Euler

White Paper

Find out how Euler works and how it differs from other popular lending protocols

Abstract

Here, we present Euler: a permissionless lending protocol custom-built to help users lend and borrow digital assets. The purpose of this white paper is to describe how Euler works at a high level and highlight new features and innovations that help to set it apart from other popular lending protocols, like Compound and Aave.

Introduction

Euler comprises a set of smart contracts deployed on the Ethereum blockchain that can be openly accessed by anyone with an internet connection. Euler is managed by holders of a protocol native governance token called Euler Governance Token (EUL). Euler is entirely non-custodial; users are responsible for managing their own funds.

A convenient and user-friendly front-end to for the Euler smart contracts is hosted at https://app.euler.finance. However, users are free to access the protocol in whatever format they wish; a popular alternative can be found at https://instadapp.io/.

Permissionless Listing

Euler lets its users determine which assets are listed. To enable this functionality, Euler uses Uniswap v3 as a core dependency (4). Any asset that has a WETH pair on Uniswap v3 can be added as a lending market on Euler (5).

Asset Tiers

Permissionless listing is much riskier on decentralised lending protocols than on other DeFi protocols, like decentralised exchanges, because of the potential for risk to spill over from one pool to another in quick succession. For example, if a collateral asset suddenly decreases in price, and subsequent liquidations fail to repay borrowers' debts sufficiently, then the pools of multiple different types of assets can be left with bad debts.

To counter these challenges, Euler uses risk-based asset tiers to protect the protocol and its users:

Isolation-tier assets are available for ordinary lending and borrowing, but they cannot be used as collateral to borrow other assets, and they can only be borrowed in isolation. What this means is that they cannot be borrowed alongside other assets using the same pool of collateral. For example, if a user has USDC and DAI as collateral, and they want to borrow isolation-tier asset ABC, then they can *only* borrow ABC. If they later want to borrow another token, XYZ, then they can only do so using a separate account on Euler.

Cross-tier assets are available for ordinary lending and borrowing, and cannot be used as collateral to borrow other assets, but they can be borrowed alongside other assets. For example, if a user has USDC and DAI as collateral, and they want to borrow cross-tier assets ABC and XYZ, then they can do so from a single account on Euler.

Collateral-tier assets are available for ordinary lending and borrowing, cross-borrowing, and they can be used as collateral. For example, a user can deposit collateral assets DAI and USDC, and use them to borrow collateral assets UNI and LINK, all from a single account.

EUL holders can vote to liberate assets from the isolation-tier and promote them to the cross-tier or collateral-tier through governance mechanisms. Promoting assets up the tiers increases capital efficiency on Euler because it allows lenders and borrowers to use capital more freely, but it may also expose protocol users to increased risk. It is therefore in EUL holders' interests to balance these concerns.

Lending and Borrowing

When lenders deposit into a liquidity pool on Euler, they receive interest-bearing ERC20 eTokens in return, which can be redeemed for their share of the underlying assets in the pool at any time, as long as there are unborrowed tokens in the pool (similar to Compound's cTokens). Borrowers take liquidity out of a pool and return it with interest. Thus, the total assets in the pool grows through time. In this way, lenders earn interest on the assets they supply, because their eTokens can be redeemed for an increasing amount of the underlying asset over time.

Tokenised Debts

Similarly to Aave's debt tokens, Euler also tokenises debts on the protocol with ERC20-compliant interfaces known as dTokens. The dToken interface allows the construction of positions without needing to interact with underlying assets, and can be used to create derivative products that include debt obligations.

Rather than providing non-standard methods to transfer debts, Euler uses the regular transfer/approve ERC20 methods. However, the permissioning logic is reversed: rather than being able to send tokens to anyone, but requiring approval to take them, dTokens can be taken by anyone, but require approval to accept them. This also prevents users from "burning" their dTokens. For example, the zero address has no way of approving an in-bound transfer of dTokens.

