# **ICLighthouse DAO**

## ICDex: A fully on-chain order book DEX on the IC

V1.1

By ICLighthouse Team

January 24, 2024

ICLighthouse DAO Whitepaper

# **1.Introduction**

## 1.1 ICLighthouse DAO

ICLighthouse DAO is a community-driven on-chain governance contract initiated on the Internet Computer SNS system by ICLighthouse. It governs ICDex and icRouter.

## ICDex

ICDex is a dApp within the ICLighthouse DAO. It's a fully on-chain order book DEX project built on the IC blockchain, with core code contributed by ICLighthouse and its development driven by the community. Governance is conducted through the ICLighthouse DAO SNS.

The Exchange Mode of ICDex includes Tunnel Mode and Pool Mode. New traders default to Tunnel Mode, where each trade order has a dedicated account (TxAccount), creating a 'Tunnel' for locking and exchanging funds. In Pool Mode, funds from all trade orders are locked in the trading pair pool (PoolAccount), and funds are transferred to the receiver when orders are matched. Tunnel Mode offers higher security, while Pool Mode provides greater efficiency. Advanced functions like Strategic Orders require Pool Mode.

ICDex incorporates a diverse range of trading features to enhance user experience and efficiency. Its order book matching engine supports four distinct types of orders: Limit (LMT), Market (MKT), Fill and Kill (FAK), and Fill or Kill (FOK). In addition to these basic order types, ICDex introduces its Strategic Order feature, which includes advanced options like Stop-Limit-Orders and a suite of Pro-Orders. The Pro-Orders consist of Grid Orders, Iceberg Orders, Time-Weighted Average Price (TWAP) Orders, and Volume-Weighted Average Price (VWAP) Orders. Further enhancing its functionality, ICDex features an Orderbook Automated Market Maker (OAMM). OAMM uniquely addresses the challenges of automated market making in order book decentralized exchanges (DEXs) by employing Grid Strategic Orders, thereby simplifying the process for liquidity providers (LPs) to contribute liquidity to the platform. This comprehensive set of features positions ICDex as a versatile and advanced trading platform in the cryptocurrency market.

## icRouter

icRouter is another dApp within the ICLighthouse DAO, facilitating decentralized

trading of multi-chain assets on ICDex. It's a cross-chain network of assets, leveraging threshold signature technology, and operates without off-chain bridges. This supports a range of networks including Bitcoin, IC, and EVM networks (such as Ethereum). Note: icRouter is still in the stages of refinement and testing. Therefore, the content of this version of the whitepaper primarily describes ICDex.

## **1.2 Internet Computer**

The <u>Internet Computer</u> (IC) is a decentralized global compute platform which uses ground-breaking blockchain technology to achieve consensus within subnets. It is globally distributed in numerous independent data centers, is tamper proof and unstoppable.

It can serve applications fully on-chain without needing any centralized frontend layer. It is extremely efficient and is several orders of magnitude cheaper to run and store data than most other blockchains. It uses a reverse-gas model so computation and storage costs are paid by the app/service providers rather than users.

#### **Canister smart-contracts**

Applications on the IC are composed of canister smart-contracts organized into subnets. A subnet can contain 100,000s of canisters and is composed of (typically 13) node machines each of which runs in a different independent data center around the globe such that the nodes within each subnet are as geographically and jurisdictionally diverse as possible. Canisters can communicate securely with canisters on other subnets allowing the IC to scale horizontally.

A canister runs on a virtual machine (as a WASM) that is replicated across a subnet. It implements the actor model, and so is single threaded, processing a queue of input messages one at a time, optionally sending messages to other canisters, and adding a response message to an output queue.

It can be called by clients (or other canisters) using queries or updates. A query can be served immediately from any node but cannot change state. An update can change state and goes through a process of consensus for the nodes to agree on the same result before responding to the caller. Achieving consensus is where the blockchain comes into play but is beyond the scope of this document.

Canisters have the property of orthogonal persistence which means as a programmer you just write data objects to memory and they are automatically persisted by the system. This removes the need for a database and is one of the reasons writing and running applications on the IC is simplified compared to traditional IT stacks.

