LITG Protocol

The Smarter Decentralized Lending Protocol to Lend, Borrow and Invest in Crypto Assets

LITG DeFi Lab

Contents

Introduction

We are witnessing the development of the decentralized financial system (also known as DeFi) on permissionless public blockchains. The extensive speed of the development of new DeFi primitives has opened up new prospects of the utilization of the crypto assets, which goes beyond its application as a transactional currency. Several instruments inherent to the legacy financial markets have migrated to the blockchain, enabling a permissionless and non-intermediated new generation of financial products. DeFi allows an unprecedented level of interoperability between different projects and protocols thanks to a common layer of deterministic computation.

One of the core innovations in the DeFi space was the emergence of the DeFi lending use-cases, which enabled programmatic lending and borrowing based on the logic incorporated into smart contracts. DeFi lending projects such as Aave, Compound, MakerDAO, Alchemix enable new source of return for crypto liquidity (for lenders) and intertemporal consumption smoothing for borrowers thanks to collateralized loans. Though DeFi lending has similarities with the traditional banks in terms of assimilation and allocation of capital, it also has unique advantages, which can be characterized by low barriers of entry and a fully permissionless executional environment. The fully permissionless interaction has enabled the protocols to assimilate billions of dollars of capital from small and big lenders, pooling the resources and providing equal opportunity for everyone to participate in the lending system.

Furthermore, the application of smart contracts has elinated the need for back-offices and potential risks related to central integration point of the whole lending flow. All transactions are publicly auditable by everyone, and the contact code itself is available for public assessment and scrutiny. Typically, the crypto-economic systems attached to these platforms are designed to enable a fair incentive mechanism to attract new capital as well as motivate the beneficial behaviour of the agents involved in the system. Fundamentally, these protocols represent crypto-capital marketplaces where the incentive mechanisms are applied to equilibrate the market for different agents.

Even though DeFi has evolved extensively in the past 2 years, this space is still in its infancy. The lack of sophistication of the protocols has lead to overcollaterization of loans, high slippage during transactions and high variability of DeFi interest rate and returns. Overall the space can be characterized as a high-risk environment with an extensive level of volatility.

DeFi offers impressive transparency, accessibility, and utility for digital asset users, but it does not match up to the functionalities offered by Centralized Finance (CeFi)—yet. The LITG protocol is designed to overcome the current deficiencies of the DeFi crypto lending space via introduction of a new generation of the crypto lending protocol, powered with a derivatives-based risk management engine and inherent derivatives DEX as well as flash loan arbitrage automation system.

We anticipate that the increase of price levels in the crypto space will trigger more capital inflow to DeFi lending infrastructures. This will require a more robust lending scheme to cope with the highly variable interest rates and better utilization of liquidity in the system. The integration of the smart contract-based interest rate swaps (and other derivatives) to the DeFi lending systems introduces higher flexibility in terms of risk hedging. Furthermore, we enable arbitragers to be able to interact with the lending system in a different way

This can translate to more stabilized interest rates for the user and better utilization of the collateral submitted to the system. In this paper, we propose a novel ZK proof-based KYC scheme based on cutting-edge cryptography. The proposed scheme can be applied to introduce privacy-preserving AML and KYC processes, which we think will help make the protocol future-proof.

1. From Traditional Finance (TradFi), to Centralized Finance (CeFi) to Decentralized Finance (DeFi)

The world of finance, money, and currency have seen many iterations. Exchange and barter have evolved from trading shells, rice, and animal hides, to precious metals. Fast forward a few hundred years, and we have moved to gold receipts and fractional reserve banking. In the age-old, tried and test system of Traditional Finance (TradFi), there are also unnecessary wide-ranging expensive fees, painfully slow transaction times, and inflationary currencies.

Enter the wave of crypto and financial technology innovation, where crypto was based on centralized finance (CeFi) wallets and exchanges such as Coinbase and Gemini for storing, buying, selling, or trading different cryptocurrencies. CeFi is in many ways similar to TradFi, centralised exchanges require new users to go through Know Your Customer (KYC) and Anti Money Laundering (AML) practices to open an account, this means transactions done on the platforms are not anonymous as the account is tied to a specific person.

It became a fiat gateway for investors to easily deposit fiat and transact cryptocurrencies, with familiar features and systems from traditional exchanges, boosting high liquidity and trading volume. However, user privacy is still in question, and they are subjected to the custodial exchange that charges fees, for assets they do not truly own.

Now comes Decentralized Finance (DeFi). DeFi is used to signify applications that function without any intermediaries, such as banks and brokerages. Instead of relying on an intermediary for custody, clearing and escrow services, DeFi relies on smart contracts operating on a blockchain. This restricts regulatory bodies from dictating monetary policies or compliance procedures.

DeFi has created an explosion of financial innovation: instant low-cost payments, high yields, liquidity pools, and advantages such as:

- **Permissionless:** Unlike many CeFi and TradFi solutions, DeFi platforms and protocols are fully permissionless. No centralized entity can restrict who can or cannot use the platform, ensuring DeFi platforms are open for absolutely anybody to use. There is also no need for KYC to access DeFi services and only a unique identification number is required.

- **Accessibility:** With digital asset wallets, DeFi represents more accessible alternatives to banks, and other TradFi platforms, opening the accessibility to engage in trading and investments using decentralized exchanges (DEXs) and trading synthetic assets.

- **Trustlessness:** Instead of relying on a trusted party, users trust the code in the smart contract, which can be audited. The auditing of DeFi services by developers informed users, and interested entities ensure better support for transparency and monitoring of transactions.

However, it remains a largely unregulated space as compared to TradFi and CeFi. While DeFi offers transparency, accessibility, and utility for digital asset users, it does not match up to the functionalities offered by CeFi—yet.

There are deficiencies in the current DeFi space, such as potential risks, which we will explore in the next section.

2. Deficiencies of the Current Defi Lending Platforms

Across the vibrant DeFi lending landscape, there is a wide array of different products, protocols and smart contracts. However, till now, there have been no tools to provide a fully-inclusive infrastructure with a robust risk management mechanism. Overall, the current deficiencies and risks of the DeFi space can be described as follows:

- **Highly Volatile Interest Rates**: The interest rates offered by the major DeFi lending platforms such as AAVE and Compound are highly volatile. High volatility of the interest rates in a lending protocol can disincentivize the adoption by the agent who is looking for a stable-rate source of liquidity or want to lend their funds for stable returns.

- **Highly Volatile of Crypto Prices:** Market prices are highly volatile, which can impact the total value of the portfolio in a relatively short period of time. Negative spikes of the price can create impermanent losses, which are allocated to the liquidity providers (LPs). Particularly, the abrupt drop of the crypto prices may lead to the undercollaterization of the lending pool (for the accounts which are engaged in the particular asset class), which assumes high risk for liquidity providers. At the same time, the high volatility creates liquidation risk for borrowers. For example, MakerDAO smart contract starts to liquidate the collateral at a potentially discounted rate if the value of the collateral (for a loan) falls below the 150 percent threshold. This implies the price volatility can impact the collateralization rate for investors leading to unexpected liquidation events, further undermining the value of the collateral submitted by borrowers.

  Another related issue is the change of market demand for a particular crypto asset, which can create difficulties for the protocol to recover the lending amount in case of collateral liquidation event. This is particularly relevant in the case of the less popular coins (also known as altcoins).

- **Overcollateralization:** One of the core deficiencies of the current crypto lending system is the need for overcollaterization. Overcollateralization

implies that the value of the staked asset (by the borrower) is significantly higher compared to the loan amount itself. The overcollaterization is applied to ensure that the borrowers' default risk is fully mitigated. Considering that the current DeFi landscape is highly characterized by the pseudonymous nature, the overcollateralization is main approach adopted to ensure that system can function efficiently. If the borrower defaults on his loan, the current lending protocols liquidate the pledged collateral to recover the lending amount and corresponding interest rate for the liquidity providers.

