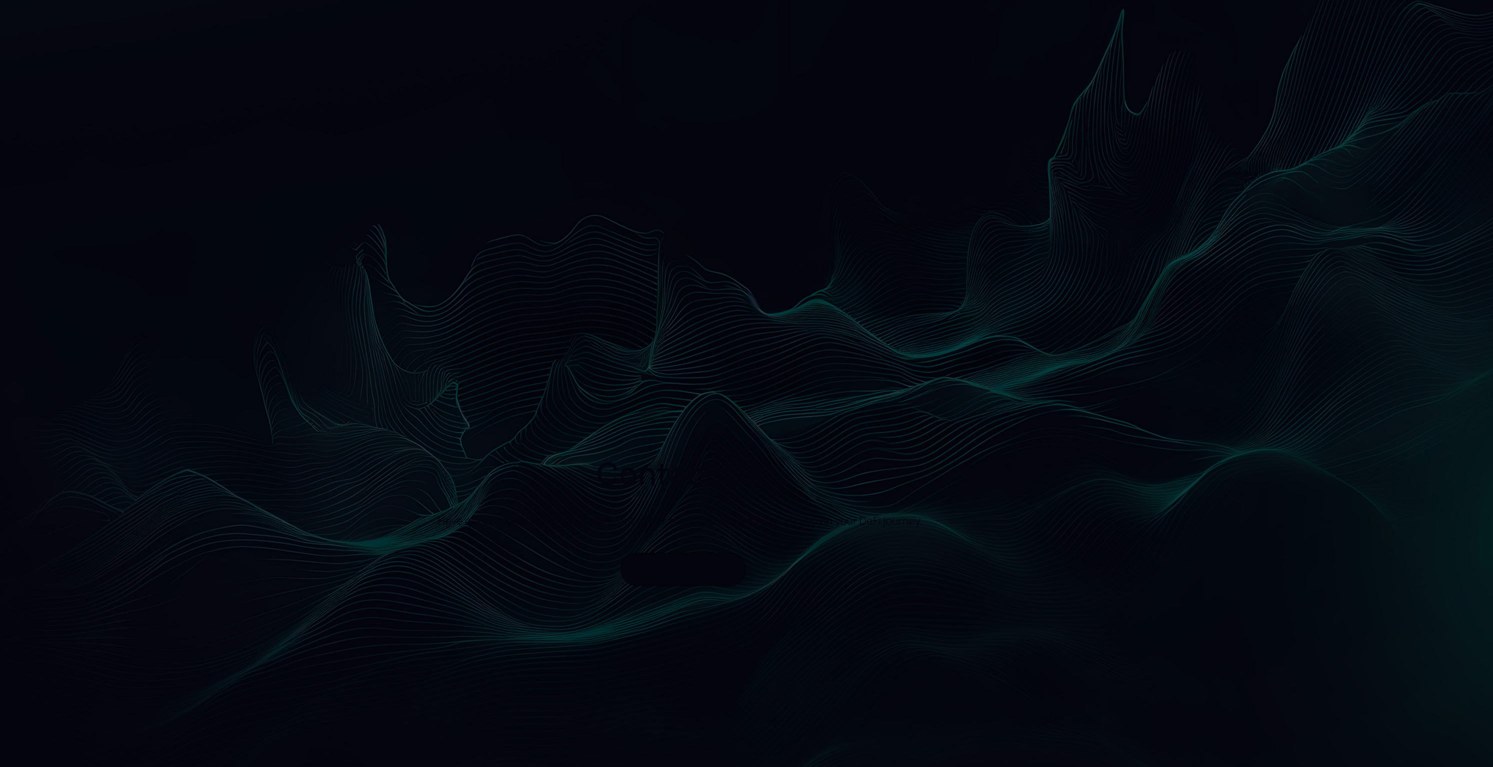
Kredly.ai



KREDLY FOUNDATION

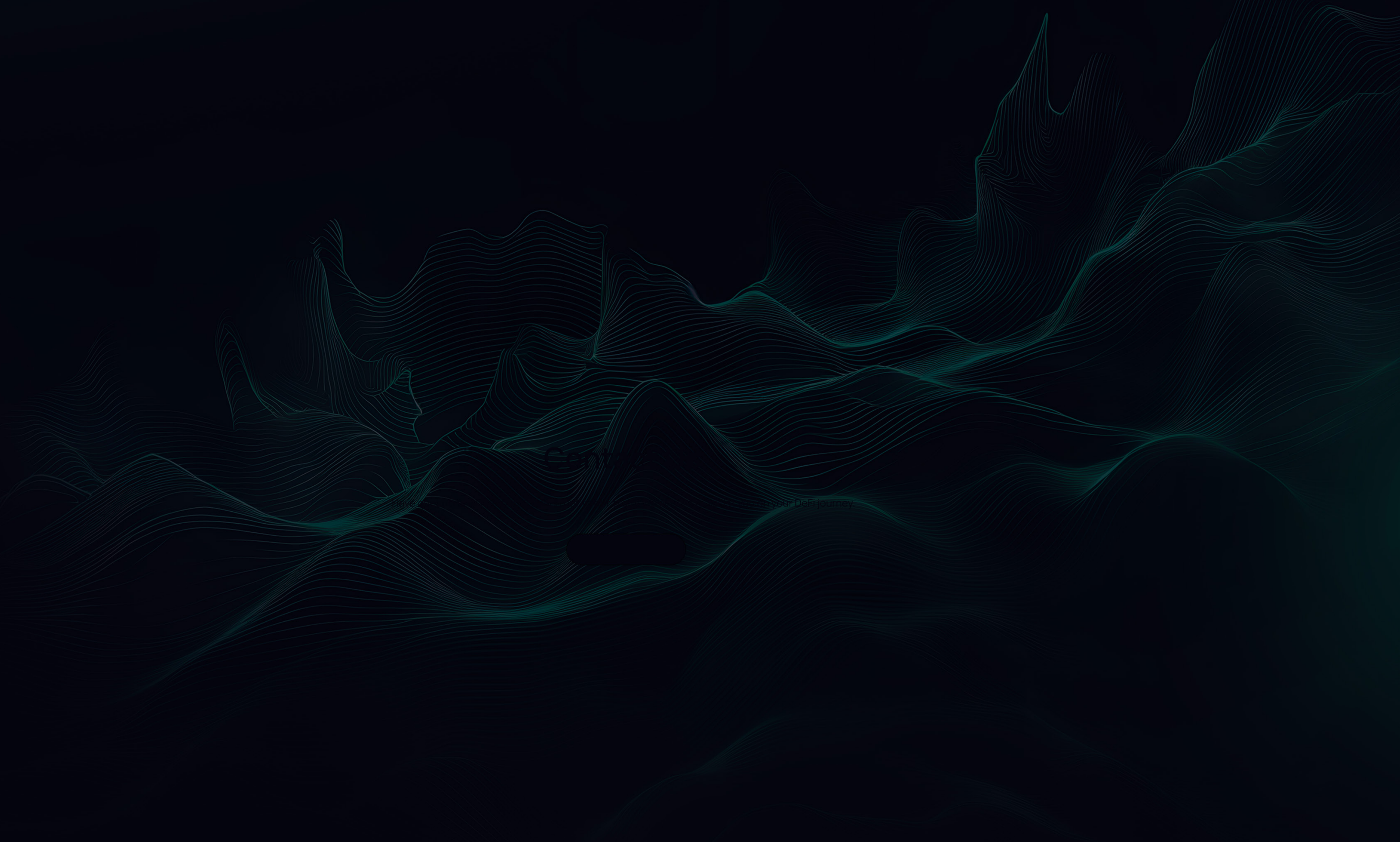
Kredly Foundation

Kredly is a decentralized lending and borrowing platform driven by algorithms, operating atop Mantle infrastructure. It empowers individuals to offer cryptocurrency collateral within the network, which can then be borrowed against by pledging overcollateralized cryptocurrencies. This mechanism establishes a safe lending ecosystem wherein lenders earn compounded annual interest rates (APY) paid per block, while borrowers incur interest charges on the borrowed cryptocurrency.

Drawing from insights garnered from past ventures in borrowing protocols like Compound and AAVE, Kredly prioritizes risk mitigation, decentralization, and user-centric design. Its objective is to introduce a superior product to the market by enhancing security, autonomy, and user experience.

Introduction

The design of Kredly is crafted to facilitate a completely algorithmic money market on Mantle. Leveraging insights from Compound and MakerDAO, the protocol architecture is built upon, integrating essential lessons learned from recent advancements in AAVE.



