zkLend Whitepaper v1.0

zkLend

Inspired by tradition and innovation to build the next generation of finance

7 April 2022

ABSTRACT

zkLend is an L2 money-market protocol built on StarkNet which combines zk-rollup scalability with Ethereum's security, enabling participants to efficiently earn interest on deposits and seamlessly borrow assets. The protocol offers a dual solution: a permissioned and compliance-focused solution for institutional clients, and a permissionless service for DeFi users - all without sacrificing decentralisation.

CONTENTS

Purpose

The purpose of this document is to outline the technical and financial components of zkLend, a money-market protocol built on StarkNet, using StarkWare's zk-rollup technology. The implementation of zkLend will be made available to public in various phases, hence this document is not intended to define exhaustively the scope of the protocol at launch, where this document will be updated from time to time during the developmental phases.

[Remaining page is intentionally left blank]

1 Introduction

1.1 Ethereum's Security

Fundamentally two observations have been made since 2021's 'DeFi Summer' and 'NFT Mania'. DeFi summer saw the explosion of various L1 and L2 chains in response to the Ethereum scalability question. Declining Ethereum dominance can be observed as DeFi total value locked from 97% at the start of 2021 to 63% in Jan 2022. The introduction of alternative L1 and L2 chains which filled a growing demand for blockchain infrastructure capable of delivering cost and speed Ethereum could not meet.

Many of these solutions captured Ethereum TVL as they offered a faster, cheaper alternative to paying high Ethereum gas fees and constant network congestion, both of them fundamental barriers to reach mass adoption and scalability.

However, these chains fundamentally sacrifice decentralisation and security for speed and scalability.

Chain	Average Cost / Txn ($) [1]	Average Blocktime (s)	Nodes / Validators	Validator Requirements	Public Sale Allocation (%)
Ethereum	32.64	13.34	5,398	4CORE / 16RAM / 500 GB	80.00
Avalanche	0.000025	2.02	1,196	8CORE / 16RAM / 200 GB / 2000AVAX	9.97
Polygon	0.00000096	2.22	66	8CORE / 16RAM / 1.5 TB / Whitelist	19.00
FTM	0.00000034	0.89	65	4CORE / 8RAM / 2TB / 500,000 FTM	1.57
BSC	0.0000054	3.05	21	16CORE / 64RAM/ 2TB / 10,000BNB	50.00

Fig1. Comparison of various metrics for various chains. Figures derived base on public data available.

- *Average Cost:*
  The average cost of gas for each transaction, converted from gwei to native currency token and converted to USD. Ethereum is more expensive than its peers.

- *Average Block Time:*
  The average time to complete a block. Ethereum is slower than its peers.

[1]Using monthly average transaction data from 1-29 December 2021, and prices as of 29 December 2021.
Sources: Etherscan, Snowtrace, PolygonScan, FTMScan.

- *Nodes / Validators:*
  The number of nodes and validators for each chain. Higher number implies a higher level of *fault security* and a lower likelihood that all nodes will fail at the same time. Higher numbers also imply greater *attack security*: it is more costly for malicious attackers to attack the nodes. Ethereum has more nodes than its peers.

- *Validator Requirements:*
  The hardware and staking requirements to participate in the consensus of the blockchain. Therefore, it indicates the barrier of entry to validating in the consensus mechanism. In theory, lower validator requirements imply a higher level of *collusion security.* This means that it is harder for insiders to act in selfish ways against the greater good of the system to benefit themselves as it is easier to become a validator in the system. Ethereum has the lowest validator requirements.

- *Public Sale Allocation:*
  The allocation of initial token sale reserved for public sale. In proof of stake blockchains, native tokens are staked to secure consensus, even used for blockchain governance. Higher public token sale indicates lower concentration of power for the underlying blockchain, implying a higher collusion security as initially it would be hard to coordinate malicious actions from a bigger number of actors. Ethereum has the highest public sale allocation.

1.2 The Next Institutional DeFi Frontier

Secondly, it is clear that although 2021 was a landmark year for DeFi adoption - DeFi market cap is still a drop compared to the market cap and legacy infrastructure of TradFi. For example, total DeFi market cap amounts to only $145B, compared to total global equities market cap of over $100T. If only as little as 1% of assets under management from the world's 100 biggest banks were invested within DeFi, it would amount to $1T of capital into the industry.

There is huge potential as TradFi players are starting to enter the DeFi arena. Already, Chainanalysis reports that 60% of DeFi transactions are made by 'large institutions', defined as transactions greater than $10M. Across the chasm from TradFi, DeFi offers lucrative yields. For example, yields on stables can be around 2-10%, and even higher for more 'degenerate' high risk opportunities that can see APYs in the thousands.

Meanwhile institutional literacy in DeFi is increasing: this year it was reported that around 30% of all crypto hedge funds use DEXes (Uniswap being the preferred choice), and Societe Generale took out a $20M in DAI using a tokenised bond as collateral.

There are two fundamental thesis:

1. Ethereum is unrivalled in terms of security and decentralisation.
2. There is a huge opportunity in institutional DeFi.

2 zkLend Protocol

zkLend is a money-market protocol built on StarkNet,[2] combining zk-rollup scalability, superior transaction speed, and cost-savings with Ethereum's security. At its core, zkLend offers a dual suite of permissioned compliance focused solutions for institutional clients ("**Apollo**") and a permissionless service for DeFi users ("**Artemis**").