Borrowers pay interest on their loans in terms of the underlying asset. The interest accrued depends on an algorithmically determined interest rate for each asset. A portion of the interest accrued is held in reserves to cover the accumulation of bad debts on the protocol.

Protected Collateral

On Compound and Aave, collateral deposited to the protocol is always made available for lending. Optionally, Euler allows collateral to be deposited, but not made available for lending. Such collateral is 'protected'. It earns a user no interest, but is free from the risks of borrowers defaulting, can always be withdrawn instantly, and helps protect against borrowers using tokens to influence governance decisions (see Maker governance issue (6)) or take short positions.

Defer Liquidity

Normally, an account's liquidity is checked immediately after performing an operation that could fail due to insufficient collateral. For example, taking out a borrow, withdrawing collateral, or exiting a market could cause a transaction to be reverted due to a collateral violation.

However, Euler has a feature that allows users to defer their liquidity checks. Many operations can be performed, and the liquidity is checked only once at the very end. For example, without deferring liquidity checks, a user must first deposit collateral before issuing a borrow. However, if done in the same transaction, deferring the liquidity check will allow the user to do this in any order.

Feeless Flash Loans

Unlike Aave, Euler doesn't have a native concept of flash loans. Instead, users can defer their liquidity check, make an uncollateralised borrow, perform whatever operation they like, and then repay the borrow. This can be used to rebalance positions, build-up complex positions, take advantage of external arbitrage opportunities, and more.

Because Euler only charges fees according to the time value of money, and from the blockchain's perspective flash loans are held for a duration of 0 seconds, they are entirely free on Euler (ignoring gas costs). We believe that flash loan fees are ultimately in a race to the bottom that will be accelerated by advances like flash minting. The ecosystem benefits gained from simple and free flash loans outweigh the relatively modest benefit from flash loan fees.

Risk-adjusted Borrowing Capacity

Like other lending protocols, Euler requires users to ensure that the value of their collateral remains higher than the value of their liabilities (except during the intermediate period when liquidity checks have been deferred). Over-collateralisation is encouraged by limiting how much borrowers can take out as a loan in the first place.

Compound achieves this in a one-sided way by using collateral factors to adjust down the value of a borrower's collateral assets when deciding how much they can borrow. This gives rise to a 'risk-adjusted collateral value' that helps to create a buffer that can be drawn upon by liquidators in the event that the value of a borrower's assets and liabilities changes over time. One of the problems with this approach is that it only adjusts for the risks associated with a borrower's collateral assets decreasing in value. There may be an asymmetric risk, however, of the borrower's liabilities increasing in value. This risk is not factored into the collateral factors.

On Euler, we therefore use a two-sided approach where we also adjust up the market value of a borrower's liabilities to arrive at a 'risk-adjusted liability value'. This approach improves capital efficiency on the protocol because it allows Euler to factor in the asset-specific risks of both downside and upside price movements. These risks are encapsulated in asset-specific collateral factors (as on Compound) and borrow factors (new to Euler). Ultimately, this approach means that the liquidation threshold of every borrower is tailored to the specific risk profiles associated with the assets they are borrowing and using as collateral.

To give an example, suppose a user has $1,000 worth of USDC, and wants to borrow UNI. How much can they borrow? If USDC has a collateral factor of 0.9, and UNI has a borrow factor of 0.7, then a user can borrow up to $1,000 * 0.9 * 0.7 = $630 worth of UNI. At this level of borrowing, the risk-adjusted value of their collateral is $1,000 * 0.9 = $900, and the risk-adjusted value of their liabilities is $630 / 0.7 = $900. If UNI increases in price, then the risk-adjusted value of their liabilities will also increase to >$900, and then they will be eligible for liquidation. The buffer allowing for liquidation is $1,000 - $630 = $370.

Decentralised Price Oracles

To be able to calculate whether a loan is over-collateralised or not, Euler needs to monitor the value of users' assets. On Compound, Maker, and Aave, various systems are used to get prices from off-chain sources and put them on-chain so that they can be accessed by the relevant smart contracts.