Problems and Solution

The rise of decentralized finance has catalyzed the creation of a dynamic financial ecosystem directly integrated with blockchains. This new landscape is distinguished by transparency and cryptographic validation through smart contracts. These platforms are fundamentally transforming the structure of monetary markets by obviating the need for central authorities or intermediaries.

In contrast to traditional finance, where users are typically required to establish creditworthiness, demonstrate income, and satisfy various criteria for lenders to make decisions, the decentralized finance space offers a departure from these norms. Even with collateral such as real estate or vehicles, traditional lenders often do not accommodate digital assets and cryptocurrencies for either pledging or acquiring loans. Moreover, opportunities to earn interest rates by providing digital assets to banks and lenders are largely absent from traditional financial systems.

Developing a protocol that facilitates a conventional money market involves establishing pools of assets featuring algorithmically determined interest rates, which fluctuate based on the asset's supply and demand. Through direct interaction with the protocol, both suppliers and borrowers of an asset can engage in transactions, earning and paying a variable interest rate. This eliminates the need for negotiating terms such as maturity, interest rate, or collateral with a peer or counterparty, streamlining the borrowing and lending process within the market.

Case Study

Eva is determined to acquire her ideal home, yet traditional lenders have rejected her loan application. Despite possessing substantial cryptocurrency holdings, she hesitates to sell them due to potential capital gains taxes and missed appreciation opportunities. Nonetheless, her confidence in the long-term potential of cryptocurrencies remains unwavering.

In her quest for funding without liquidating her assets, Eva explores Kredly, a decentralized finance platform operating on Mantle. Opting for an alternative to traditional banking channels, she utilizes available bridges to seamlessly transfer her Bitcoin to the Mantle Network without incurring significant fees. With her Bitcoin now integrated into the Mantle ecosystem, Eva accesses the Kredly Dashboard through her browser to offer her Bitcoin as collateral. This strategic move enables her to capitalize on potential Bitcoin price appreciation while earning a respectable APY on her holdings.

Subsequently, Eva calculates her borrowing requirements and efficiently secures a loan in USDC directly from the dashboard. The protocol evaluates the value of her collateral and grants her an over-collateralized loan, providing immediate access to USDC funds.

Eva promptly converts the USDC to her local fiat currency via her crypto exchange account, allowing her to proceed with the purchase of her dream home while awaiting favorable market conditions. Notably, she is not constrained by monthly payments, and any appreciation in her collateral benefits her. Furthermore, she enjoys the flexibility to make payments at her convenience, with interest rates compounded per block.

Money Markets

- Earn a variable APY by supplying cryptocurrencies and stablecoins, secured by over-collateralized assets, to the protocol.
- Access cryptocurrencies and stablecoins swiftly and without a credit check, directly on Mantle.
- Utilize existing portfolios as collateral to fund new ICO investments for traders.
- Enable traders to short a token by borrowing it, sending it to an exchange, and capitalizing on declines in overvalued tokens.
- Empower dApps to amplify their tools within the ecosystem by borrowing tokens without the need for off-chain behavior or waiting for fulfilled orders.

Supplying Assets

Kredly users are presented with the opportunity to deposit various supported cryptocurrencies or digital assets onto the platform. These deposits serve several functions: they act as collateral for loans, contribute to liquidity for earning an APY, or enable the minting of synthetic stablecoins.

By depositing assets like cryptocurrencies or digital assets into Kredly, users effectively become lenders while ensuring the security of their collateral within the protocol. Users are entitled to earn an interest rate that adjusts according to the utilization of the yield curve in the specific market. All user assets are pooled into smart contracts, allowing for withdrawal at any time, provided the protocol maintains a positive balance.

Users who opt to deposit their cryptocurrency or digital assets into Kredly will receive a KToken, such as KBTC, in exchange. This KToken functions as the exclusive token for redeeming the underlying collateral deposited. Through this mechanism, users can hedge against other assets or transfer them to cold storage wallets compatible with the Mantle Network.

Borrowing Assets

Users interested in borrowing any of the supported cryptocurrencies, stablecoins, or digital assets from Kredly are required to provide collateral, which will be securely locked within the protocol. These assets must exceed the loan amount and can enable borrowing up to a certain percentage of their collateral value. These collateral ratios are established on a token-by-token basis.