At a high level, Artemis enables users to deposit assets to earn a yield, while utilising some of these assets as collateral to borrow. Apollo functions similarly but is only open to permissioned users that go through a KYC/KYB process approved by the protocol. As a result, the two protocols will function independently with separate capital pools and governance.

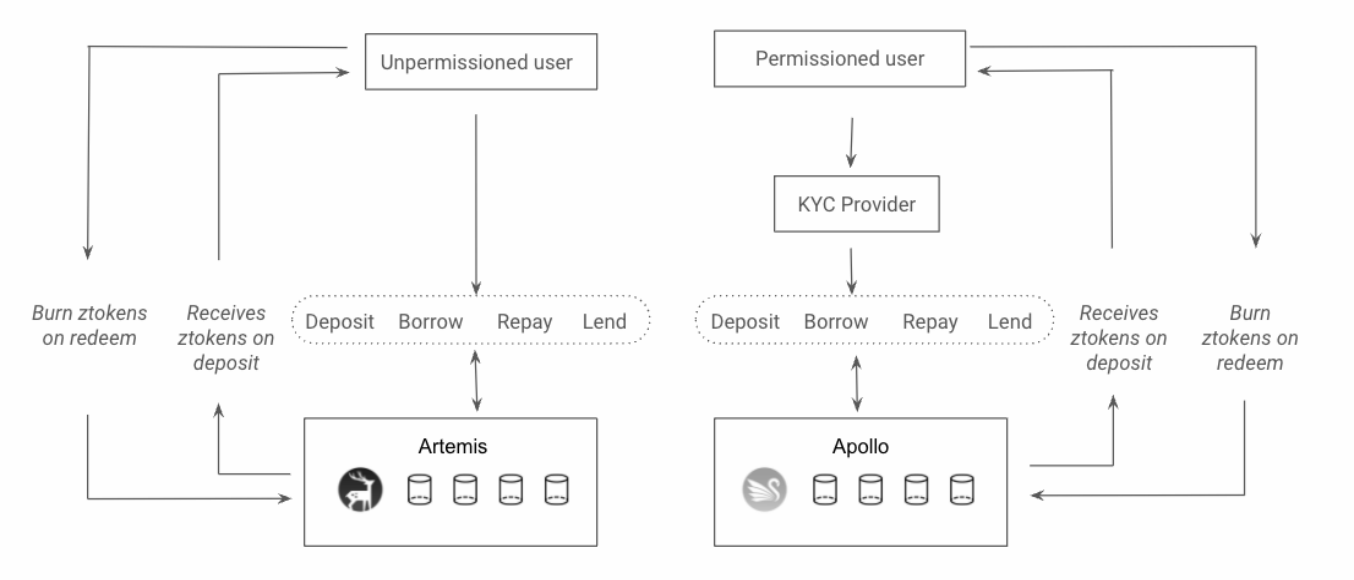


Fig2. High level overview of zkLend.

2.1 Artemis

2.1.1 Lend

Users will be able to deposit their assets into a reserve pool, thereby providing liquidity to each money market. In return, users will get interest-bearing zTokens which represent their deposited share of the pool in addition to a claim on interest earned from the pool. The total assets in the pool grows over time from interest earned from borrowing, where the interest earned will depend on the interest rate model of each asset. Users can deposit any amount into the pool with no lock up period.

[2] For more information, please refer to https://starkware.co/starknet/.

2.1.2 Borrow

Users will be able to borrow assets deposited into various money markets using their zTokens as collateral. The borrowers' financing rate for each asset will depend on the interest rate model (more details in Section 3.2), which is a function of market demand and liquidity pool utilisation. Maximum borrowing amount is determined by users' borrowing capacity. If the users' total loan exceeds their borrowing capacity, their position may be liquidated to protect the protocol against systemic risk.

2.1.3 Tokenised Debt

zkLend tokenises debt on the protocol with ERC20-compliant zTokens. Upon deposit, the depositor receives a corresponding amount of zTokens that maps the prevailing exchange rate relative to the underlying asset(s). The depositor receives a fixed number of zTokens with a floating exchange rate to the underlying asset that reflects interest accrued overtime. The zTokens represent claims on the deposit pools as well as a form of collateral determining borrowing capacities. In future iterations of the protocol, zTokens can be used in derivative product construction, such as debt obligations and credit swaps.

2.1.4 Flash Loans

Borrowers will be able to leverage reserve pool liquidity without any collateral to exploit arbitrage opportunities in the market as the loan is paid back within the same block. Borrowers will pay a fee for their flash loan with the proceeds distributed evenly back to all liquidity providers of the pool they borrowed from. This feature will also be made available to institutional users through the Apollo protocol (where applicable).

2.1.5 Assets Tiers

High risk assets will be monitored more closely in case of price downturns to isolate market risk of these assets. Assets with similar risk characteristics may be segregated into separate categories with similar collateralisation ratios and interest rate curves. In addition, assets with high volatility may be restricted from being used as collateral, but only available for lending and borrowing. The protocol will review the assets periodically to determine whether they can move to become collateral.

zkLend classifies assets into three tiers, details of which have been shown in the below table:

	Category A	**Category B**	**Category C**
Price Volatility	Low	Medium	High
Lending	Yes	Yes	Yes
Borrowing	Yes	Yes	Yes
Pledged as Collaterals	Yes	Yes from restricted pools	No
Interaction with zkLend	Assets can be borrowed, lent and pledged as collateral.	Assets can be borrowed, lent, and pledged as collateral.	Assets only available for lending and borrowing, but not available to be

	Lenders with Category A assets as collaterals can borrow from Category A, B and C pools.	Lenders with Category B assets as collaterals can only borrow from Category A and B pools.	pledged as collateral.