This approach is unsuitable for Euler's purposes because it requires centralised intervention whenever a new lending market needs to be created. Euler therefore relies on Uniswap v3's decentralised time-weighted average price (TWAP) oracles to assess the solvency of users (4). The reference asset used to normalise prices on Euler is Wrapped Ether (WETH), which is the most common base pair on Uniswap (5).

TWAP

Uniswap TWAP is calculated using the geometric mean price of an asset over some interval of time. TWAP in general is both a smoothed and lagging indicator of the trade price: a TWAP over a short interval is a less smooth function, but more up-to-date, whilst a TWAP over a long interval is a smoother function, but less up-to-date. TWAP is ideal for Euler's purposes for several reasons.

First, TWAP is resistant to price manipulation attacks. It cannot be manipulated within a transaction or block (for example, with flash loans or flash bots) because it is calculated using historic data. It is also expensive to manipulate using large market orders because the manipulated price must be maintained for some period of time relative to the TWAP time interval. During this time, other users can take advantage of the manipulated price with arbitrage, which will cause it to revert back to the broader market price. Arbitrage is especially practical on the blockchain because arbitrageurs have access to large amounts of capital (including from flash loans) and the atomic nature of transactions means that arbitrage transactions have a low execution risk. For these reasons, manipulating the price on a single decentralised exchange usually requires more widespread manipulation of all on-chain exchanges simultaneously, although even this can't prevent the (less practical but still possible) arbitrage between on and off-chain exchanges.

Second, the smooth nature of TWAP helps to remove the impact of price shocks on borrowers. In the event of a large trade, the current price on Uniswap can be moved significantly. Usually, arbitrage bots will quickly converge this to the broader market value, so the maximum deviation of the TWAP will only be a fraction of the temporary price movement. This prevents some unnecessary liquidations and loans that may quickly become undercollateralised.

Third, instead of instantly jumping between two price levels, TWAPs change continuously, second-by-second. This property is used by Euler's liquidation process to implement Dutch auctions that reduce the value captured by miners and front-running bots.

Time Interval

One of the challenges in using TWAP is determining the right interval over which it should be calculated for a given asset. The trade-offs involved with shorter (longer) intervals may sometimes need to be taken into consideration and altered for specific assets. Euler therefore allows the default time interval to be updated by governance if EUL holders deem it necessary.

Liquidations

A borrower is considered to be in violation on Euler when the value of their risk-adjusted liabilities exceeds the value of their risk-adjusted collateral. A borrower that has just become in violation still has enough collateral to repay their loan, but is adjudged to be at risk of defaulting on their loan. Consequently, they may be liquidated in order to limit the potential for them to default.

MEV-resistance

On Compound and Aave, liquidations are incentivised by offering up a borrower's collateral to liquidators at a fixed percentage discount, which typically ranges between 5-10%. One of the issues with this strategy is that would-be liquidators often have no choice but to engage in priority gas auctions (PGA) for profitable liquidations, which exposes the liquidation bonus as so-called miner extractable value (MEV) (7). Another issue with this approach is that a fixed discount can be punitive for large liquidations, and therefore discourage large borrowers, whilst being insufficient to cover costs and incentivise smaller liquidations.

To remedy these issues, Euler uses a different approach. Rather than a fixed discount percentage, we allow the discount to rise as a function of how under-water a position is. This turns a one-shot opportunity, where liquidators have no option but to engage in a PGA, into a type of Dutch auction. As the discount slowly increases, each would-be liquidator must decide whether or not to bid for a liquidation at the current discount on offer. Liquidator A might be profitable at 4%, but liquidator B might run a more efficient operation and be able to jump in sooner at 3.5%. The Dutch auction is aided by the TWAP oracles used on Euler because a shock to the price does not bring with it a singular point at which every liquidator becomes profitable all at once. Instead, the price moves more smoothly over time leading to a continuum of opportunities to liquidate, which further helps to limit PGAs. Overall, this process should help to drive the discount price towards the marginal operating cost of liquidating a borrower.

