# Lien L2 Alpha

Lien Protocol

April 2021

## 1 Summary

In April 2021, the Lien team launches an alpha version of our Layer 2 (L2) application. Through this application, we provide an opportunity to trade options (the **solid bond token**, SBT, and the **liquid bond token**, LBT) without paying the high transaction (gas) fees to the Ethereum validators.

In the Lien L2 Alpha, the Lien team serves as an aggregator and handles all the transactions sent via L2. Users can create an account on the L2 marketplace by staking a certain amount of L2 tokens, and transfer their wealth to it by depositing ETH to a smart contract placed on the Ethereum main chain. After that, the users can trade the SBT and LBT with the Lien team as many times as the user likes until the maturity date of options arrives. On the maturity date, the Lien team aggregates all the L2 transactions, and the aggregated transactions are processed in the Ethereum main chain.

While this is an alpha version of our L2 service, and there may exist a risk of unexpected attacks, we do our best to secure the entire procedure using cryptographic technology and minimal trust. To reduce the risk, the implementation is kept as simple as possible, and the Lien team works as an only aggregator and processes all the transaction requests exclusively. These features may be updated later.

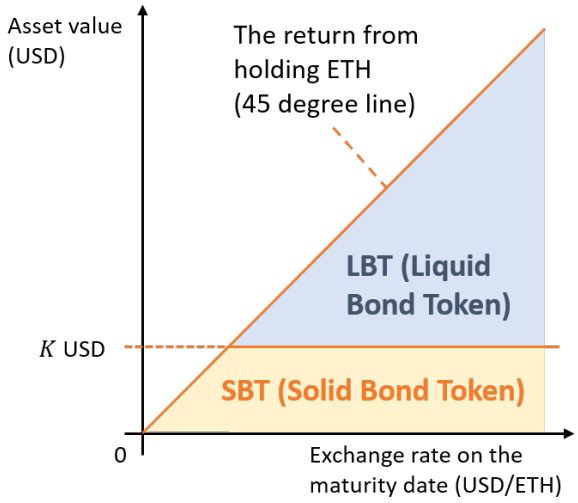


Figure 1: The return from an SBT and LBT.

# 2 How It Works

## 2.1 SBT and LBT

The SBT and LBT are the derivatives generated from ETH. To generate a unit of SBT and LBT, a user must deposit a unit of ETH to a derivative contract. A derivative contract is specified by a maturity date $T$ and a strike price $K$. On the maturity date, the derivative contract refers to the USD/ETH exchange rate (from a trusted oracle) and returns $\max\{K/P, 1\}$ ETH to the SBT holder and $1 - \max\{K/P, 1\}$ to the LBT holder (Figure 1). The return of an LBT is equal to the return of a call option that provides a user with the right to purchase one ETH at the price of $K$ USD.

The strike price $K$ is (typically) selected in such a way that the case of $K/P > 1$ is not likely to occur. Whenever an SBT pays off $K/P$ ETH, its value in USD is $K/P \times P = K$ USD; thus, the value of an SBT is pegged to $K$ USD on most occasions. In this sense, an SBT is a "safer" asset than the ETH itself because an LBT holder is taking a large portion of the price risk. By trading SBT and LBT, users can decide how they take and insure the ETH price risk.

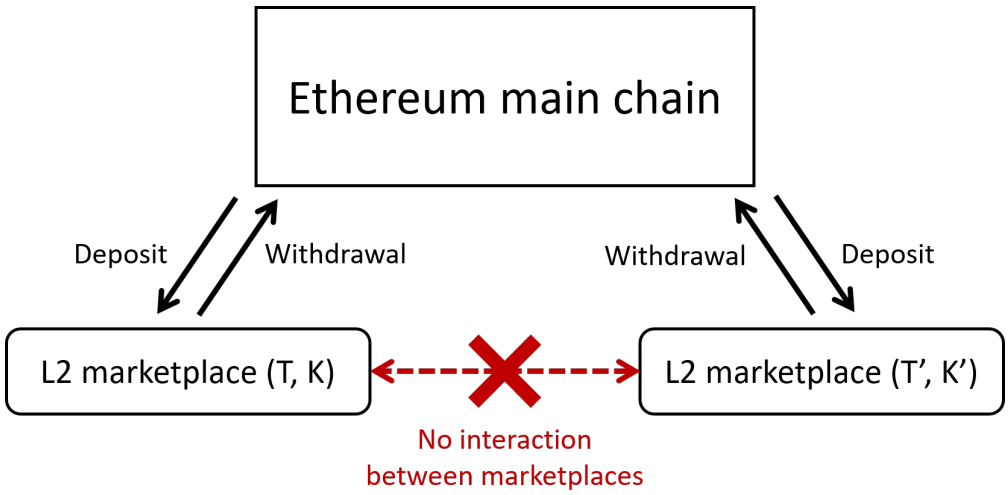


Figure 2: The relationship between the Ethereum main chain and L2 marketplaces.