Fig3. Asset tiering and attributes.

2.2 Apollo

2.2.1 Whitelisting Layer and Whitelisters

The whitelisting layer ensures that only permissioned participants will be able to deposit and borrow from reserve pools. The whitelisting process typically includes legal compliance checks (KYC, KYB, AML and CFT), administrative onboarding procedures (understanding terms and conditions, fiat-to-crypto on ramping, due diligence) and technical procedures (providing permissions for the selected Ethereum wallet addresses).

Whitelisters will be responsible for the whitelisting process, separate from zkLend, with the necessary authorisation to duly conduct compliance checks, maintain relevant records and deploy standards required for permissioned users' participation specific for each Apollo market deployment.

zkLend will decide on the regulator-approved and/or licensed whitelisters in the implementation of Apollo markets. However there are several factors considered in determining whitelister suitability, such as (but not limited to):

- Whether they employ KYC, KYB and compliance standards in accordance, or to the same degree as FATF / local jurisdiction guidelines to identify and accept their users;
- Robustness of their AML / CFT programs (if any); and
- Reputation (licensed or otherwise) in their selected jurisdiction.

Further details of responsibilities and duties of whitelisters and zkLend protocol will be built out as Apollo is developed to ensure further risk control, adequate compliance standards, and oversight are implemented. zkLend will work closely with financial and legal advisors.

2.2.2 Institutional Onboarding

The institutional onboarding process comprises both on-chain and off-chain components. The off-chain component consists of working with regulator approved and/or industry recognized service providers for background and reference checks. The on-chain component includes cooperating with service providers on blockchain to handle whitelisting and custodian services.

Apollo will offer a 'high touch' and high client engagement approach. Dedicated institution and compliance team will engage with institutions to understand their product needs and compliance requirements prior to onboarding, provide onboarding guidance and liaise with various KYC/KYB service providers, custodians and whitesliters to streamline the process.

2.2.3 Deposit / Lend

Whitelisted participants will be able to deposit their assets into each pool, thereby adding liquidity to each money market. Counterparties in the pools are whitelisted. In return, participants will receive corresponding zTokens representing their deposited share of the pool in addition to any interest earned from the pool. There is no lockup on assets deposited and any amount can be deposited into the pool. The interest earned will depend on the interest rate model of each specific asset. The scope of assets supported will be more limited than Artemis with an emphasis on short-tailed assets.

2.2.4 Borrow

Institutional participants will be able to borrow in markets against other whitelisted addresses. Borrow rates will be determined by asset specific interest rate curves. Institutional participants will similarly have a borrowing capacity based on zToken balance and each asset collateral ratio.

If the participants' total borrow exceeds their borrowing capacity, their position may be liquidated as a risk control management procedure to protect the protocol against systemic risk.

Institutional users will also be able to access Apollo's flash loans.

2.3 Artemis and Apollo Comparison

	Artemis	**Apollo**
Description	Permissionless money market protocol	Permissioned money market protocol
Target Users	DeFi users Anyone with an internet connection	Institutions, SMEs, Family Offices, Hedge Funds, etc. Compliance-conscious entities
Asset Types	More, Long tail	Fewer, Basic
KYC / Whitelisting Layer	N	Y
Interest Rate Model	Dynamic	Dynamic & Fixed
Ouroboros Model[3]	Y	N
Flash Loans	Y	Y (where applicable)
Variable Liquidation Fees	Y	Y
Under-collateralised Loans	**N**	**Y (later iteration)**

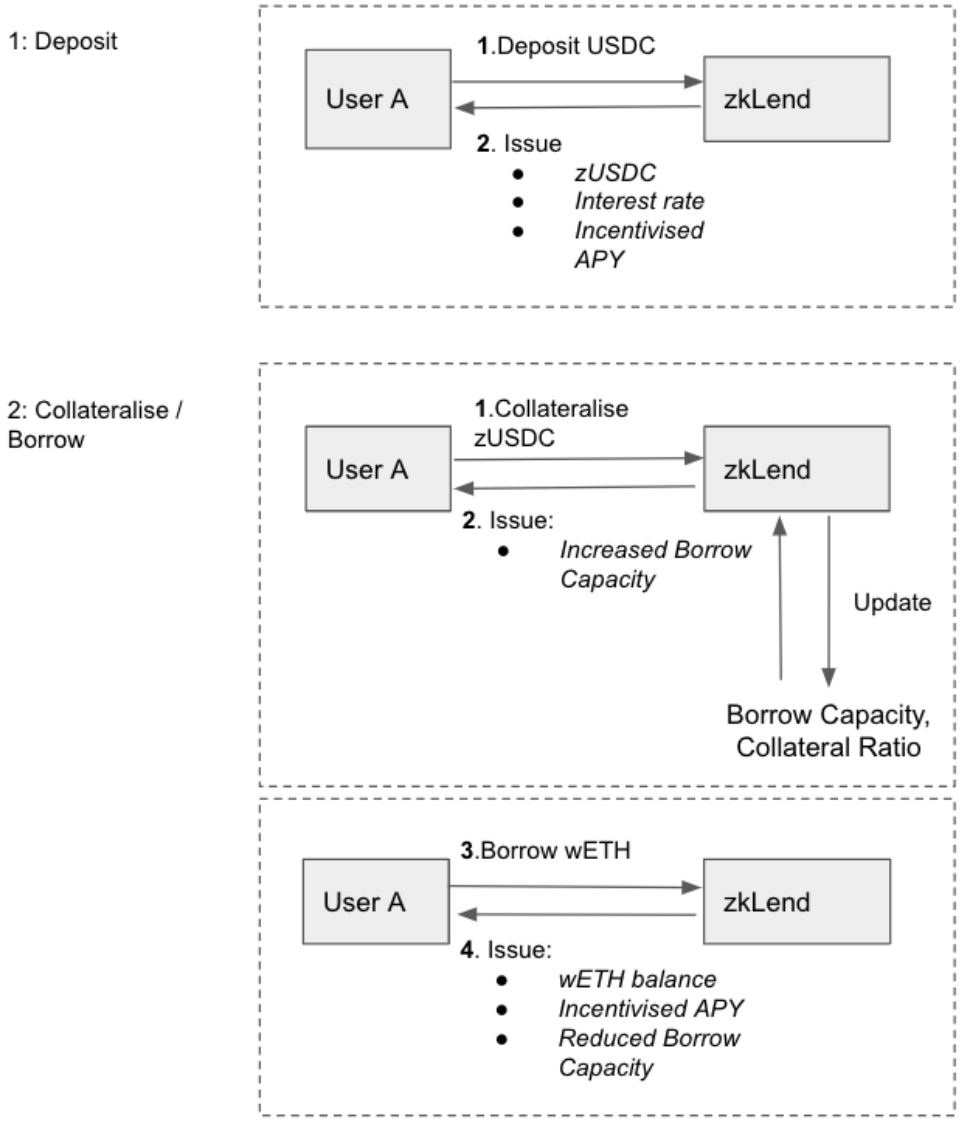
Fig4. Comparison of Artemis and Apollo by product feature.