However, by itself, this process does not prevent MEV because miners and front-runners can still steal a liquidator's transaction. To limit this form of MEV, we allow liquidity providers on Euler to make themselves eligible for a "discount booster", which allows them to become profitable in the Dutch auction before miners and front-runners (who do not have the booster).

Soft Liquidations

The fraction of a borrower's debt that can be paid off by liquidators in one go is referred to by Compound as the 'close factor.' On both Compound and Aave, the close factor is currently fixed at 0.5, meaning liquidators can pay off up to half a borrower's loan in one go, regardless of how underwater their position is. This approach has a couple of potential drawbacks.

First, allowing liquidators to liquidate half a loan could be considered excessive if a smaller liquidation would have been sufficient to bring the borrower back to health. Larger borrowers are likely to be put off by such a process. Second, a large fixed discount can sometimes drive a borrower closer to insolvency and disincentivise them from repaying their loans (see (8)).

On Euler, we therefore use a dynamic close factor to try to `soft liquidate' borrowers. Specifically, we allow liquidators to repay up to the amount needed to bring a violator back out of violation (plus an additional safety factor). This means that borrowers who are only slightly in violation will often have much less than half their debts repaid during a liquidation, whilst borrowers who are heavily in violation will often have much more than half their debts repaid during a liquidation (their whole position might be closed in some circumstances).

Reserves

In rare circumstances, the value of a borrower's collateral might become less than the value of their liabilities. In this situation, the borrower is said to be 'insolvent.' Insolvent borrowers will typically be liquidated repeatedly until they have little to no collateral left. Any leftover liabilities after liquidations have stopped can be considered 'bad debt' that we can assume will never be repaid. If bad debt accumulates on the protocol, it increases the chance that lenders might all rush at once to withdraw their funds (to avoid becoming the bearer of the bad debt). This phenomenon is known as `run on the bank.'

To reduce this risk, Euler follows Compound by allowing a portion of the interest paid by borrowers in each market to accumulate into a reserve. The idea behind this is to allow the reserves to act as a lender of last resort in the event of a run on the bank. Providing that reserves accumulate at a faster pace than bad debt, lenders do not need to worry about being able to withdraw their funds. Euler reserves operate similar to those on Compound, except that Euler reserves are tracked in eToken units, rather than underlying units, which means that Euler reserves earn interest automatically whereas Compound reserves do not.

The proportion of interest paid into the reserves is called the `reserve factor' and it is a parameter specific to each lending market. There are trade-offs to consider when setting the reserve factor. A reserve factor of zero would mean no reserves accrue, which could stifle lending because of the bad debt issue. Nevertheless, a high reserve factor would mean a large portion of interest is diverted away from lenders, which could also stifle lending as lenders seek a better rate elsewhere. Thus, EUL holders may wish to use governance to select a reserve factor that balances these trade-offs for each type of asset.

Liquidation Surcharge

During a liquidation, the liquidator is required to provide a slightly larger amount of the borrowed asset than is being repaid on behalf of the violator. This extra amount is contributed to the reserves for the borrowed asset as a fee. The base liquidation discount starts at the level of this fee, so it is ultimately paid by the violator.

As a result, more volatile assets, which generally trigger more liquidations, will tend to accrue reserves at a faster pace than less volatile assets, helping to protect lenders of those assets. Additionally, this fee ensures that 'self-liquidating' is always net-negative, which adds a profitability threshold that some undesirable manipulation strategies are unlikely to meet.

Interest Rates

Both Compound and Aave use static linear (or piecewise linear) interest rate models to guide the cost of borrowing on their protocols. Broadly speaking, as demand for borrowing from the pool increases or supply decreases, interest rates go up, and when supply increases or the demand for borrowing decreases, interest rates go down.