#### Network Nervous System (NNS)

A key feature of the Internet Computer blockchain is the Network Nervous System (NNS), an open algorithmic governance system that oversees the network and the token economics.

Read here for more information on the NNS.

#### Service Nervous System (SNS)

A Service Nervous System (SNS) is an advanced form of a DAO. A digital democracy that can run any dApp such as a social network in a fully decentralized way, fully on chain. No corporation, no board of directors, no CEO required. Read <u>here</u> for more information on the SNS.

## **1.3 ICLighthouse Team**

Based in Singapore, the ICLighthouse Team is the foundational development group of this project. Key contributors to the project's code repository, the team consists of IC ecosystem developers, Ethereum ecosystem experts, and finance industry professionals. Known as a committed builder in the IC ecosystem, the ICLighthouse Team has been awarded multiple grants from the Dfinity Foundation's Developer Grant Program for projects like ICTC, ICDex, icRouter, among others. In January 2023, they achieved second place in the Singapore Blockchain Innovation Programme (SBIP) Hackathon.

# 2. Market Background

## 2.1 Market Background of DEX Evolution

The prominent usage of DEX platforms today begins roughly back in the 2017-2018 crypto frenzy with the rise of self-custody platforms like EtherDelta (now defunct) and similar smart contract orientated exchanges. These exchanges really brought the concept of being able to trade while still retaining full control of your funds to the average crypto user by not only having a strong security proposition but also by having less red tape in listing new assets due to the more free and open nature of these decentralized platforms. With new ICOs happening all the time during this period and performance often being wildly speculated on for these new assets it drove massive volumes to DEXs and laid the groundwork for them to become a staple in the cryptocurrency ecosystem.



Above we can see the meteoric rise of value locked in the EtherDelta smart contract during this time period

As these platforms gained prominence the choking points began to reveal themselves. Namely gas costs, tx processing times due to spikes in gas fees, and slow loading times due to heavy loads on off-chain components of the architecture.



Following this rise of Orderbook DEXs new platforms such as Uniswap emerged using a different model: Automated Market Maker (AMM) which removed the need for a lot of these off-chain components used by platforms such as EtherDelta because they no longer offered or required orderbooks. Instead, users would trade liquidity available in a pooling contract to buy or sell at market price. And while this did prove to increase reliability of the DEX in relation to the infrastructure without compromising security it didn't help to alleviate the need of traditional web hosting or tackle the problem of extreme gas costs and trans-actions being stuck pending long periods of time since these are things which began to prove unavoidable on Ethereum as a whole.



Historical DEX volume on Ethereum

With these massive growth rates and strong interest in the ecosystem there's no doubt De-centralized Exchanges like these are here to stay. And strongly believing this to be true, a goal of tackling these problems ourselves without compromising on UX and security is what drove the inspiration for ICDex and other critical DeFi tools we've built here at ICLighthouse.

With ICDex being built on the IC we've managed to provide the full experience of a centralized exchange while being entirely on-chain and offering the same self-custody security prospects DEX users have come to trust and love without the risk of extreme fees regard-less of network load.

Through the launch of ckBTC and ckETH by Dfinity and added support for these assets on icRouter (our cross-chain swapping tool) we aim to bridge the gap in liquidity between these chains easier and safer than ever— unlocking the true potential of the IC and paving the way for platforms like ICDex to become prominent in the seemingly inevitable boom of next generation decentralized platforms.

## 2.2 So what makes ICDex stand out from it's competitors?

ICDex has a unique exchange structure which noticeably stands out from its competition in the ecosystem. Unlike most DEX trading platforms, which are largely AMM swapping platforms, ICDex has a much smoother CEX like trading experience and offers the benefit of live orderbooks and multiple order types to give users the option to trade at something other than the current market price. And given the technological advancements of the IC network we're able to provide these features entirely on-chain and without the same choking points faced by similar Ethereum based decentralized exchanges in relation to gas fees and off-chain architecture.

AMM-style platforms often present challenges in predicting and estimating price levels

where buying or selling interest might peak. This difficulty arises because trades can only be initiated at those specific price levels. In contrast, ICDex offers a more sophisticated approach, providing experienced traders with tangible and clearer metrics that can significantly enhance their trading strategies.