[3] Ouroboros model focuses on rewarding borrowing activities in the market pools with the highest fee generated, where a portion of the revenue generated will be used towards funding rewards for token holders to create a circular incentive of fees generated to fund further borrowing pools with the next highest revenue generation capability.

3 Architecture & Implementation

3.1 zToken

zTokens are minted when users deposit assets in any market. Minted zTokens represent ownership to an underlying pool. As the pool accrues interest, the zToken entitles holders to an increasing amount of the underlying asset upon redemption. zTokens are redeemed when the user would like to withdraw their funds from the pool.



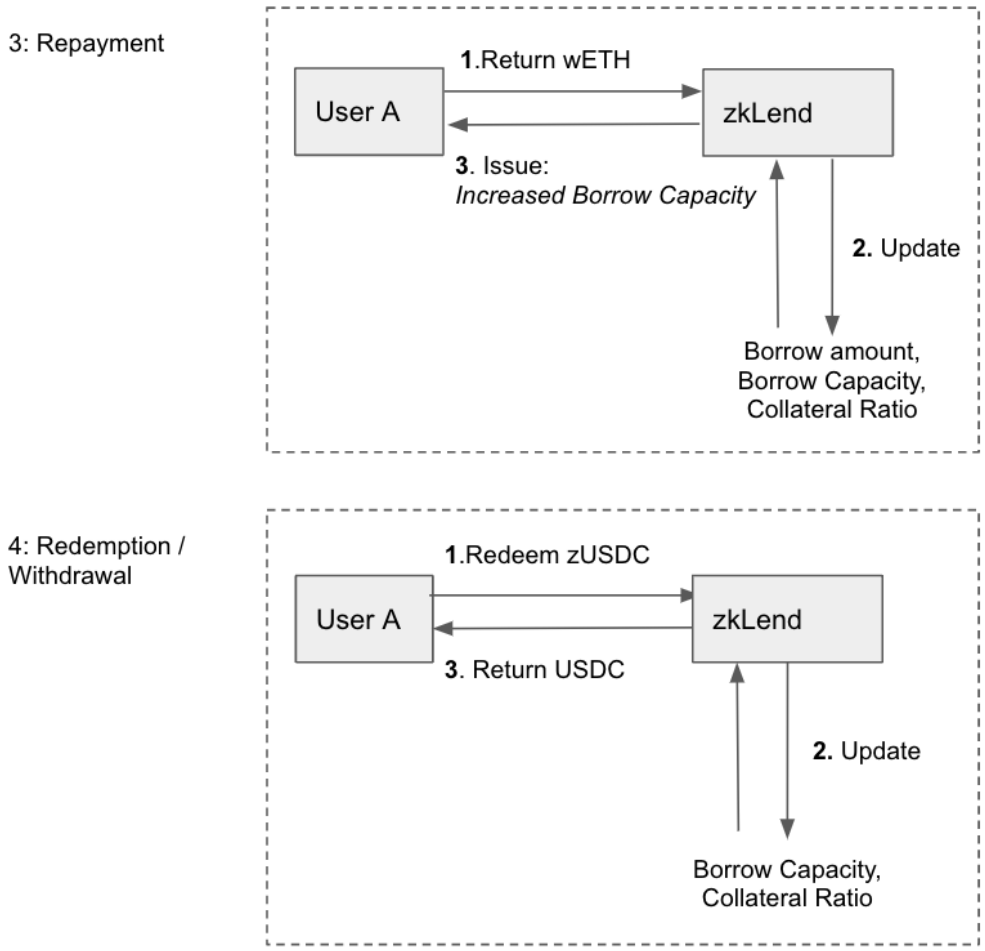


Fig5. Example of zToken lifecycle within the protocol, using zUSDC as collateral to borrow wETH.