Upon depositing assets, borrowing eligibility is contingent upon the collateral ratio of the asset. Typically, collateral ratios vary between 40% and 75%. For example, if Bitcoin has a collateral value of 75%, borrowers can access up to 75% of their BTC value. For a user with $100,000 in BTC supplied to the Kredly protocol, they can borrow up to 75% of that value. However, should a user's collateral value fall below the specified collateral ratio, it may trigger a Liquidation event, details of which will be elaborated later.

Users are subjected to a compound interest rate applied per block on these assets, with no monthly payment obligations. To redeem the collateral, the user must settle their origination balance and compounded interest within the protocol.

Market interest rates are determined by the specific yield curve designated in the contract. Depending on market utilization, the interest rate for the specified market will be determined accordingly.

Risk Management

Kredly strengthens risk management across multiple dimensions by implementing various strategies: it maintains separate pools for securely onboarding long-tail assets, adopts an innovative price feed comprised of multiple oracles to mitigate single points of failure, and employs more advanced risk parameters to enhance the protocol's resilience against insolvency.

Separate Pools

Conventional lending protocols like Compound typically consolidate assets into a single liquidity pool. However, this arrangement exposes the protocol to significant liquidity risks during periods of extreme volatility in any of the included tokens. Furthermore, the absence of specific risk parameters complicates the process of listing new tokens.

To overcome these challenges, Kredly introduces separate pools as a solution. Isolated pools comprise distinct collections of assets with customized risk management configurations, enabling enhanced diversification to manage risks and facilitate lending and borrowing activities. By segregating pools, potential failures are contained, preventing them from impacting unrelated markets and the overall risk profile of the protocol. Additionally, rewards within isolated pools can be tailored for each asset, providing personalized liquidity incentives to users.

Risk Fund and Shortfall Handling

Shortfall accounts, where borrowers have borrowed beyond the value of their collateral, present a significant risk to decentralized lending protocols. When the value of the unlocked collateral falls below that of the loan, borrowers have minimal incentive to repay these loans. Consequently, these accounts strain the protocol's liquidity, and previous protocols lacked mechanisms to address them.

To mitigate this risk, Kredly establishes a risk fund for each pool, with a portion of protocol revenue allocated to cover potential insolvencies. In the event of insolvency following liquidation, a shortfall handling mechanism will be triggered, involving the auctioning of the risk fund for the corresponding asset.

Liquidations

Liquidations play a vital role in risk management within lending protocols such as Kredly, where fluctuations in asset prices can jeopardize protocol liquidity. To mitigate this risk, a liquidation mechanism is implemented.

When an account's collateral drops below a predefined threshold, liquidator bots, motivated by profit, sell a portion of the collateral on the market to repay the borrower's debt. The liquidation threshold varies depending on the quality of the collateral, with more volatile assets necessitating a lower threshold, thus requiring more collateral to secure a position from liquidation.

Upon reviewing past implementations, we identified issues in the liquidation process of some protocols and proactively sought to resolve potential issues. In many cases, underwater positions were not fully liquidated; instead, liquidations occurred incrementally, repaying only a portion of the borrowed amount in each event. This incremental process could lead to inefficient liquidation, where remaining collateral became insufficient to cover gas costs for liquidators, making further liquidation economically unfeasible.

Ensuring adequate liquidator incentives proved challenging. It was often difficult to determine on-chain whether liquidators had sufficient motivation to perform necessary liquidations. Distinguishing actual account insolvency from positions potentially requiring further liquidation to track total bad debt was frequently impractical.

Moreover, liquidation incentives were often not aligned with the quality of the collateral. As a result, liquidators tended to prioritize seizing stable assets over volatile ones, potentially increasing risks for accounts with volatile collateral.

Adjusting collateral factors for specific assets could trigger liquidations, potentially exerting additional selling pressure on the collateral asset and leading to further liquidations.

To tackle these issues and learn from the shortcomings of other protocols, Kredly introduces the following liquidation logic:

- The liquidation threshold is set independently from the collateral factor. For example, setting the collateral factor to zero prevents new borrow positions without impacting the solvency of existing loans. This adjustment also enables users to borrow up to 100% of their borrowing limit without immediate liquidation risk.

- Liquidation incentives can be customized per asset, ensuring better alignment with collateral quality.