At the heart of ICDex's innovation is its Orderbook Automated Market Maker (OAMM), which effectively tackles the challenges associated with automated market making in order book DEXs. The OAMM system utilizes a Grid Strategy based order mechanism. This de-sign not only simulates the effects of a traditional AMM but also streamlines the process for Liquidity Providers (LPs) to supply liquidity to ICDex. By integrating these advanced features, ICDex enhances the predictability and understanding of market movements, offering a more professional and strategic trading environment.

Among the classic "Limit" and "Market" order types we offer two more advanced order types "Fill and Kill" and "Fill or Kill". With these 4 types available most traders from new to experienced should find their styles and strategy supported here. In our team's long and dedicated history in the crypto markets we've found that most traders prefer these types of trading options and we believe historically the reason AMM platforms outperformed the orderbook DEXs of the day was simply due to the expensive costs to operate on these plat-forms and the limitations off-chain infrastructure imposed.

To further cater to the needs of sophisticated traders, we also implemented strategic order options. This feature allows traders to create more nuanced and complex trading strategies, leveraging our platform's advanced capabilities.

# **3. Order Book DEX Protocol**

## 3.1 icRouter

icRouter is a cutting-edge, bridgeless cross-chain network, leveraging threshold signature technology to connect Bitcoin, IC, and EVM networks such as Ethereum, enhancing security and interoperability in the blockchain space.

#### icRouter



icRouter is currently in its refinement phase. The next stage will introduce the integration of Bitcoin and Ethereum networks. Details will be provided in the upcoming version of the whitepaper.

## 3.2 ICDex

ICDex, a sophisticated order book DEX, is constructed on the IC network and adeptly accommodates both ICRC1 and DRC20 token standards.

## 3.2.1 Infrastructure

The ICDex project comprises three main components: ICDexRouter, ICDexPair, and ICDexMaker.

#### **ICDex Infrastructure**



Governed and controlled by the SNS, ICDexRouter acts as a Factory, responsible for creating and managing both ICDexPair and ICDexMaker.

## **3.2.2 Accounts and Roles**

Traders are identified by `AccountId` within the pair and support subaccounts. Each account may fulfill one or more of the following roles:

• Trader (User):

An ordinary trader, requiring no authorization.

• Maker:

A trader who places an order into the order book leaving it open for another trader to fill thereby increasing liquidity and assuming the Maker role for that order.

• Taker:

A trader who places an order that immediately matches with existing orders, thereby removing liquidity, and is designated the Taker role for that order.

• Vip-Maker:

Granted by ICDexRouter, this role allows a trader to receive a trading fee re-bate, specified as a percentage, when acting as a Maker.

• Trading Ambassador (Referrer):

A trader with a trade volume greater than 0 can become a Trading Ambassador without specific authorization. They can refer new users to the trading pair, with their referrals and the total trade volume of these referrals being tracked.

• Broker:

Other dApps can integrate with ICDex as a 'Broker', By specifying the broker parameter when using the trading API, they can earn commissions paid by the Taker. No authorization is required for the Broker role.

• Pro-Trader:

A Trader utilizing the Strategy Orders feature is called a 'Pro-Trader'. This role

also requires no authorization.

Dedicated accounts within the trading pair include:

#### • TxAccount:

Specifically allocated for each order in tunnel mode, this account temporarily holds funds for the order. It remains in a locked state until the order is either filled or canceled, preventing the transfer of funds to the recipient beforehand. Every order maintains a distinct TxAccount, identified by the address { owner = pair\_canister\_id; subaccount = ?txid }. In exceptional cases, funds remaining in a TxAccount can be reclaimed through a fallback operation.

#### • PoolAccount:

This central account for trading pairs is utilized to hold temporary funds for all orders collectively. Its ownership and status are regulated by the records in the TraderAccount ledger, for example, { owner = pair\_canister\_id; subaccount = null }.