1: Deposit

1. User deposits asset (USDC) into the zkLend protocol
    a. Deposit rate will vary based on the asset's interest rate model and will include any additional incentives for each pool
2. zToken is minted with the value of equivalent of asset (zUSDC) with associated interest and incentivised pool APY

2: Collateralise / Borrow

1. User adds his/her zTokens (zUSDC) as collateral
2. zkLend increases the users' borrowing capacity
3. User borrows asset (wETH) from the zkLend protocol
    a. Borrow rate will vary depending on the interest rate model and any additional incentives for each pool
4. zkLend issues wETH for the user
    a. Users' borrowing capacity will be updated (reduced) upon issuance

3: Repayment

1. User returns asset owed (wETH) on zkLend
2. zkLend updates:
    a. Record of asset borrowed, and
    b. Borrowing capacity (increased)

4: Redemption / Withdrawal

1. User will choose the withdraw feature and select any amount up to the maximum allowed in account (depending if the user has an outstanding borrowing position)
2. zkLend will calculate new borrowing capacity of user*
3. USDC corresponding to zUSDC exchange rate will be released

**Upon withdrawal, if the users' new borrowing capacity falls under the borrowed asset's collateral ratio, the user's deposits may be auctioned to liquidators to facilitate rebalancing*

3.2 Interest Rate Model

The interest rate model determines the interest and lending rate for each money market on the protocols. Artemis offers a dynamic interest rate model. Apollo may offer both a dynamic and fixed interest rate model, subject to further development.

For the dynamic interest rate model, each asset market has a separate interest rate curve based on the market's utilisation rate. The utilisation rate is calculated as:

$$U_x(Utilisation\ rate\ of\ market\ 'x') = Borrowings_x \div (Cash_x + Borrowings_x)$$

In the initial (or data gathering) phase, the interest rate model will follow a simple two-sloped model where optimal utilisation will be assessed and readjusted periodically to best reflect actual market utilisation. The utilisation rate of each pool is a function of the current loaned amount and the liquid positions available to loan out, and this number will be refreshed intraday. Lender and borrower participation will help to provide data points in assessing the best representation of the elastic demand.

The utilisation rate of each asset pool will have a specific optimal utilisation rate (U_o). The interest rate model has two slopes - under U_o, the interest rate curve will follow the optimal slope (Slope 1 or 'S1'). Should pool utilisation rate be greater than U_o, the interest rate curve will sharply increase (Slope 2 or 'S2').

$$Rt = Ro + S1 \cdot \frac{Ut}{Uo} \qquad \textit{(for Ut < Uo)}$$

$$Rt = Ro + S1 + S2 \cdot \frac{(Ut - Uo)}{(1 - Uo)} \qquad \textit{(for Ut >=Uo)}$$

where

$Rt = borrowing\ rate\ at\ Ut$

$Ro = base\ rate$

$S1 = slope\ for\ Ut < Uo$

$S2 = slope\ for\ Ut > Uo$

$Ut = current\ utilisation$
$Uo = optimal\ utilisation$

Example Interest Rate Curve Parameters

Asset	***Uo (%)***	***Ro (%)***	**S1**	**S2**
USDC	[90]%	[0]%	[4]%	[60]%
USDT	[90]%	[0]%	[4]%	[60]%
DAI	[80]%	[0]%	[4]%	[75]%
ETH/wETH	[65]%	[0]%	[8]%	[100]%
wBTC	[65]%	[0]%	[7]%	[100]%

Fig6. Example interest rate curves.[4]

The point at which the two slopes intersect at U_o represents a discontinuity, or a 'kink'. In order to accurately incentivise supply and demand of liquidity, zkLend will move from the two-sloped interest rate to the following dynamic interest rate model in subsequent iterations once there is working data in relation to the functions on interest rates versus utilisation rates:

$$I_{Ut} = \alpha e^{Ut} + c$$

where
I_t = Interest rate at given utilisation ratio (Ut)
α = Interest rate curve coefficient
c = minimum interest rate at zero utilisation ratio

t A utilisation ratio above a prescribed market equilibrium would result in a higher financing and deposit rate. This is especially useful in managing long-tail asset liquidity pools, where the optimal utilisation ratio (and the respective curves' coefficients) would also take into account risk of increased borrowing against long-tailed assets as collaterals.

To determine coefficients *α* and *c*, the protocol will leverage a regression model based on historical liquidity supply and demand data (from data gathering phase) to determine the most representative model for each asset market. For example, the borrowing curve of short-tail assets would likely have a lower incline which will closely resemble a linear curve. For long-tailed assets, the interest rate curve will be steeper and due to the accelerating degree of risk at higher utilisation of the pool.

[4] Interest rate parameters to be adjusted and refined prior to launch of testnet and subsequently reviewed periodically.

