not be able to compromise this system.

If the liquidators do not fulfill their job in a timely manner during times of volatility, it could cause individual positions, and eventually the system, to go insolvent. By starting with a higher minimum collateralization of 115% and a liquidation reward of 5%, the decentralized network of liquidators should be properly incentivized to perform their role.

If liquidity providers do not properly understand the risk they are taking upon contributing to the system's automated market maker (AMM) pools, it could result in financial losses. By supporting asset pairs that are likely to trade within a range (for example, DAI-USDC), closely monitoring their positions, or performing hedging strategies, liquidity providers can take on less risk of impermanent loss (IL).

Disclaimers

This document was written to explain how Dolomite's protocol works. It was not written to constitute investment advice. Readers should always perform due diligence on any products they are looking to use and they should exercise caution when using new and experimental technologies.