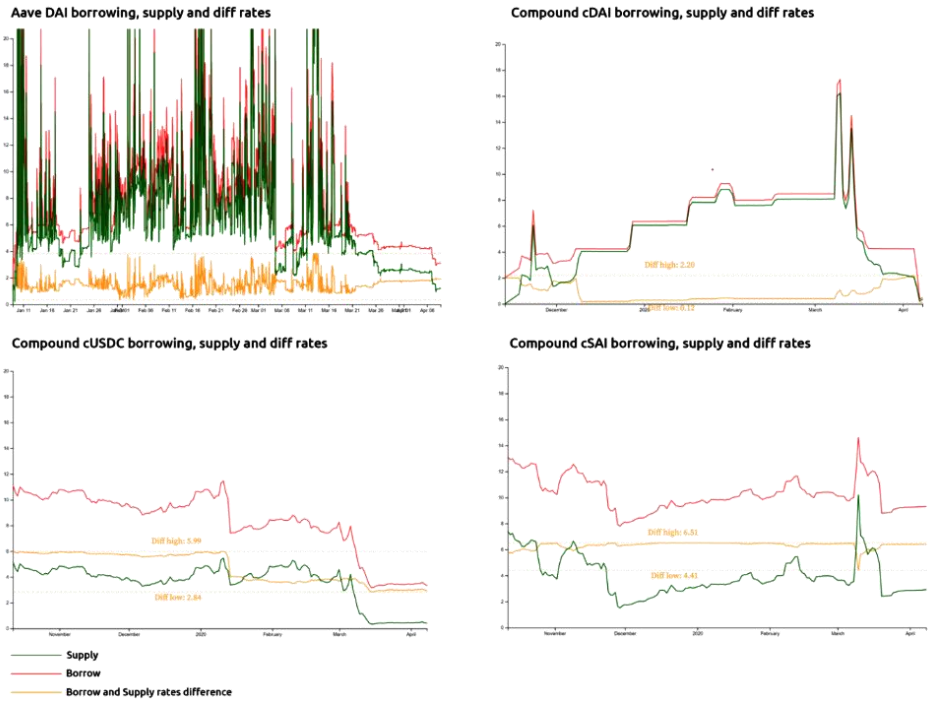
The reason for this is that in the current lending protocols, there are no effective mechanisms and toolsets for lending pool level risk mitigation and active management, which leaves the whole system fully reliant on overcollaterization. According to our analysis, overcollaterization will stay a relatively efficient approach in the bull market. However, in a bear market, as there will be lower demand by investors to have open positions for specific crypto assets or whole crypto space in general, we anticipate a significant outflow of the crypto-capital from the current DeFi lending protocols (due to overcollaterization).

- **Prone to Attacks by Malicious Users:** The current lending protocols are prone to over-utilization and under-utilization of the submitted liquidity, and this inefficient utilization of the lending pool can lead to attacks by malicious users. Generally, assets are considered under-utilized if, after the collaterals are being submitted to the lending pool (by LP), it has not been lent out to borrowers. The current lending protocols inherently do not have built-in options to enable other sources of utilization in case if the demand of the capital (lending activity rate) has significant variations. This makes the protocol dependent on the efficient discovery of optimal interest rates. This also makes the crypto-lending system vulnerable to 'flash loan' and under-utilization attacks by malicious users. These types of attacks assume that the malicious users participating in the protocols take significantly big loans and then repay loans abruptly, creating the temporary dislocation of the effective interest rates, manipulating the market and exploiting vulnerable DeFi protocols for their own personal gain.

- **Difficult Management of "Impermanent Loss":** The other deficiency of the current lending systems is the potential impermanent losses. This type of event can happen if after provision of liquidity, the prices of the crypto assets change in a negative direction, creating unrealized losses for liquidity providers (LPs). The current DeFi lending schemes do not have optimal approaches to protect LPs effectively.

2.1 The Need for Fixed-Rate Lending Systems

Fixed-rate lending is by far the most common type of lending in CeFi. For instance, of the $15.3 trillion of debt outstanding in the US corporate debt and mortgage markets in 2018, 88% of it was in fixed-rate terms[1]. Overall, fixed-rate loans allow participants to lock in a predetermined rate without having exposure to interest rate volatility



Currently, in the DeFi space, the interest rates are mainly directly correlated with the supply and demand of the capital in a particular platform (such as in

[1] https://www.magnifymoney.com/blog/mortgage/u-s-mortgage-market-statistics-2018/

Aave). So far, primarily, there has been only one form of credit in DeFi, overcollateralized crypto-backed loans with variable rates. The DeFi interest rates are a function of the utilization rate of a pool. When liquidity is in great demand, the loans will gradually become more expensive, while when the liquidity is readily available, loans will become cheap. Thus the high volatility of available liquidity in the DeFi market results to highly variable interest rates.

The playing field is wide open for fixed-rate lending systems. The attractive proposition of fixed-rate lending, the stabilization of interest rate in crypto marketplaces is a complex endeavour. The LITG protocol has been designed to meet this market need. We believe that the derivatives and protocols enabling active risk management (combined with the current mechanism of collateralization) are essential components for structuring and implementing fixed yield lending schemes.

2.2 Utilization Rate Issues in the Lending Protocol

In the asset management protocols the utilization rate is core consideration point as it indicates overall of the efficiency of the deployment of the asset into productive usage. The utilization rate is particularly crucial in the banking industry as it is direct indication of the health of institution.

Overall, 2 states of not optimal utilization can be defined: overutilized and underutilized. Underutilization implies that at least one of the tokens provided to the protocol is not lent out to any user. Thus, it does not result any gains for the lenders. On the other hand, over-utilization occurs when some users have borrowed fund, however, the lending pool has no deposited funds to effectively back the position. In this case, users can neither borrow or redeem. Under- and over-utilization is not desirable and should be avoided. Typically, the lending pool interest rate change models as structured to discover a utilization equilibrium between under- and over-utilization. However, we realize that these type of designs are normally non favorable for new and less popular DeFi lending platforms as they lead to the low interest rates, disincentivizing lenders to lend their funds to these protocol.

With LITG, we introduce lending pool integrated asset management system (yield farming), which would enable to optimize the utilization rate without compromising the return for LPs (lenders).

3. Introducing LITGProtocol: The Transformation to DeFi Lending

LITGProtocol's main design proposition aims to transform DeFi lending with its decentralized lending pool and in-built derivatives decentralized exchange (DEX) system. The decentralized protocol is an ecosystem of next-generation financial products, making lending, borrowing and earning interest on crypto assets more accessible for everyone.

LITGDeFi Investing

- **Arbitrage Bot Automation System:** Users can potentially profit from margin trading by simultaneously buying and selling assets from different exchanges by scanning for arbitrage opportunities, known as Flash Loan Arbitrage.

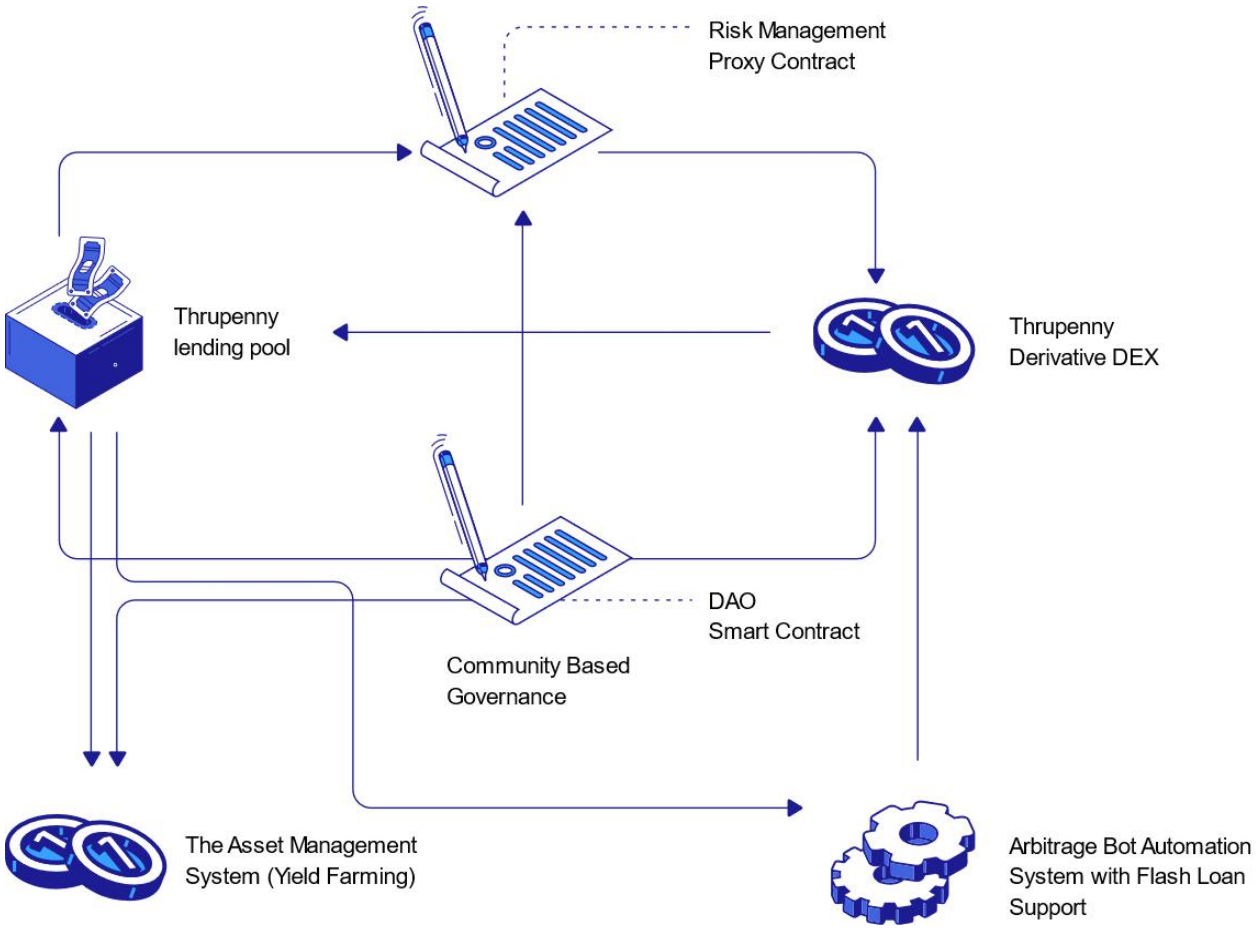
- **Asset Management System:** Yield Farming, which is lending or staking cryptocurrency in exchange for interests and rewards.