3.3 Deposit APY

Deposit APY is a function of the total interest earned by each pool's liquidity providers, represented by zTokens, excluding a share which will be reserved for the ecosystem. It is calculated the following way:

$$D_t = U_t\,(S\,B_t \bullet S_t + V\,B_t \bullet V_t) \bullet (1 - R_t)$$

where

D_t = *Deposit APY*
U_t = *Utilisation Rate*
$S\,B_t$ = *Weight in Stable Borrowing*[5]
S_t = *Stable Borrowing Rate*[5]
$V\,B_t$ = *Weight in Variable Borrowing*
V_t = *Variable Borrowing Rate*
R_t = *Asset-specific Reserve Ratio*

3.4 Borrowing Capacity

Specific borrowable amounts, the users' borrowing capacity, will vary according to the asset tiers of the users' deposits and the borrowing asset's collateral requirements (loan-to-value ratio). The collateral value represents how much can be borrowed against the deposited amount for each market. In general, more volatile, small cap assets will have lower collateral value as they will not be considered the best collateral - and vice versa for more stable, large cap assets. A users' borrowing capacity is calculated as:

$$\textit{Borrowing Capacity} = \Sigma(\textit{Value of underlying Token Balance}) \times \textit{Collateral Factor}$$

zkLend utilises two-way collateralisation approach to refine risk management: (1) collateral will be subject to "Collateral Factor" which governs the maximum loan-to-value users may be able to borrow against the particular pledged assets, and (2) the borrowing will also be subject to 'Borrow Factor' which dictates the maximum limit at which users may be able to borrow such target asset.

The protocol also will build in a specific "Reserve Ratio", such that a predetermined percentage of the revenue generated from the asset pool will go towards the safety module in the event of a liquidity shortfall.

Assets	**Can be used as collateral**	**Collateral Factor**	**Borrow Factor**	**Reserve Ratio**
USDC	Y	[85]%	[95]%	[15]%
USDT	N	[0]%	[70]%	[15]%
DAI	Y	[85]%	[95]%	[15]%
ETH/WETH	Y	[85]%	[95]%	[15]%
WBTC	Y	[75]%	[85]%	[15]%

[5] Apollo intends to over stable rate borrowings to institutional users in the subsequent developmental iterations.

3.5 Liquidation

A borrower whose outstanding loan exceeds his/her borrowing capacity will be liquidated at market rate. Instead of a static close factor, zkLend will implement a variable close factor where liquidators can only repay the portion of loan position that has exceeded the borrowing capacity. While the liquidation threshold for each borrower varies on his/her assets pledged as well as the borrowing asset, liquidations happen when the underlying collateral decreases in value relative to the borrowed asset and/or if the outstanding loan value (asset value + accrued interest) now exceeds the borrowing capacity. Examples may include large price increases in a borrowed asset, or dramatic price decrease in the underlying collateral.

Upon reaching liquidation threshold, any StarkNet address will be able to call the liquidation contract as long as they hold the right collateral type and sufficient amount to cover the portion of the borrowers' loan position that is underwater and enough to cover transaction fees. Liquidators can keep calling the liquidation contract until the users' loan position falls back under their borrowing capacity. This ensures an open, frictionless yet efficient way to ensure the protocol risk is managed.

3.6 Price Oracle

The price oracle fetches off-chain data for the protocol such as token prices to enable the calculation of collateral ratios for each market and any necessary liquidations should positions fluctuate beyond a users' borrowing capacity.

The protocol will aim to integrate in-house and decentralised oracles providers like Chainlink. Oracle pricing information will be verified with TWAP Uniswap V3 Oracle data. TWAP time range will also be designed and adjusted to filter out potential price manipulation (i.e. from flash loans). As the StarkNet ecosystem becomes more mature, zkLend may look to take in a wider variety of decentralised oracles to further pricing reliability.

3.7 ZEND Token

The native cryptographically-secured fungible protocol token of zkLend (ticker symbol **ZEND**) is a transferable representation of attributed governance and utility functions specified in the protocol/code of zkLend, and which is designed to be used solely as an interoperable utility token. ZEND will be an ERC-20 token, a standard interface for fungible (interchangeable) tokens on Ethereum.

ZEND tokens holders will be entitled to certain rewards and incentives by engaging with the protocol on the below forms of 'Active Participant Incentives':

1. A portion of the protocol's borrowing fees (revenue) would be allocated to users as rewards to encourage them to interact within the network, for example borrowing/lending activities, providing protocol liquidity, community events, or participation in marketing/airdrop campaigns.

2. Approximately [20]% of such protocol's operating profit will be allocated to governance treasury directed for specific asset markets (as and when needed) to fund the incentives as highlighted above, with another [5]% will be redirected to the treasury for the safety module[6].

   (Please refer to "Appendix - Representations of ZEND Tokens" for more details.)