## 2.2 Marketplace

A **marketplace** is an L2 platform in which users can trade SBTs and LBTs. SBTs and LBTs are specified by the pair of the maturity date and the strike price, $(T, K)$. In the Lien L2 Alpha, marketplaces are opened for each $(T, K)$, and there is no interaction between different marketplaces. A marketplace opens when the maturity date becomes close enough to the current time (in the beginning, we plan to open it two weeks before the maturity date). Once the marketplace is opened, users can join it anytime until the maturity date comes. On the maturity date, the marketplace will be cleared, and the only action users can take is to withdraw their profit.

## 2.3 Actions

In a marketplace, a user can take the following four actions.

### 2.3.1 Registration

To create an **account** on a marketplace, a user needs to stake a certain amount of Lien tokens (as a usage fee). Once the required Lien tokens are deposited (sent) to a smart contract placed in the Ethereum main chain, a **user ID** is issued. The aggregator monitors

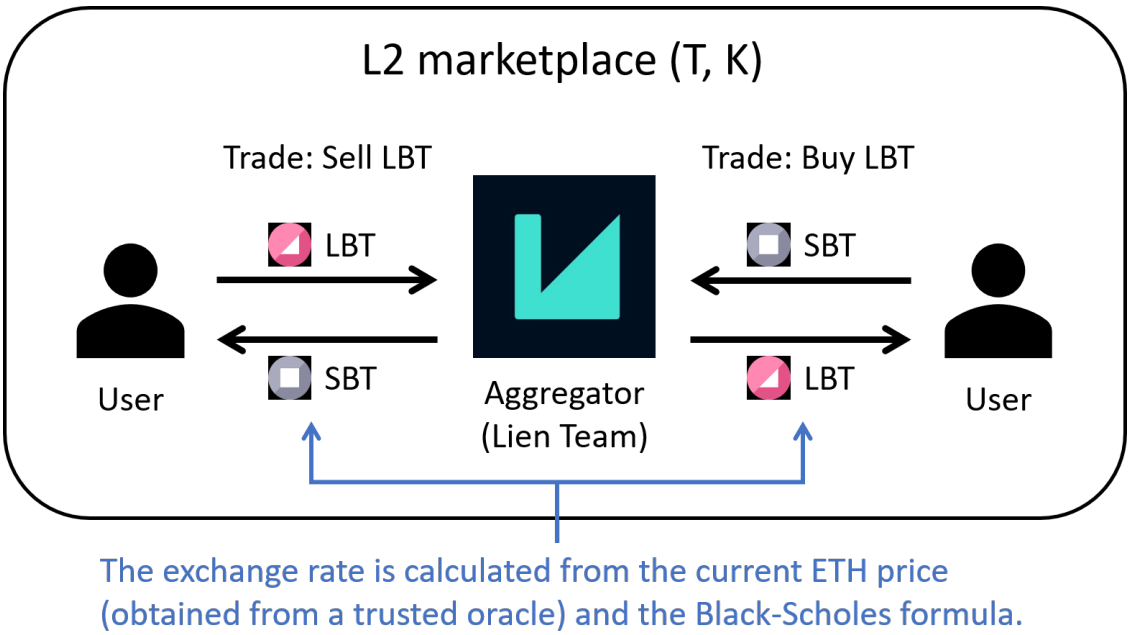


Figure 3: The structure of each L2 marketplace.

the Ethereum main chain and creates a new account on the relevant marketplace. Each registered account is expressed as a **register data** in L2.

### 2.3.2 Deposit

After an account is issued, a user needs to transfer his wealth to the marketplace to start L2 transactions. To do this, a user must send his ETH to a designated contract. The aggregator monitors the amount deposited and adds the tokens to the L2 marketplace. The deposited ETH is automatically split into SBTs and LBTs and added to the user's L2 account. Each deposit information, namely, the account and the amount of the deposit, is expressed as a **deposit data** in L2.

While ETH is deposited until the maturity date, the aggregator can process transactions only when a user submits a valid transaction in L2 (the marketplace). Accordingly, the aggregate can never steal the deposited ETH.

### 2.3.3 Trade

A user can exchange his SBT and LBT with the aggregator. In the Lien L2 Alpha, a user-to-user trade is not allowed; thus, users do not have to worry about the market-making system nor slippage.

When a user submits a transaction request, a user must specify (i) whether he wants to buy or sell LBT (i.e., whether he wants to sell or buy SBT), (ii) the quantity to be traded, and (iii) the Chainlink round ID that specifies the current ETH price (the ETH/USD exchange rate). The set of the round ID and the price is expressed as a **price data** in L2.