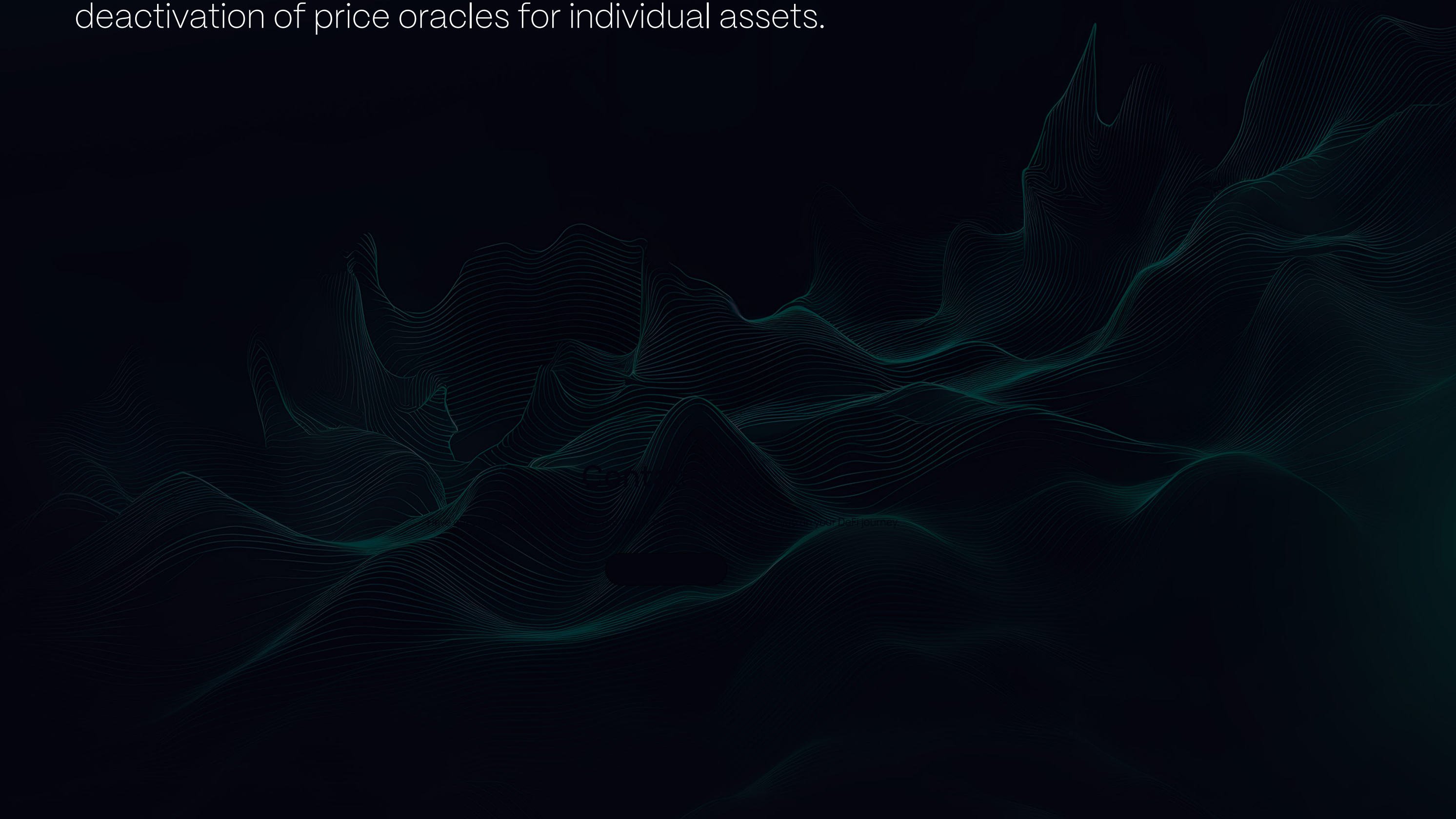
- Two special types of liquidations, batch liquidation and account healing, are introduced to facilitate full position liquidation. Batch liquidations incentivize liquidators to address small accounts, while account healing manages bad debt by allowing liquidators to seize remaining collateral and write off any leftover bad debt.

Redundant Oracle System

Many protocols rely on a single oracle data provider setup, which unfortunately lacks a mechanism to validate prices and guard against price manipulations or stale data. This setup poses an existential threat to the protocol and establishes a single point of failure.