3.8 Technical Architecture Summary

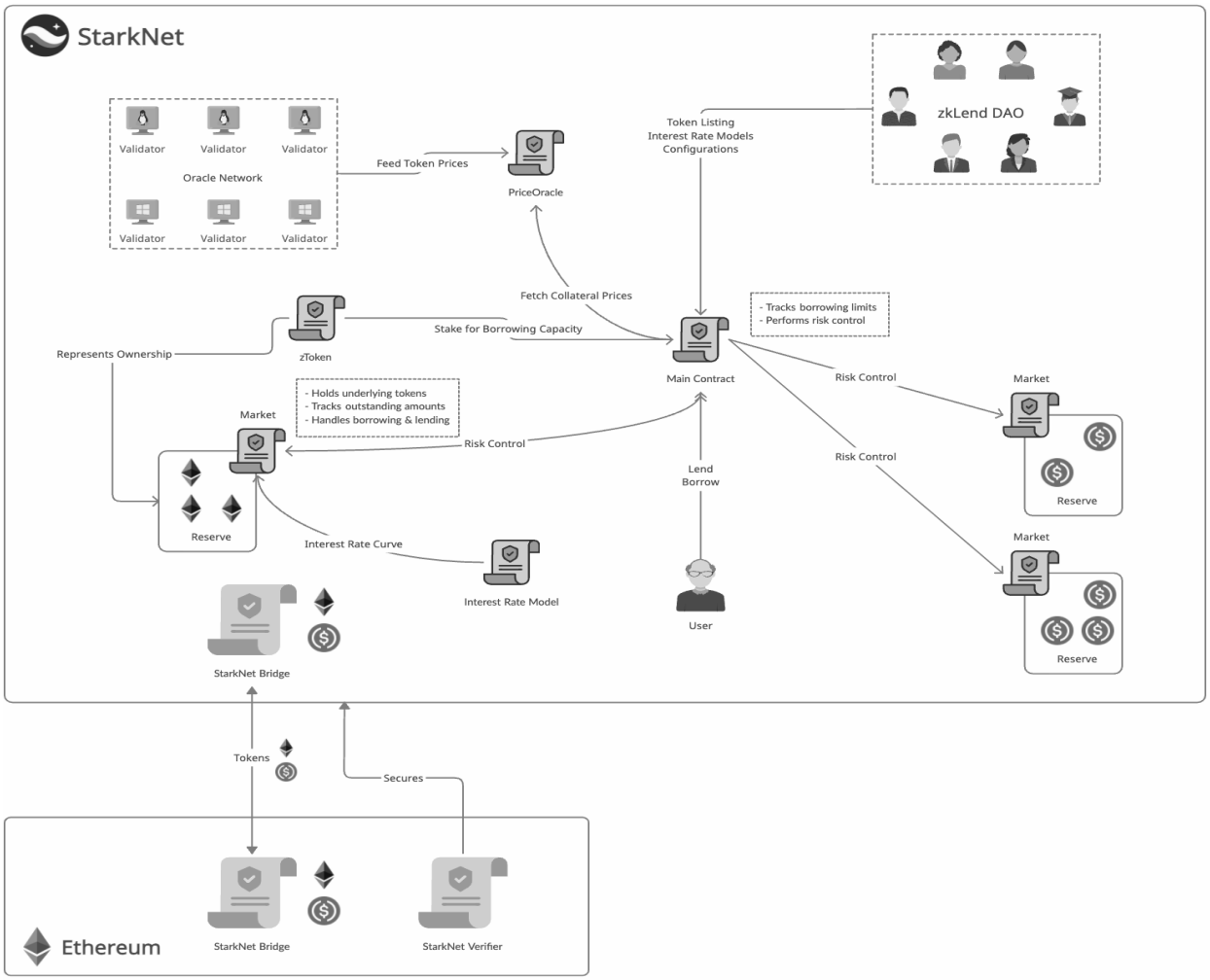


Fig8. zkLend architecture built on StarkNet, using Ethereum for settlement.

[6] Figures to be finalized. Structure and purpose of the safety module as explained in Section 4.

4 ZEND Token Utilities

4.1 ZEND

Users can stake their ZEND tokens in exchange for stZEND. Upon the staking of ZEND, users will receive an equivalent amount of staked ZEND, which represents a claim to the underlying token, ZEND. Staking consists of depositing ZEND tokens into the protocol's safety module. The purpose of the safety module is to act as a risk management tool in the event of a liquidity shortfall, primarily as a result of extreme asset prices fluctuation, liquidity squeeze events, oracle inefficiency/failure and liquidation risks. The safety module may use up to [30%] of the stZEND to cover the shortfalls.

To incentivise users to actively participating to provide risk backing for the protocol, holders of stZEND may enjoy the following:

1. Revenue sharing
2. Emission rewards
3. Governance rights

The cooldown period for converting stZEND back to ZEND is [10] days upon trigger. Rewards for stZEND, however, will be claimable in the form of ZEND directly.

4.1.1 Protocol Governance

zkLend will only have one native token, ZEND with a single governance structure for Artemis and for Apollo. Holders of stZEND will be able to vote on matters pertaining to both protocols, with voting rights weighted proportionally to the number of ZEND tokens staked.

Examples of community proposals may include:

1. Listing new asset markets
2. Modifying Interest rate models
3. Incentives threshold
4. Deprecating old asset markets

The right to vote is restricted solely to voting on features of zkLend; it does not entitle ZEND holders to vote on the operation and management of the Company, its affiliates, or their assets or the disposition of such assets to token holders, or select the board of directors of these entities, or determine the development direction of these entities, nor does ZEND constitute any equity interest in any of these entities or any collective investment scheme; the arrangement is not intended to be any form of joint venture or partnership. After governance launch there will be no individual or corporate entity or other active promoter, sponsor, or group or affiliated party that maintains sole control over zkLend.

5 Use cases

5.1 Artemis

5.1.1 Liquidity Providing

Bob holds $150 worth of ETH, and he intends on holding it because he wants to take a long-term view. Bob can provide liquidity with his assets, and at the same time support the protocol to earn rewards for his contributions.

5.1.2 Leveraging

Let's assume Bob is bullish on ETH and is holding $150 worth of ETH. He can use his $150 in ETH as collateral and receive a loan on USDC. Once Bob receives $100 USDC, he can then buy $100 worth of ETH. Bob now has a $250 position on ETH while only owning $150 in ETH.

5.1.3 Shorting

Unlike Bob, Alice is quite bearish on ETH. She holds $150 USDC which she uses as collateral to receive $100 worth of ETH. Alice can now sell her $100 worth of ETH on any DEX or CEX and will now be holding $100. Assuming Alice was right and ETH price dropped 20% she can now buy the same amount of ETH she borrowed for $80. She can repay her ETH loan on zkLend and keep the profits minus the borrowing and transactions fees to herself.