LITGDeFi Borrowing and Lending

- **Lending Pool with In-Built Derivatives Decentralized Exchange (DEX):** Crypto-backed loans on a platform with pooled assets, security aided by smart contracts. The LITG lending procotol aims to address the current problems in DeFi lending through the incorporation of DEX, where its mechanism allows for a more stable interest rate, efficient utilization of lending pool, avoid overcollaterization and better risk management to protect participants from impermanent loss.

    - **Smart Contract-Based Interest Rate Swap (IRS):** Stabilizing highly volatile interest rates by combining an interest rate swap with a floating-rate borrowing position to net out to a fixed-rate borrowing rate.

- **Risk Management and Automatic Derivative Position Origination Scheme:** Enabling liquidity providers as well as individual participants to hedge against and speculate on a different type of risk exposure via DEX.



3.1 Arbitrage Bot Automation System

The fragmentation and inefficiencies of DeFi markets mean that prices for the same financial instruments vary across different DeFi venues and its inefficiencies mean that they adjust differently to the same market movements. These provide great arbitrage trade opportunities. Arbitrage allows users to simultaneously buying and selling assets from different exchanges. Users can make money by searching for price discrepancies

across numerous exchanges, without the need to pose huge risks and stake their own assets.

LITG's flash loan arbitrage system is a powerful DeFi mechanism and liquidity protocol for no-code generation DeFi arbitrage bots , which would look for arbitrage opportunities in the market and trigger execution of arbitrage logics as soon as identified opportunity corresponds user's expected profit specification. Even though the system is fully automated the bot design is fundamentally based on smart contract and user granted permissions, maintaining high level of decentralization and trustlessness in the execution logic.

Overall, the LITG protocol uses a smart scan of the most favorable price quotes across exchanges for the users' selected token, comparing the bid and ask prices to identify price discrepancies which subsequently can be leveraged with flash loans to execute profitable arbitrage trades.

3.2 Asset Management System

Overall the yield farming flow represents set of smart contracts that enables to aggregate the market participant's crypto assets and programmatically manage it investing in an array of different DeFi protocols. Normally these type of protocols are aiming to maximize the return (in terms of Annual Percentage Yield) while minimizing the risk that has assumed via investing the liquidity into different protocols. Generally, the yield farming aggregation contract can be characterized as smart contract based fund manager which invests in the DeFi universe.

The LITG has native on-chain asset management (Yield farming) protocol integrated which is attached to the lending liquidity pool, aiming to optimize the utilization rate of the assets/liquidity submitted to the LITGecosystem. As we mentioned in section 2 this type of optimization can significantly improve the health of the whole system as well as contribute to high utilization rate, i.e. higher return for lenders.

One of the main advantages of the smart contract-based LITGasset management process is the cost saving that these types of systems can bring. Instead of paying an investment manager to balance your portfolio as a LP, smart contracts automatically and directly match your provided liquidity to a qualified professional trader capable of liquidity mining strategies that maximize returns.

3.3 Derivatives Decentralized Exchange

With the in-built derivatives decentralized exchange, the lending pool contract enables the protocol itself to open derivatives positions, achieving dynamic and automated hedging of some of the risk in the system. Furthermore, the scheme has incorporated decentralized autonomous organization (DAO) to allow the community-driven decision making regarding the risk levels that the lending pool will assume.

The utilization of this toolset in terms of incorporation of a native derivative marketplace can:

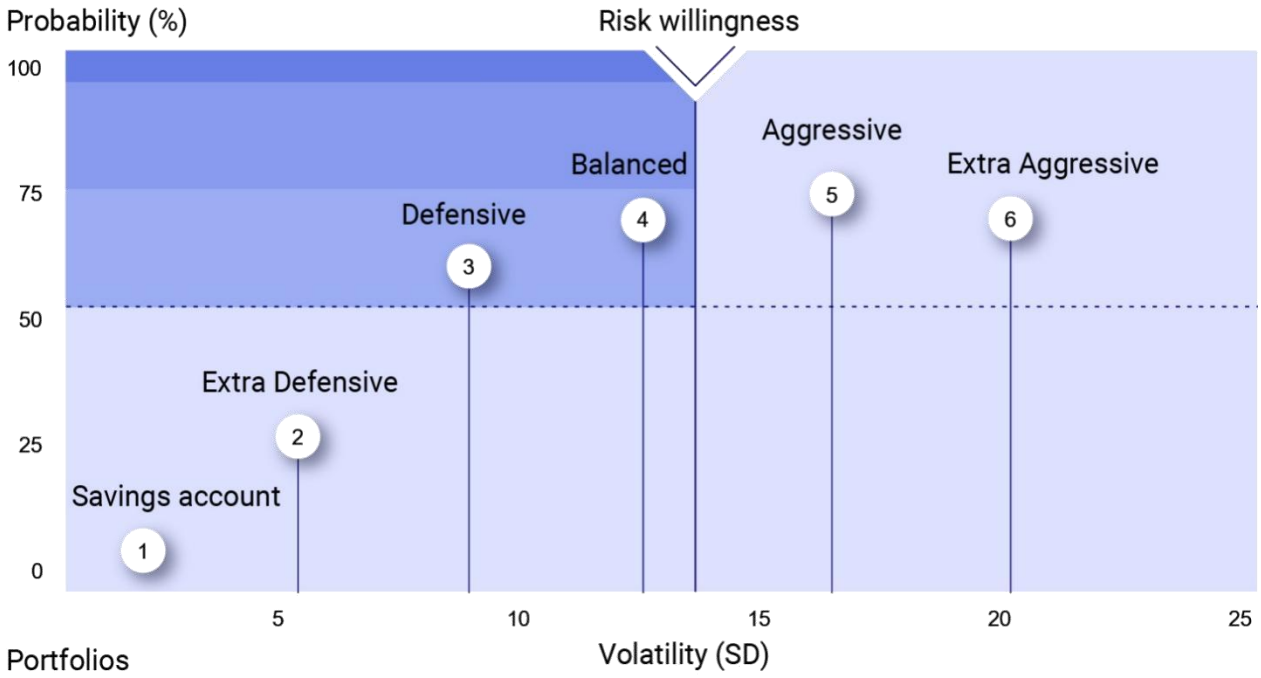
- **Enhance efficient utilization of the lending pool**;
- **Mitigate the need of the over-collaterization**;
- **Enable fixed interest rate based loans and returns**.

All 3 value propositions described above are not comprehensively addressed by the currently available lending protocols, which represents opportunity and gap in the current DeFi space.