To mitigate these vulnerabilities, Kredly introduces a redundant oracle system capable of fetching prices from multiple feeds and validating them using other decentralized sources. A price validation algorithm is utilized to cross-reference prices obtained from two or more price oracle sources. If a primary source is deemed untrustworthy or fails to provide data, the resilient oracle seamlessly switches to a secondary source.

This advanced oracle system brings additional benefits, including the ability to integrate new price oracles on the fly and support the activation and deactivation of price oracles for individual assets.



Variable Interest Rates

Kredly adopts a distinctive approach to liquidity risk management and utilization optimization while maintaining modularity through the implementation of interest rate models.

The interest rate for each market pair is dynamic and determined based on the ratio of borrowed assets to supplied assets in the market. This ratio is precisely determined by the interest rate model implemented for the pair.

In essence, the interest rate model mitigates liquidity risk by incentivizing users to support liquidity: when capital is abundant, low interest rates encourage borrowing, and when capital is scarce, high interest rates encourage loan repayment and additional deposits. Thus, the interest rate models are functions of utilization; the more of an asset is borrowed, the higher the interest rate will be for it.

Kredly employs variable interest rates for different markets using two models: Linear and Kinked.

Models In Practice

The primary distinction between the models lies in the introduction of a kink in the interest rate curve by the Kinked model when an asset surpasses a certain level of utilization. This adjustment aims to deter borrowers from taking out excessive loans and encourages the repayment of outstanding loans.

For example, if we designate 70% as the optimal utilization rate for an asset, borrowing up to or less than 70% of a pool's reserves will not trigger a kink in the interest rate. The interest rate slope will gradually increase as assets are utilized. However, once more than 70% of the liquidity is borrowed from the reserves, a kink occurs, and the interest rate slope steepens rapidly. This sharp increase in interest rates discourages further borrowing and encourages loan repayment, thereby lowering the pool's utilization rate back towards the optimal level of 70%.

This mechanism is particularly valuable when large amounts of volatile tokens are collateralized, while the other side of the pair consists of more stable tokens such as BTC or ETH. In the event of a significant drop in relative price, the collateral amount may become insufficient to support the loan. By implementing the Kinked model, borrowers now face significantly higher interest rates, compelling them to reduce borrowing or repay the loan.

The optimal utilization rate is initially determined through market simulations and analysis but can be adjusted dynamically in response to significant changes in an asset's economy. This adjustment not only mitigates liquidity risk but also aligns interest rates with periods of high demand.

Linear Model

In the linear model, the interest rates are calculated using simple linear equations. The borrow rate and supply rate are given by the following formulas:
For the borrow rate:

$$\text{borrow \_rate}(u) = a \cdot u + b$$

And for the supply rate:

$$\text{supply \_rate}(u) = \text{borrow \_rate}(u) \cdot u_S \cdot (1 - \text{reserve \_factor})$$

In this model, the borrow rate is a linear function of the utilization rate u, and the supply rate is a function of both the borrow rate and the adjusted utilization rate u_s . The reserve factor represents the part of the interest income that is withdrawn from the protocol and not distributed to suppliers.

Kinked Model

The Kinked model introduces a kink in the interest rate curve when an asset surpasses a certain level of utilization. This adjustment aims to dissuade borrowers from taking out excessive loans and encourages the repayment of outstanding loans.

For the borrow rate, the formula is different depending on whether the utilization rate u is less than or greater than the kink:

If u < kink:

$$\text{borrow \_rate}(u) = a1 \cdot u + b$$

If u > kink:

$$\text{borrow \_rate}(u)=a1 \cdot \text{kink}+a2 \cdot (u-\text{kink})+b$$

And for the supply rate:

$$\text{supply \_rate}(u) = \text{borrow \_rate}(u) \cdot u_s \cdot (1 - \text{reserve \_factor})$$

In this model, the borrow rate is a piecewise function of the utilization rate u, with a kink at the optimal utilization rate. The supply rate is a function of both the borrow rate and the adjusted utilization rate u_s. The reserve factor represents the part of the interest income that is withdrawn from the protocol and not distributed to suppliers.

Artificial Intelligence Enhanced Feeds

Problem Statement:

Price manipulation attacks are increasingly occurring in DeFi due to on-chain data being collected from unverified or disputable resources and it has become crucial to bust these attacks prior to any big losses. To fulfill this AI has to jump into the ground because it holds prediction capabilities by consuming a large set of data which is not applicable on-chain within smart contracts framework.