5.1.4 Efficient Liquidity Management

If Alice holds a substantial amount of crypto, selling it a profit may incur large transaction-related fees. In order to avoid significant slippage, Alice decides to use her crypto as collateral and take a loan on a stablecoin. These funds can now be used freely without having to monetise her crypto position and bearing fees.

5.1.5 Arbitraging

Using flash loans, users can bundle all their trades into one transaction and save on transaction fees. The transactions for the arbitrage operation would be the following:

a) Use a flash loan to borrow USDC;
b) Use USDC to buy ETH on Uniswap (assuming lower ETH price);
c) Sell the recently bought ETH on Sushiswap (higher ETH price) for USDC;
d) Repay your USDC loan plus the fees;

5.1.6 Collateral Swapping

Using flash loans, if Alice has already taken out a loan with some crypto as collateral, she can replace the collateral with a different asset. Let's say she already took out a USDC loan using ETH as collateral. Alice

can take a USDC flash loan to repay her debt and collect the collateral ETH, she can then swap that ETH to the asset of her choice and use it as collateral to get another USDC loan.

5.1.7 Self-Liquidation

Using flash loans, traders can avoid having their positions liquidated when the price of their collateral is falling. Bob can take out a USDC flash loan to close his collateralised debt position and unlock his collateral, let's say ETH. Bob can now swap his ETH for USDC and repay the flash loan and keep the rest of his remaining position.

5.1.8 DeFi Protocol Funding (DAO-to-DAO)

zkLend will be able to offer undercollateralised lending to selected protocols - allowing protocols a revolving line of credit at a more efficient rate than current models of liquidity bootstrapping and liquidity-as-a-service.

5.2 Apollo

5.2.1 Cash management

Established institutions (blue chips, funds, insurance companies, family offices etc.) often have excess cash positions sitting idly in the bank. By placing it in a checking account, institutions only earn ~0.01% APY and are exposed to inflation risk. They could consider lending their cash in the form of USDC or other stablecoins to hedge against inflation. Meanwhile, this mechanism also allows them the flexibility to withdraw their positions at any time and avoid price fluctuations associated with other crypto assets.

5.2.2 Liquidity Providing

Similar to retail users, institutional investors that are looking to take a long-term position on an asset (i.e. Ethereum) could look to provide liquidity with their assets, and at the same time support the protocol to earn rewards for their contributions.

5.2.3 Borrowing

Collateralised
Entities that hold a significant amount of crypto assets can deposit them as collateral to borrow. Like retail users, they could take out a loan on either a stablecoin to leverage up their positions or borrow another coin (i.e. UNI) in order to sell it on the open market and take a short position on it. Utilising the best of DeFi, this trade will be compliant, automated and transparent, with rates set by parties involved.

Under-collateralised
Borrowers who opt to borrow without collateral will be able to do so. At inception, the borrower will need to submit a loan request complete with loan term and principal amount while a borrowing rate will be calculated by the system based on the above and credit characteristics of the borrower. Prospective lenders will then assess whether to opt into the pool based on the borrower's credit, loan term, and interest rate offered.

6 References

1. Aave Protocol. “Aave Protocol Whitepaper.” *Aave GitHub*, Aave, January 2020, https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf. Accessed 15 01 2022.
2. “An Introduction to Aave Arc.” *Aave GitHub*, Aave, October 2021, https://github.com/aave/protocol-v2/blob/feat/permissioned-market/aave-arc-whitepaper.pdf. Accessed 15 01 2022.
3. Buterin, Vitalik. “The Meaning of Decentralisation.” *Vitalik Buterin Medium*, February 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Accessed 15 01 2022.
4. Compound Finance. “Compound: The Money Market Protocol.” *Compound Finance*, Compound Finance, February 2019, https://compound.finance/documents/Compound.Whitepaper.pdf. Accessed 15 01 2022.

Appendix – Representation of ZEND Tokens

ZEND is the native utility/governance token which also provides the economic incentives which will be distributed to encourage users to exert efforts towards contribution and participation in the ecosystem on zkLend, thereby creating a mutually beneficial system where every participant is fairly compensated for its efforts. ZEND is an integral and indispensable part of zkLend, because without ZEND, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on zkLend. Given that additional ZEND will be awarded to a user based only on its actual usage, activity and efforts made on zkLend and/or proportionate to the frequency and volume of transactions, users of zkLend and/or holders of ZEND which did not actively participate will not receive any ZEND incentives.

ZEND does not in any way represent any shareholding, participation, right, title, or interest in the Company, the Distributor, their respective affiliates, or any other company, enterprise or undertaking, nor will ZEND entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Panama, Singapore or any relevant jurisdiction. ZEND may only be utilised on zkLend, and ownership of ZEND carries no rights, express or implied, other than the right to use ZEND as a means to enable usage of and interaction within zkLend. The secondary market pricing of ZEND is not dependent on the effort of the ZkLend team, and there is no token functionality or scheme designed to control or manipulate such secondary pricing.

ZEND functions as a loyalty membership point which embeds a licence granting active participants exclusive access to selected products or services, so users will be classified into different loyalty tiers based on the amount of ZEND staked, user activity, and/or volume of transactions. The premium membership tiers would allow users to get greater access to the ecosystem features and more preferential terms, for example (i) preferential borrowing rates, (ii) boosted borrowing capacity, and (iii) governance participation. For the avoidance of doubt, users will still need to engage with the ecosystem to access these rewards.