The interest rate derivatives enable the swap of the floating rate interest-bearing instruments against fixed rates. Thus, they represent very valuable instruments for interest rate hedging in traditional financial markets (CeFi). In the DeFi context, the application of the interest rate derivatives enables a more customized state-contingent payoff structure, which allows the assumption of a smaller amount of risk on the lending pool level. In addition, it enables converting the payoff function of the lending pool interests to be non-state-contingent. Even though, as part of our lending protocol, these

derivatives positions will be opened fundamentally assuming zero expected payoff, they will provide significant value for the whole ecosystem enabling a hedging layer.

Overall, the system is based on smart contracts, which represent computer programs that can enable immutable automation of the life cycle process both for the lending as well derivative origination. Furthermore, the core advantage of the smart contract is the fact that it does not introduce the central point of integration and can not be tempered by a single malicious agent involved in the process.



The Governing Community Can Adopt Different Strategies for a Lending Pool

Via the application of the LITG Protocol, we are aiming to enable a more sophisticated risk mitigation mechanism via the introduction of the native derivatives marketplace attached to the lending infrastructure. The LITGprotocol comes to fill the current gaps in the DeFi lending space.
The system does not enforce the same type of liquidation event as the Aave and other available protocols and adopts more advanced approaches to cope with credit risk, currency and interest rate risk via origination and trade of crypto derivatives.

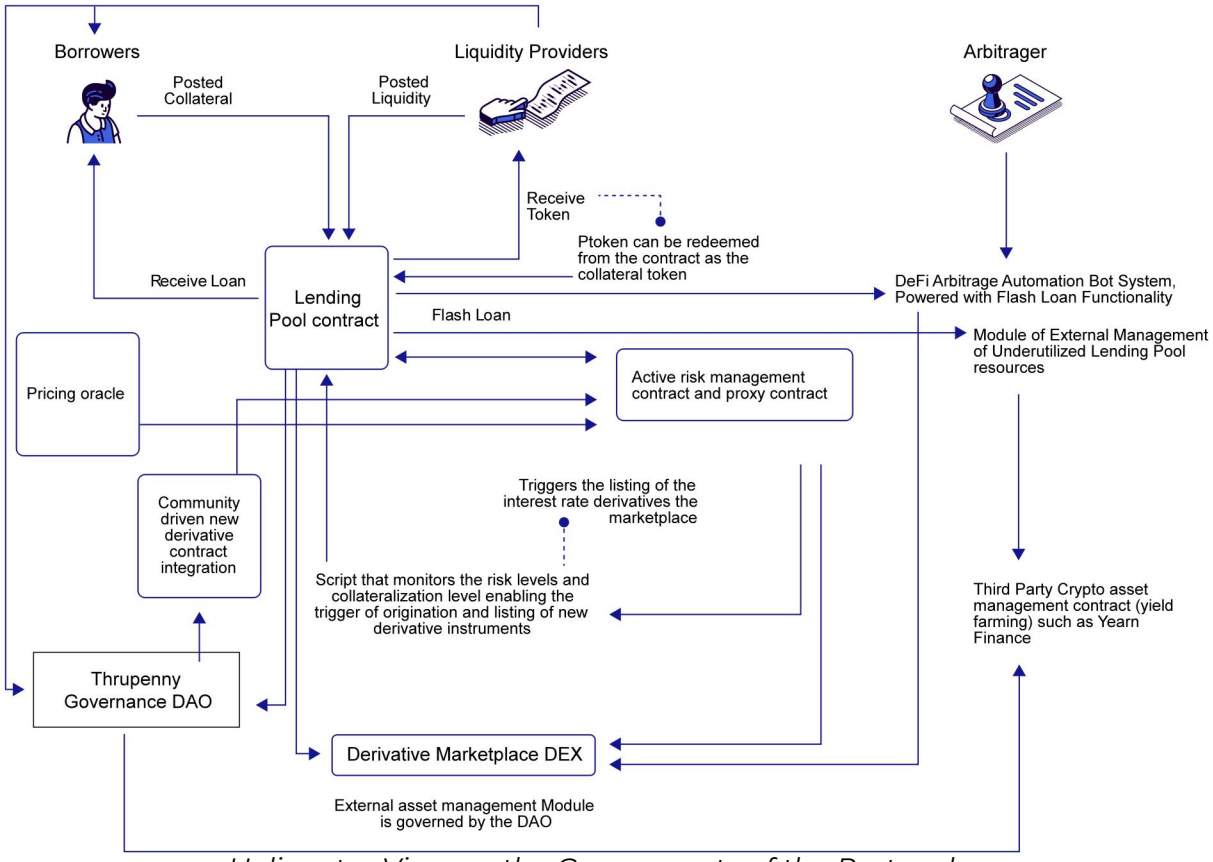
The whole concept behind our inclusive infrastructure is to ensure that appropriate and prudent risk limits, sound measurement procedures, continuous risk monitoring are in place in the system, attached to the execution layer.

4.LITGProtocol Infrastructure

The LITG ecosystem is designed to be the new evolution in DeFi infrastructure for investing, lending and borrowing. The protocol is powered with the inherent derivative DEX and risk management contract, which enables derivative origination and listing in the derivatives marketplace.

The following modules are applied to the protocol's infrastructure:

- **Lending pool smart contract:** Lending pool smart contract that facilitates the P2C interaction of the users with the system for the crypto asset pooling and lending. It includes all the necessary checks and balances to ensure the deterministic calculation of the interest rate and collateralization ratio. Within it has a Flash Loan Arbitrage system that allows users to potentially profit from margin trading by simultaneously buy and sell assets from different exchanges by scanning for arbitrage opportunities.
-
- **Derivatives marketplace attached to the lending protocol:** The design of the DEX is based on the 0x protocol. It enables both users as well as the proxy risk management contract to open derivative positions in the system to hedge risks.
-
- **Risk management contract and related backend service**: It monitors the open lending positions, interest rates and collateralization ratio in order to make a decision regarding the derivative positions that need to be opened.
- And other supporting infrastructure such Augur DAO-based governance mechanism, Chainlink-based Oracle service, etc.



Helicopter View on the Components of the Protocol

In terms of the technical stack, the whole system is designed in a composable way which enables the application of each of the main components as stand-alone building blocks for other cryptosystems.

In the system as settlement layer, we apply Polygon Layer 2 blockchain. It allows the network to store ownership information securely and ensures that any state changes adhere to its ruleset. The blockchain can be seen as the foundation for trustless execution and serves as a settlement and dispute resolution layer.

The asset layer of the protocol consists of assets that are issued on top of the settlement layer. This includes the native LITGtoken as well as any additional ERC20 compliant tokens that are accepted in the lending system.

4.1 LITGLending Pool System

In contrast to the legacy banking infrastructure in the DeFi lending protocols, smart contracts are applied to ensure the automated execution of the parameters of the contract based on predefined logic.

The design of the lending pool system of the LITGProtocol is has based on the kinked rate structure where certain events can trigger jump movement of the interest rate. To derive the core variable rate, we apply a similar approach applied in the Aave lending protocol. However, LITG protocol proposes a completely innovative way of stabilization of the interest rate via application of the derivative-based risk management.

Overall, the variable interest rate in the system is dynamically changing depending on the total funds deposited in the smart contract as well as the utilization rate of the deposited funds[2].

In the scheme, one of the main variables that affect the lending rate is pool utilization rate U. Overall the utilization rate of a lending pool in each block (epoch e) can be defined as follows:

$$U_e = \frac{L}{P}$$

Where L is correspondingly the total loans originated in the contract and P is the pool size.

In the logic of the contract, the interest rate is designed to ensure that on the lending pool level, the utilization rate is close to the optimal level (hardcoded in the system), dynamically adjusting the interest rates to target a certain level.

$$r_e = \begin{cases} r_0 + \frac{U}{U_{optimal}} r_{slope1}, if\ U \leq U_{optimal} \\ r_0 + r_{slope1} + \frac{U - U_{optimal}}{1 - U_{optimal}} r_{slope1}, if\ U > U_{optimal} \end{cases}$$

[2] Aave Protocol Whitepaper, January 2020, https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf

Where :

r_0 : is the base variable borrow rate;

r_e :The interest rate per block is denoted by.