The primary reason is that smart contracts are not directly connected to off-chain data that is not stored on the blockchain. Due to interacting with off-chain data that can lead to multiple states of the blockchain, it is not allowed to interact with off-chain data. Smart contracts often have small storage. On the other hand, the size of an AI model is much bigger. So at the current stage of development smart contracts cannot run AI models inside, and it is impossible to directly integrate an AI model into a smart contract. AI models provide complex approaches, such as neural networks, and clustering.

Solution Statement:

The adaptive characteristic of AI based on historic data patterns plays an important role in designing a system that enhances the reliability of oracle data for lending protocols, particularly through the integration of AI for monitoring and analysis, involving multiple layers of architecture and technology. This system aims to utilize AI to detect anomalies, monitor market trends, perform cross-references on data from multiple sources, and potentially identify discrepancies or manipulation and adapt to changing market conditions.

It's a sophisticated task that requires a mix of on-chain and off-chain components due to the computational intensity of AI processes and the need for access to broad data sources. Let's outline a conceptual architecture and a basic implementation framework for this system:

System Architecture Overview

1. Off-chain AI Analytics Engine:

Purpose: Analyze data from multiple sources first off-chain and then on-chain, perform market trend analysis and further cross-references to detect anomalies. Implementation: Python scripts utilizing AI/ML (e.g. DAD: Deep Abnormality Detection, Isolation Forest or SVM).

Data Sources: on-chain, off-chain, historic data

2. On-chain Smart Contracts:

Purpose: To interact with the off-chain AI analytics engine, receive final trustable feed, and use this data to make lending decisions or adjust protocol parameters.

Implementation: Receive verified AI-analyzed results through Mantle.xyz or directly from a custom oracle built to interface with the AI engine.

3. Custom Oracle for AI-Analyzed Data:

Purpose: To serve as a bridge between the off-chain AI analytics engine and the on-chain smart contracts.

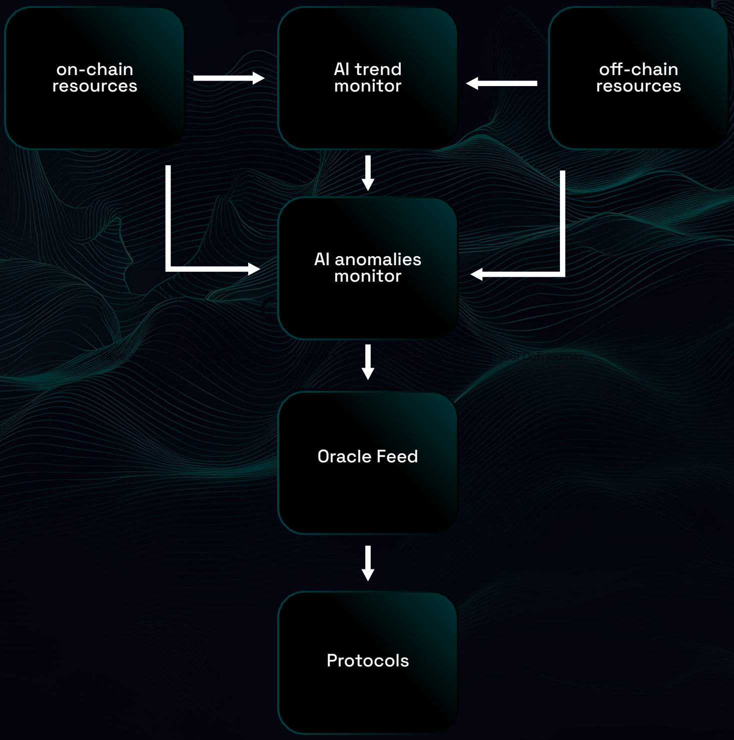
Implementation: A set of smart contracts that validate and relay the Analyzed data back to the requesting contracts on-chain as an API.

4. Data Verification Layer:

Purpose: To interact with the off-chain AI analytics engine, receive final trustable feed, and use this data to make lending decisions or adjust protocol parameters.

Implementation: Receive verified AI-analyzed results through Mantle.xyz or directly from a custom oracle built to interface with the AI engine.

The graphical presentation demonstrates how data flows from diverse unverified resources through AI models towards smart contracts:


on-chain resources
AI trend monitor
off-chain resources
AI anomalies monitor
Oracle Feed
Protocols