Static models work well if they are appropriately parameterised ahead of time, but can be problematic when parametrised incorrectly. For example, if the slope of the static linear function is too shallow, it can lead to the cost of borrowing being underpriced, with lenders unable to withdraw their assets because a pool has become over-utilised. On the other hand, if the slope of the static linear function is too steep, it can lead to the cost of borrowing being too expensive, which can stifle borrowing and lead to low capital efficiency.

Reactive Interest Rates

To avoid the problem of having to choose the right parameters for every lending market, Euler uses control theory to help autonomously guide the cost of borrowing towards a level that maximises capital efficiency on the protocol. Specifically, we use a PID controller to amplify (dampen) the rate of change in interest rates when utilisation is above (below) a target level of utilisation. This gives rise to reactive interest rates that adapt to market conditions for the underlying asset in real-time without the need for ongoing governance intervention. A similar approach has also recently been described by the Delphi Labs team (9).

Compound Interest

Compound interest is accrued on Euler on a per-second basis. This differs from other lending protocols, where interest is typically accrued on a per-block basis. A per-second basis is generally expected to perform more predictably in the long-run, even if upgrades to Ethereum lead to changes in the average time between blocks.

Gas Optimisations

Euler’s smart contracts minimise the amount of storage used, implement a module system to reduce the amount of cross-contract calls, and have had a number of other gas usage optimisations applied. This makes the protocol cheaper on most operations than other lending protocols.

Transaction Builder

The user interface includes a convenient tool to help users batch up multiple transactions and reduce their gas costs, which we call a transaction builder. Advanced users can use this feature in conjunction with a 'defer liquidity checks' option provided on the protocol to rebalance loans or perform flash loans.

Sub-accounts

Asset tiers help to isolate risks on Euler, but they open up a new user-experience problem. Specifically, it would quickly become cumbersome for borrowers to use Euler if they had to send collateral to a new Ethereum account for each new isolation-tier loan they wanted to take out.

Euler therefore enables every Ethereum account using the protocol to access up to 256 sub-accounts (including the primary account), which can be used to cost-effectively manage multiple positions at the same time. A user only needs to approve Euler's access to a token once, and can then deposit into any sub-account. Additionally, no approvals are required to transfer assets and liabilities between sub-accounts, which allows users to isolate and segregate their collateral and debts as desired.

Governance

Euler will broadly follow the governance model pioneered by Compound (10). The protocol will be managed by holders of a protocol native governance token called Euler Governance Token (EUL). EUL tokens will represent voting powers of the protocol software. Holders with enough EUL tokens will be able to make a formal proposal for change on the protocol. Token holders will then be able to vote on the proposal themselves or delegate their vote shares to a third party. Examples of the kinds of decisions token holders might vote on include proposals to alter include:

- The tier of an asset
- Collateral and borrow factors
- Price oracle parameters
- Reactive interest rate model parameters
- Reserve factors
- Governance mechanisms themselves

Acknowledgements

With special thanks to Shaishav Todi, Luke Youngblood, Charlie Noyes, samczsun, Hasu, Dave White, Rick Pardoe, Ayana Aspembitova and the Delphi Labs team, Mariano Conti, Lev Livnev, and Chainguys.

References

1. https://docs.ethhub.io/built-on-ethereum/open-finance/what-is-open-finance/
2. https://compound.finance/documents/Compound.Whitepaper.pdf
3. https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf
4. https://uniswap.org/whitepaper-v3.pdf
5. https://weth.io/
6. https://www.theblockcrypto.com/post/82721/makerdao-issues-warning-after-a-flash-loan-is-used-to-pass-a-governance-vote
7. https://research.paradigm.xyz/MEV
8. https://docsend.com/view/bwiczmy
9. https://members.delphidigital.io/reports/dynamic-interest-rate-model-based-on-control-theory
10. https://medium.com/compound-finance/compound-governance-5531f524cf68