U : Utilization rate of the fund deposited in the system;

$U_{optimal}$: Optimal utilization rate;

r_{slope1} : Interest rate slope below optimal utilization;

r_{slope2} : Interest rate slope above optimal utilization;

Two interest rate slopes, parameters of the system, are used to compute the variable interest rate: r_{slope1} in case if $U < U_{optimal}$ and correspondingly r_{slope2} is applied when $U \geq U_{optimal}$.

Furthermore, the whole logic itself assumes tokenization of the lending positions. Upon provisioning liquidity, the liquidity providers receive $Ptokens$, which certifies the liquidity providers share in the total liquidity pool. The liquidity provider can liquidate their positions via selling their $Ptokens$ without withdrawing their liquidity from the lending pool smart contract. This mitigates the risk of the sudden spikes of the utilization rate due to highly volatile liquidity level. The $Ptokens$ also assume the distribution of the benefits in the form of the interest to the liquidity providers as compensation for the provisioned liquidity.

LITG is the application of the automated derivative issuance based on the liquidity accumulated in the lending pool. Interest rates on decentralized lending protocols change with every block, which means interest rate swap orders must be filled quickly before they go stale. In order to ensure deep liquidity and efficient price discovery in such a volatile market, we incorporated DEX into system.

4.2 No-code Arbitrage Bot Integration for Flash Loan Support

LITG system introduces no code generation of DeFi arbitrage bots (powered by flash loans), where the users of the platform can easily adjust the parameters of the arbitrage bots and deploy them for finding arbitrage opportunities across numerous decentralized exchanges. Once the bots find the arbitrage opportunity, the smart contract will execute the arbitrage trades, repay the Flash Loan amount, all within a single transaction for the user.

Generally, the flash loans are non-collateral borrowing contracts, where the assets are lent to users by a flash loan as long as the borrowed assets can be paid back within the same transaction. If any part of the transaction fails to happen, the flash loan contract instantly reverts the transaction to its initial state, thus returning the assets.

LITG flash loan arbitrage bots will include an easy to use drag and drop interface to enable the users to borrow flash loans from a third-party markets and arbitrage it in other decentralized exchanges for profit. The users can add the parameters of the bots on the platform (e.g., the profit margin, slippage percentage, gas price etc) according to their preferences, sign the transaction on their end, and deploy them on a dormant position. The deployment of the bot happens as soon as the parameters specified by the user are met, the bot triggers the smart contract for the arbitrage.

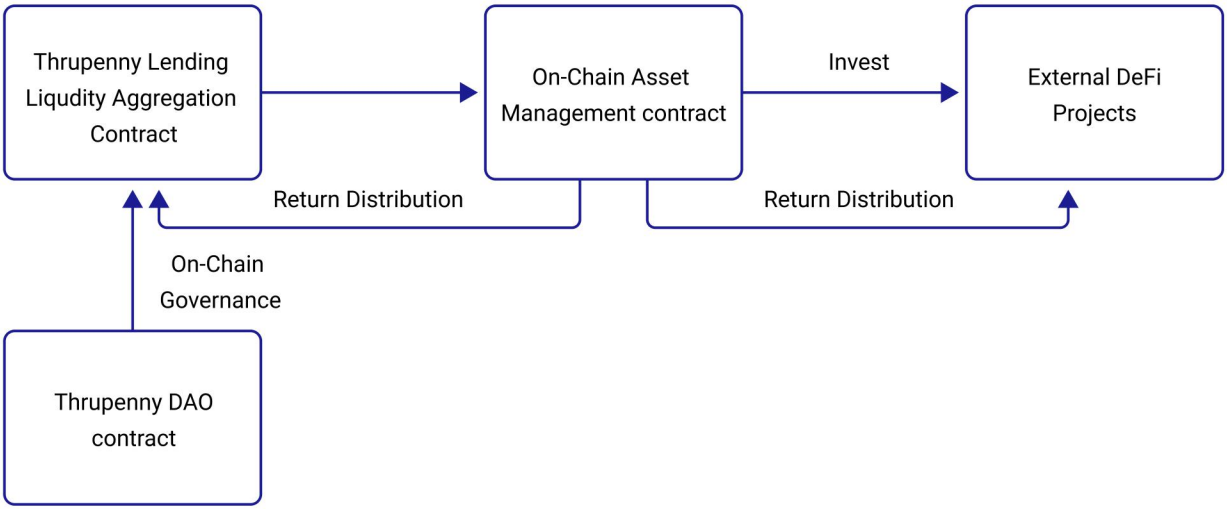
DeFi infrastructure has new features such as atomic batch-based processing of transactions which potentially enable new trading strategies with no analog in traditional financial markets. In the later version of the protocol the DeFi arbitrage bot system will be also attached to LITG liquidity pool enabling the user to directly take flash loan from the native liquidity pool execute the arbitrage and return the loan and small fee back to the pool. This design creates a holistic and seamless experience for the user.

On the smart contract level, the flash loan module temporarily transfers the funds to a smart contract which is based on a specific interface. After the funds are transferred, the trade execution method executes the trade on the external contracts based on the user prespecified execution logic. The

contract executes whatever action is necessary with the borrowed funds. After the execution is completed, a check is performed to verify that the funds plus fee have been returned to the LendingPool contract. The fee is then accrued to the reserve, and the state of the reserve is updated.

4.3 Yield Farming Integration for Maximization of Utilization Rate

The system will have an integrated yield farming mechanism which serves to incentivize the pooling of the liquidity by LPs. Yield farming is a highly effective reward distribution system, where on one hand the platform receives the necessary funds for aggregating value through its different components (flash loans and Yearn Finance) and in return provides native token to the LPs and distributes the vast majority of the revenue generated over the platform to the LPs.



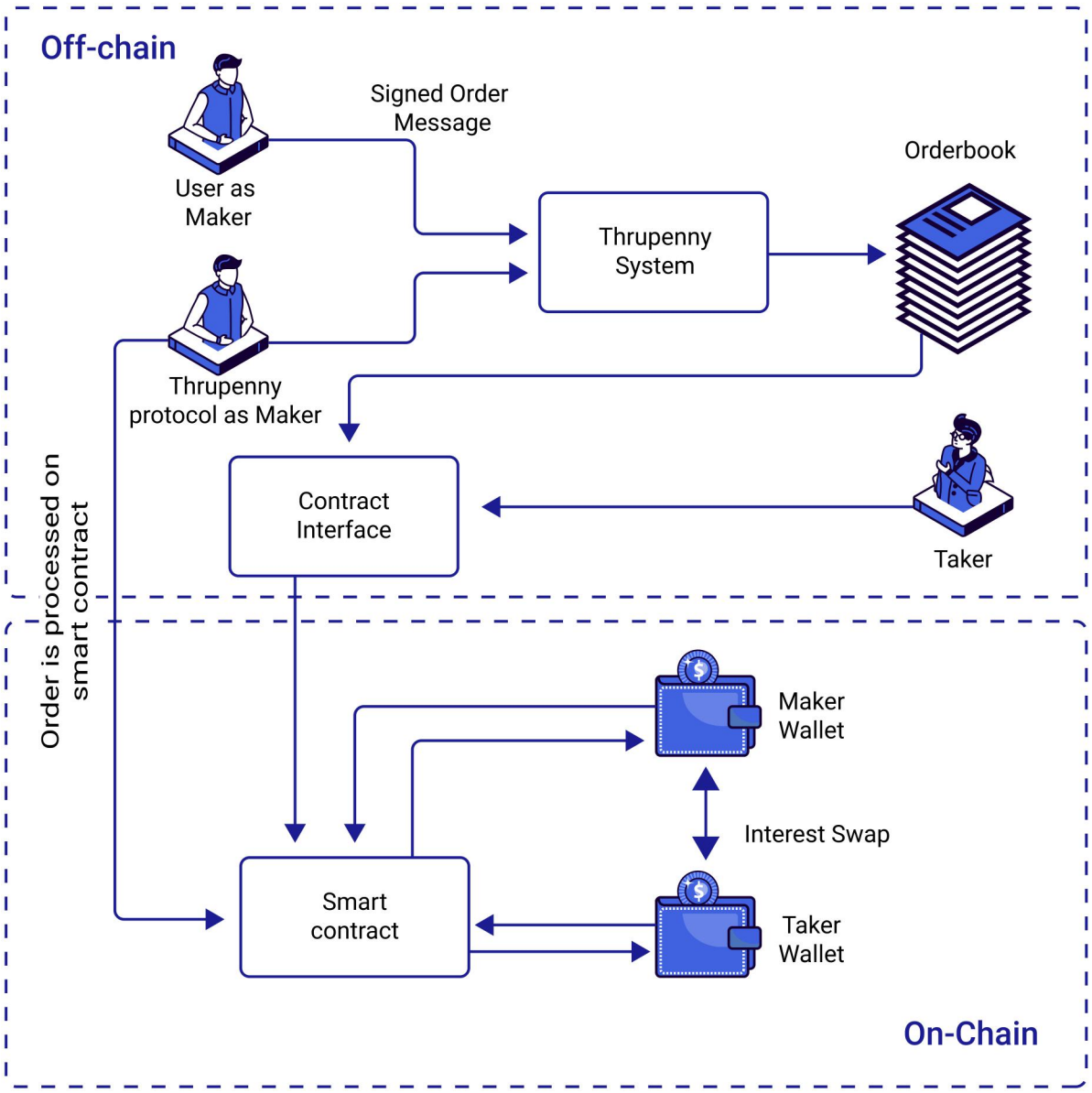
The yield farming module is designed to ensure that the utilization rate of lending liquidity pool is always in the optimal rate , ensuring optimization of the safety and return. The optimal utilization rate will be based on parameters defined by the LITG DAO. If the overall utilization rate of the lending pool is lower than the prespecified amount, it would trigger the investment of some of the aggregated liquidity to the external projects. In the opposite scenario, the contract will pull the invested liquidity back to the liquidity