Once the aggregator receives a transaction request, the aggregator confirms whether the price and round ID are valid. Then, the aggregator subtracts a fixed percentage of transaction fees (which appears as a bid-ask spread), and calculates the SBT/LBT exchange rate based on the submitted ETH/USD exchange rate and the Black–Scholes formula.

Since the relationship between the SBT/LBT exchange rate and the ETH/USD exchange rate is fixed and disclosed publicly, users can verify whether the aggregator is calculating the rate in a proper manner. Whenever a transaction request is processed, the SBT/LBT exchange rate is calculated based on the ETH/USD exchange rate specified by the transaction request.

### 2.3.4 Withdrawal

Until the maturity date, the L2 marketplace manages users' account balance using a Merkle tree constructed with the hash algorithm "MiMC-7" [1]. Since computation of MiMC-7 is not gas-friendly, if a user directly uses this Merkle tree to verify his account balance to withdraw his profit, he would suffer from a high gas fee. To avoid this problem, in the Lien L2 Alpha, the aggregator reconstruct a Merkele tree using a gas-friendly hash algorithm, Keccak-256. Once the Merkle tree is transformed, users can cheaply verify their account balance. This procedure is called the **tree transformation ceremony**.

After the ceremony, users can verify their account information to withdraw their profit

from the L2 marketplace. Withdrawal is the only transaction a user can execute after the maturity date. After withdrawing his profit, a user can also withdraw his Lien token deposited for creating his account.

### 2.4 ZK-Rollup

As a L2 protocol, we adopted ZK-Rollup. It verifies the validity of the above actions in L2 with zero-knowledge proof systems, which compresses a complex computation into an efficient proof verification. Users can trade their options with almost zero without compromising the security level. [2] is an excellent guide on ZK-Rollup.

### 2.5 Risk Management Protocol

While we do our best to eliminate all the technical troubles, there always exists the risk of bugs, attacks, and other unanticipated troubles. To secure the users' asset, the Lien L2 Alpha starts with a risk management protocol: If a certain time has passed after the maturity date while no one has withdrawn their profit from the L2 marketplace, the Lien L2 Alpha returns all the deposits to all the users. In this case, while all the transactions made in the L2 marketplace is canceled, users can receive their initial deposit.

## 3 Advantages

Here, we list the advantages of the Lien L2 Alpha compared with the other DeFi exchanges located on the Ethereum main chain.

### 3.1 Low Transaction Fee

If a marketplace is located on the Ethereum main chain, users must pay a gas fee to the Ethereum validator every time they submit a new transaction request. Due to the popularity of DeFi, the transaction demand on Ethereum has been increased, and the gas price has

stayed high. The high gas price prevents users from adjusting their positions frequently in accordance with the current market situation because the total amount of transaction fees grows linearly in the number of transactions. This is undesirable because the aim of Lien is to provide users with an opportunity to adjust their risk positions flexibly, depending on the market condition.

The Lien L2 Alpha saves the gas fee by reducing the computation cost to verify transactions and the storage cost to maintain users' last balances. All the transactions sent in L2 are aggregated and the proof to attest their validity is written on the main chain. Instead of directly validating all transactions, a contract simply verifies this proof. Moreover, users' states are committed into a Merkle tree, and only the root of this tree is stored. For these reasons, while users must process a few transactions on the main chain (registration, deposit, and withdrawal), the transaction cost for these actions is significantly lower than that of existing DeFi products.

## 3.2 No Slippage

Most DeFi services decide the price using the market demand and supply directly. Such a mechanism would perform well if transactions were processed immediately. However, since blockchains validate transactions slowly, the market condition could be changed during the submitted transactions are yet to be processed. Consequently, the price when the transaction is processed often differs from the price a user observes when he makes a decision. Such a price difference is called **price slippage** and is well-known as a serious disadvantage of DeFi.

In contrast, the Lien L2 Alpha does not suffer from price slippage. We do not use the demand and supply for SBT/LBT to determine the price. Instead, we look at the price of ETH and derive the theoretical price of SBT/LBT using the Black–Scholes formula. A user can attach the ETH price obtained from a trusted oracle (Chainlink) to the transaction. Whenever the transaction is processed, the SBT/LBT price for the user is calculated from the ETH/USD price attached to the transaction.

### 3.3 No Frontrunning

The structure described in the previous subsection also effectively prevents the frontrunning. Since the price is not directly determined by the demand and supply of the marketplace, a user's transaction will never change the price. Accordingly, the well-known frontrunning attack, which is possible and actually executed in many DeX (such as Uniswap), is impossible in the Lien L2 Alpha.

## References


[1] Jordi Baylina and Marta Bellés. Eddsa for baby jubjub elliptic curve with mimc-7 hash.

[2] Vitalik Buterin. An incomplete guide to rollups, 2021. https://vitalik.ca/general/2021/01/05/rollup.html.