aggregation contract, ensuring optimal fund utilization rate in the LITG system. In the context such a flow resembles characteristics of a bank.

4.4 LITGIn-Built Derivatives DEX Infrastructure

In the system, we also have integrated derivatives DEX as a composite infrastructure designed to facilitate efficient risk diversification via enabling users and protocol itself to open up new derivative positions in the system. The derivative DEX represents one of the core building blocks of the whole system. In its construct DEX system is utilizing some of the characteristics of 0x protocol leveraging of out-of-box advantages of the technology such as the possibility of liquidity aggregation between several decentralized exchanges as well as the composability enabling attachment of unique modules to the core system for extending the functionality provided by the DEX. The smart contract embedded in the protocol supports derivative positions that can be opened both by the user as well as the protocol itself.

On the user side, the proposed design is fully based on non-custodial logic for the user keys (keys are held by the user), eliminating any possibilities of the single point of failure (which the centralized exchanges are prone to).



Overall, the derivatives will be issued by the Risk Management Contract (of LITG protocol) as well as by any market participant. Our system enables users of the whole DeFi ecosystem to utilize LITGLending pools to enter derivative positions to hedge their exposures opened with LITG lending pools as well as other DeFi projects. Furthermore, users can leverage their exposure via getting a loan from the LITG lending pools and then using the funds to enter a derivative contract with the LITG Marketplace.

The system enables users to directly trade with lending pools of the LITG system, so the lending pool, in most cases, assumes the role of a market maker. Considering that liquidity pools are aggregated within the system, it overall provides higher depth and security to LITGderivative marketplace.

Furthermore, users via trading in the system do not need to fill full derivatives positions. They can choose to enter into positions with almost any notional value (that corresponds with their needs), which can represent a fraction of the position.

As soon as users want to enter into a contract, an order message is signed by the user and is sent directly to the relayer who exposes the LITG derivatives in his exchange. Relayers in this context have a similar type of role in the system as to the ones introduced by the 0x protocol. Many decentralized exchange protocols only use the blockchain as a settlement layer and rely on off-chain order books.

Relayers are external actors who match orders of users off-chain and then broadcast them to the blockchain. Relayers are incentivized by optional settlement/relayer fees paid by the user as well as LITGsystem. Overall, they provide takers with the information they need to enter into a derivative contract and fill one of the positions opened. The protocol uses a three-step process for each trade. First, as soon as there is a change of the open positions on any of the derivatives positions issued by the LITGprotocol, the relayer gets notified. Second, a potential taker inquires the relayer and selects one of the available orders. Next, the taker signs and submits the order, collateral to the derivative smart contract, entering into a derivative contract with LITG.

4.5 Risk Management and Automatic Derivative Position Origination Scheme

Derivatives have always been a useful way for financial institutions and systems (in CeFi) to manage risk. In LITGlending system, credit risk,

interest rate risk and currency risk will be hedged so that the customer, or the financial institution, is only taking on selected risk, not the whole package. Further application of the derivatives enables to separate different types of risks from each other, such as credit risk from cryptocurrency price risk and interest rate risk.

The provision of the derivative marketplace as an integrated part of the LITGecosystem creates significant value enabling the lending pools (liquidity providers in the LITGsystem) as well as individual participants to hedge against and speculate on a different type of risk exposure.

In the more legacy banking settings, the decisions made regarding lending, financing and hedging is based on the objective of maximization of the wealth for equity holders, which is function to risk-neutral security pricing in the capital market. A similar approach is also adopted by the LITG protocol, targeting a community-driven risk management strategy.

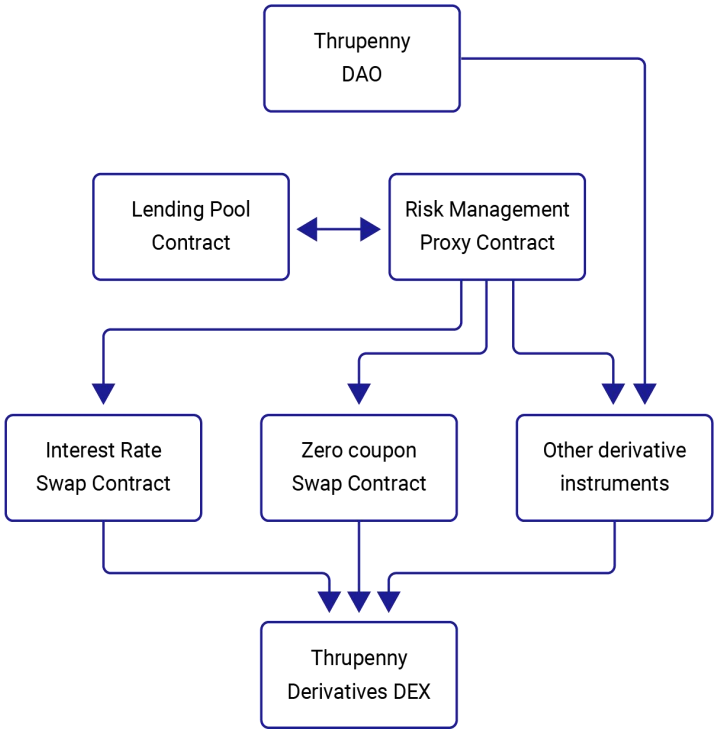
Via enabling the origination of the smart contract-based derivatives, the system further facilitates transfer of unwanted interest rate, credit and crypto-currency price risk. Derivatives may also be used to increase the yield of certain crypto assets and reduce financing costs.

Overall the system heavily relies on the pooled interest rate swap as a solution for the mitigation of the risk and conversion of the maturity and interest rate variability. The active risk management scheme is composed of two smart contracts, and the whole system is attached to derivative DEX.

There are many factors that can affect the behavior of the risk management contract, including but not limited to the utilization rate of the lending pool, the crypto assets involved in the lending and borrowing process, the collateralization threshold for each crypto asset, amount of deposited and borrowed crypto capital that has preference over the fixed rates, etc. Based on the market's state and risk target (defined by the DAO), the protocol will open and close derivative positions in the native derivative DEX.

The initial derivative instruments incorporated in the system will include interest rate swaps and other interest rate derivatives such as interest rate caps(floors), zero-coupon swaps as well credit derivatives, such as credit risks

swaps will be incorporated. Furthermore, the derivatives instruments that the protocol can apply will be community-driven, enabling the community to suggest its own derivatives, which can be accepted via a decentralized governance mechanism (using DAO).



Overall, the origination of new derivative positions enables a dynamic collateralization ratio and more efficient utilization and rehypothecation of collateral.

Of course, the system will involve collateral constraints putting an upper bound on the amount of debt and swaps. The smart contract is set to receive the swap rate $r + p(r)$ at the epoch $t + 1$ and must hold enough funds to pay both the liquidity providers as well as for the worse-case floating rate on swaps.

The open position in the system might go up as well as down based on which type of lending and borrowing transactions has been conducted in the lending pool.

Derivatives users can also restore their future lending capacity by using swaps to transfer funds to future investment states. Using LITGthey do not cut lending as much as would otherwise be the case. This yields asymmetric effects between booms and busts periods of crypto space.

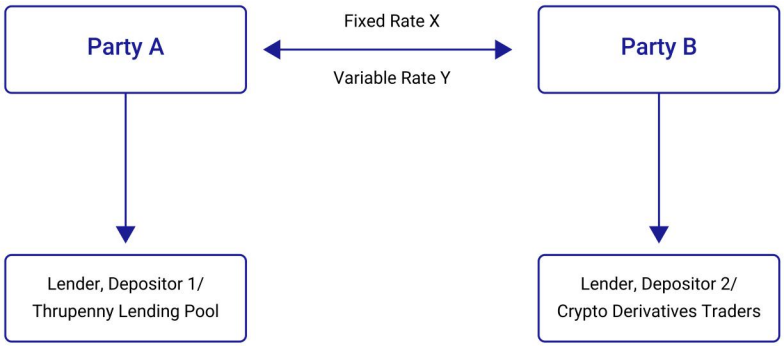
5. LITGDerivative Smart Contract Systems

5.1 Smart Contract-Based Interest Rate Swap (IRS)

As crypto markets are characterized by much higher volatility of the interest rates than CeFi market, interest rate derivatives are great products in the market and can add significant value to the ecosystem. Interest rate derivatives can be used to hedge risk or speculate on the volatile interest rates of on-chain assets. Furthermore, combining an interest rate swap with a floating-rate borrowing position can be used to net out to a fixed-rate borrowing rate.

Interest rate swaps are derivative contracts between two parties to exchange one stream of interest payments for another over a set period of time. The parties do not exchange the underlying principal amounts, only the streams of interest payments. Interest rate swaps include the exchange of a fixed interest rate for a floating rate (or vice versa) or the exchange of one type of floating rate for another (basis swap). Currently, the DeFi lending interest rates are mainly directly correlated with the supply and demand of the capital in a particular platform (such as Aave). The development of CDS instruments has the potential of stabilization of interest rate in this marketplace and enable market-based default risk assessment attracting new users who appreciate the stable interest rate on their crypto assets. Furthermore, the application of these products by the LITGsystem will enable to hedge the interest rate risk of the LITG Lending Pools (performed by the Active Risk Management contract).

Basic overview of the Payment Flow between parties Entered into IRS contract



The contractual interaction between parties is handled by LITGInterest Rate Swap smart contract, executed on the blockchain. Given the prevalence of variable-rate yields in the DeFi ecosystem, there is a huge opportunity for interest rate swap (IRS) protocols to step in and allow lenders and borrowers to swap out their floating yields and lock in fixed yields.

Opening interest rate swaps allow traders to hedge risk on an underlying interest rate. Within this transaction, a trader can decide upon the swap's notional amount and if they would like to pay or receive the fixed-rate loans using LITGas well as the user as a trading counterparty. Of course, this swap is conditional on whether LITGhas opened a corresponding derivative (IRS) position in the marketplace. Furthermore, the trader can choose to receive the floating rate and to pay the fixed rate, putting the trader on long positions on the floating rate, and doing the opposite constitutes a short position. Once a swap has expired, anyone can call a function to close the swap; if action is not performed, the protocol will roll over the derivative position.

Helicopter view on the LITGIRS contract

Overall, interest rate swaps are designed to enable the exchange of the fixed and variable flow streams (also called legs) between counterparties, where the payment is determined by the variable interest rate prevailing in the LITGlending pools. If the default event happens, it fully halts the future flows between counterparties.

When designing the Interest rate swap smart contract, following the main variables have been considered:

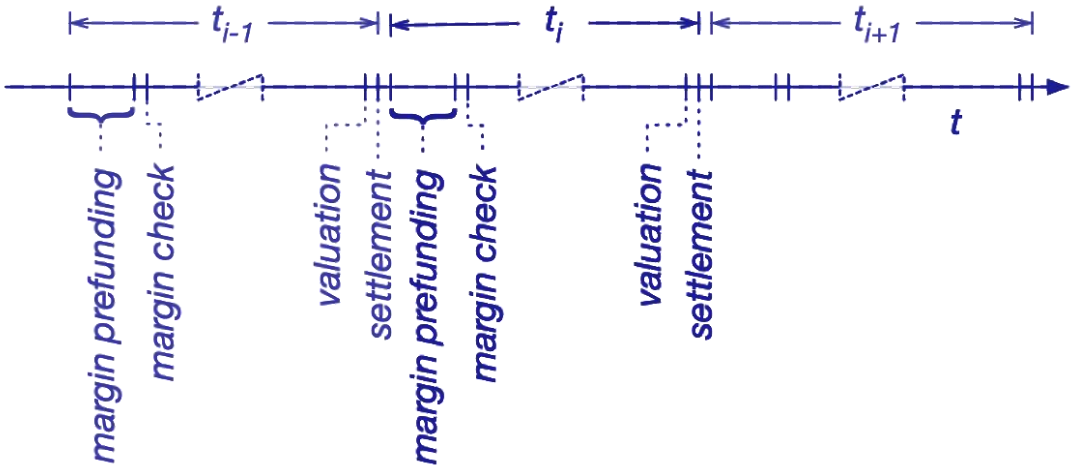
- **a.** The life-span of the contract: This includes the total timeframe where the contract will be active, i.e. the counterparties involved in the contract cannot get back the collateral submitted to the contract.
- **b.** Frequency of the Variable Interest Rate submission (calculation frequency).

c. Payment frequency: The payment frequency may or may not concede with rate submission frequency, which is determined by the party originating the contract.

d. The Variable rate: Generally, variable rates are based on the reference rate, which is prevailing in a particular DeFi marketplace. However, the parties who originate the contract can customize adding basis points on top of the rate or even peg the rate to the interest rate in legacy financial markets (such as LIBOR).

e. Token applied in the contract: The party originating the contract can determine the token (ETH & ERC20) that will be applied for the settlement.

f. Margining Procedure: The smart derivative contract also has integrate the margining procedure. The margin buffer is conceptionally the pre-funding of an expected maximum variation margin consumed at every settlement. In case of an insufficient margin balance, the smart derivative contract terminates prematurely.



6. LITGKYC Smart Contract System

Unlike CeFi, where the identity of all participants is known, and correct behavior can be enforced via regulation, DeFi actors are pseudonymous, and DeFi systems need other means to prevent users from misbehaving. The increase in the popularity of the DeFi, as well as the institutionalization of the DeFi protocols, will assume that a certain level of permissioning will be required in the DeFi ecosystem. This would be related to the application of more stringent KYC and AML requirements to ensure that these protocols are not subject to exploitation for criminal activities and money laundering. In the LITGprotocol, we also propose a novel scheme of the KYC model designed to enable potential integration of the KYC processes without centralization and without compromising the user privacy and secrecy of the identifier information. For this reason, we particularly apply zero-knowledge proofs and other cutting edge cryptographic primitives that can enable on the one hand to have unfalsifiable checks and verification of the user ability to participate in the protocol and, on the other hand, does not reveal any information in the process that can be applied against the user.

It is important to highlight that the LITGcommunity will have the ability to choose to instigate the KYC checks or disable the KYC from the system (via using the DAO based governance mechanism).

In the next subsection of the process, we introduce some of the cryptographic primitives that have been considered for application in the system as well as we provide more in detail elaboration on how the KYC module operates.

Helicopter View on the Scheme

In the protocol, several cryptographic primitives have been applied to enable homomorphic operations as well as the privacy-preserving verifications on the encrypted data. As the first primitive, we apply Pedersen commitment, which in a nutshell represents an encryption mechanism that had homomorphic properties under the discrete logarithmic assumptions.

Particularly, the identifier information of the user can be converted to the Pedersen commitments

$$Com_{ck}(i; r) = g^i\ h^r$$

Where

G represents the cyclical group designed prime order p and random generators g and h.

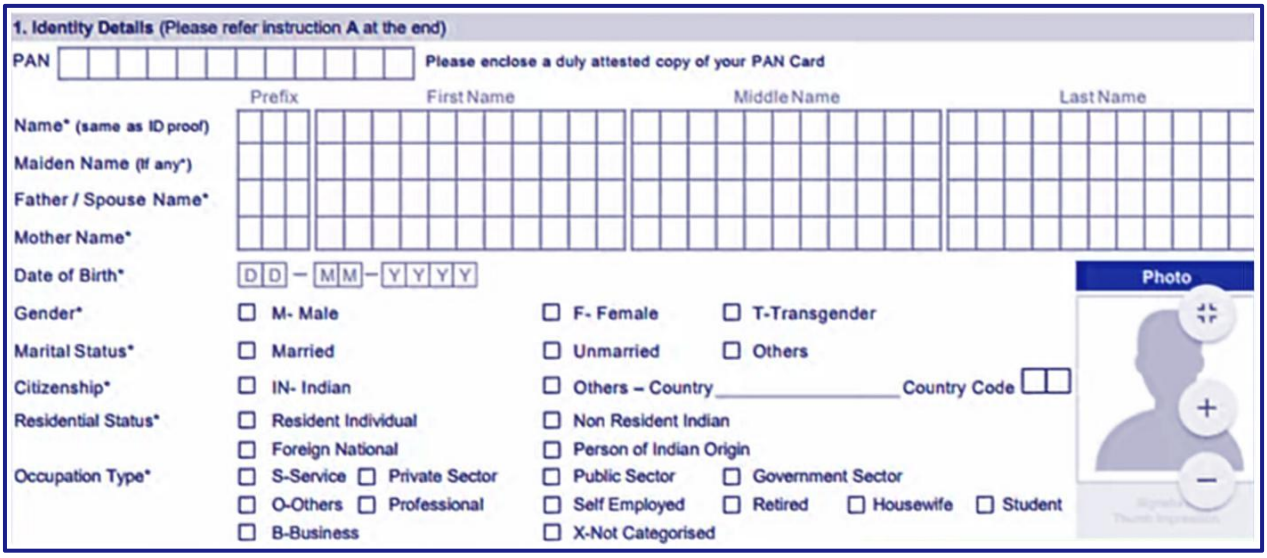
The commitment key is ck = (G,p,g,h),

i is the user identity information.

Furthermore, the process can be generalized a full list of the identifiers, enabling a very efficient scheme for the conversion of the big list of the identifier information into a simple commitment

$$Com(i_1, i_2, \ldots, i_n; r) = h^r g_1^{i_1} g_2^{i_2} \ldots g_n^{i_n}$$

Sample KYC Template



The high useful property of the Pederson commitment scheme is the additive homomorphism which assumes that different identifying scores (for different information) can be combined to calculate a total KYC score for the user, without the need of decrypting and revealing the information in the middle:

$$Com_{ck}(i;r)\ .\ Com_{ck}(i';r') = Com_{ck}(i+i';r+r')$$

$$\frac{Com_{ck}(i;r)}{Com_{ck}(i';r')} = Com_{ck}(i-i';r-r')$$

After the score is calculated, it can be compared with the requirement of the protocol to see whether a specific user meets the KYC & AML conditions of the system.

The comparison process can be organized by the application of zero-knowledge proof cryptography, which enables to verify whether a particular data meets specific conditions without requiring revealing the plain text. For this type of verification, zero-knowledge proofs are applied (Bulletproofs technology has been selected for that).

If i ∈ Zp and V ∈ G is Pedersen commitment to i using randomness r . The proof generated via Bulletproof scheme shall convince the verifier that i ∈ [0,2n − 1].

R={g,h ∈ G,V,n; i,r ∈ Zp | V=$g^{i}h^{r}$ ∧ v ∈ [0,2n − 1]}

The proof as mentioned in our use case will imply that a particular user complies with the KYC requirements of the lending platforms. The provided scheme can be further optimized via aggregate proofs. It is achieved via the modification of the proof system.

$$R = \{g, h\ \in \mathrm{G}, \qquad \mathrm{V} \in \mathrm{G^m}; \quad v, r\ \in \mathrm{Z_p^m} \mid V_j\ = h^{r_j} g^{v_j} \wedge\ \mathrm{v} \in [0.2\mathrm{n} - 1]\}$$

After proof is generated, anyone can check the accuracy of the proof. The proof itself could be incorporated into the smart contract allowing application of the smart contract for verification, which further opens up new possibilities for the seamless integration into the protocol smart contracts.

7. LITGToken Utility

LITGnative token is the composite part of the whole protocol. On one hand, it acts as a facilitator of the whole economic activity in the system between different agents and creates appropriate incentives to ensure the effective functioning of the whole process, and on the other hand, it is applied as a governance token enabling the efficient, community-driven decision making in the LITGsystem.

LITGEcosystem

LITGserves as one of the main transactional currencies of the platform, enabling lenders and borrowers to enjoy discounted interest rates from the lending system.

Governance Token

Furthermore, the token of the platform will also be applicable for the facilitation of the internal governance mechanism, effectively determining the voting rights of the user in the LITGDAO. As mentioned, a decentralized DAO based approach has been adopted by the system to govern some of the aspects of the Risk Management contract as well as the changes in the DeFi lending and DEX systems. The token is important to enable efficient alignment of the incentives for all the agents of the system to motivate the optimal decision making for the whole LITGecosystem.

LITGtoken will be utilized to make decisions for the overall spec, risk management configuration and decision regarding the introduction of new derivatives strategies for the system.

LITGReward Pool

Furthermore, the protocol token is applied as a staking token designed to facilitate the reward distribution to the participants of the protocol who are ready to provide liquidity to the system. The liquidity provider in the protocol earns LITGtoken, which at the same time they can stake in the Reward pool to get distribution from LITGReward Pool. The reward pools are generated from all the products involved in the LITGsystem (lending

system, derivatives DEX, yield farming, arbitrage bots), where the transaction fees (such as DEX fee, lending fee, infrastructure fee) are accumulated to be distributed to service providers (i.e. liquidity providers).

Overall the platform will have two layers of revenue sharing mechanisms and one layer of liquidity mining mechanism integrated in the system, making it financially rewarding for the participants to stake their funds in the liquidity pool and stake their native tokens for receiving their share from reward pool.
By staking their funds in the liquidity pool, the LPs receive tokens that represent the proportion and the absolute amount of their contribution to the liquidity pool. The system allocates major part of the net return generated using the funds of LPs to them, and when LPs decide to liquidate their funds from the liquidity pool, they will be able to redeem the revenue in addition to their initial stake in the pool. The system by default incentivizes the LPs to keep their funds staked in the pool, as the revenue generation has a compounding effect.

Additionally, the LPs receive fixed daily distribution of native tokens (TPY) in proportion to their contribution to the overall liquidity on the platform. TPY holders will derive significant value from it, the TPY tokens are used for the governance of the platform. Thus with the popularity of the platform and increasing number of LPs the native protocol token will receive a wider distribution among the community, representing ownership and giving proportional votes for participating in the overall governance of the platform.

As a third component to the system, their TPY holders can stake their tokens in the Reward Pool of the platform, and in exchange they will receive daily distribution of the return aggregated in the Reward Pool.

8. LITGToken Economy

Token Name/Ticker	LITG/ TPY
Issuing Company	LITG
Tokens for Sale	
Token Price (USD)	
Minimum Purchase	
Accepted Modes of Payment	

9. Token Distribution

Intended Use	Description	Percentage	
LITG Liquidity Mining Program	Maintenance of Thrupenny Ecosystem and Liquidity	25%	75%
LITG Development	LITGstrategic development and investment	25%	
LITG Backers	Distributed to LITGInvestors and Backers	25%	
LITG Team and Contributors	Distributed to LITGcore contributors with a with a 2-year lock up period, disperese d in 20 % in half a year, 20% after one year, 15 % ever y three months thereafter.	25%	

Disclaimer

This Whitepaper does not represent any financial advice. Any action you take is solely your own responsibility. Cryptocurrencies are extremely volatile, only invest with what you can afford to lose.

This notice is intended to address all readers who view or access it on any communication channel or platform. The Whitepaper is presented strictly for information purposes only, and shall not, under any circumstances be treated as an offer of securities or an invitation to participate in any regulated investment scheme, howsoever defined in any jurisdiction around the world. In addition, none of the information contained herein is intended to form the basis of any advice or inducement to engage in any sort of investment activity.