#### • TraderAccount:

Functioning as the local ledger within a trading pair, it tracks the balances traders maintain in the PoolAccount. Balances in the TraderAccount are categorized into locked and available sections. Traders can adjust their available balance by depositing or withdrawing funds. The TraderAccount does not directly hold tokens; instead, balances are accessible through the accountBalance() and safeAccountBalance() methods of the trading pair.

#### **DepositAccount:**

This is a temporary account used by traders to deposit funds into the available balance of their TraderAccount. Each trader possesses an individual DepositAccount, specified by { owner = pair\_canister\_id; subaccount = ?accountId }. In case of anomalies, funds left in the DepositAccount can also be recovered through a fallback operation.

## 3.2.3 On-Chain Orderbook Matching Engine

The matching engine differentiates between incoming orders and book orders. An incoming order is currently being entered, while a book order is already placed in the order book.



To conceptualize a matching engine, think of it as a specialized function operating in a sequential manner. Firstly, it accepts two key inputs: an order (1) and an "order book" (2). Upon processing these inputs, the engine outputs two critical components: a list of completed trades (3) and a collection of all resting orders (4). These resting orders are then assimilated into the "order book," serving as the basis for processing the next incoming order by the matching engine. This cyclical process ensures continuous and efficient order matching in the trading environment.

#### **Matching principles**

ICDex Orderbook employs the First-In-First-Out (FIFO) algorithm for its matching engine. This price-time algorithm prioritizes buy orders by price and then time. Buy orders with the same maximum price are further prioritized based on the time of bid, with the earliest bid receiving precedence.

### **Order Types**

ICDex Orderbook supports various order types including Limit (LMT), Market (MKT), Fill-And-Kill (FAK), and Fill-Or-Kill (FOK) orders.

• LMT:

A Limit Order lets you set a specific price for buying or selling an asset. You can place a Limit Buy Order to buy at a price below the current market value or a Limit Sell Or-der to sell above the current market value.

#### • MKT:

A Market Order facilitates immediate buying or selling at the current market price. This order type ensures execution but may be partially canceled if insufficient matching orders exist.

• FAK:

A Fill and Kill Order is ideal for bulk orders at a set limit price, with any unfilled portion being canceled post-execution.

• FOK:

A Fill or Kill Order must be executed in full immediately or not at all. It can match with multiple existing orders, resulting in several trades, but is never displayed in the order book.

## **3.2.4 Exchange Mode**

ICDex offers two main trading modes: Tunnel Mode and Pool Mode. New traders automatically use Tunnel Mode, while more advanced options like Strategic Orders need Pool Mode.

### **Tunnel Mode:**

When a trader places an order, the funds are deposited into an order-specific account known as `TxAccount` (Order Tunnel Account). Funds are transferred from this account to the counterparty's account only upon the order's fulfillment or cancellation. Each order is associated with a distinct Tunnel, identified by { owner = pair\_canister\_id; subaccount = ?txid }.

TunnelMode



#### **Pool Mode:**

When a trader places an order, the funds are deposited into the pool account of Trading Pair ('PoolAccount'). On order fulfillment, funds move from the Pool to the

counterparty's account. The PoolAccount is defined as { owner = pair\_canister\_id; subaccount = null }.



## 3.2.5 Strategy Orders

Strategy Orders, also termed Algorithmic Orders, allow traders to set parameters based on the trading pair's strategy rules. When market prices align with these conditions, the trading pair autonomously places orders for the trader. These are categorized into Pro-Order and Stop-Limit-Order.

Pro-Order supports Grid Order, Iceberg Order, TWAP Order, and VWAP Order. Among these, the Grid Order is fundamental to the implementation of the Orderbook Automated Market Maker (OAMM)

The strategy order lifecycle comprises two phases:

- 1) Strategy Configuration: Pro-traders select a strategy, configure its parameters, and initiate it.
- 2) Order Triggering: When the latest price in the trading pair aligns with the strategy order's conditions, the Strategy Manager (Worktop) automatically triggers the order.

Notes:

- Ordinary orders may trigger a strategy to place an order when they are filled, while strategy orders will not trigger a strategy to place an order again.
- Strategy triggers do not guarantee immediate or successful order placement, subject to multiple uncertainties.
- In busy times, trigger prices may deviate, leading the system to ignore frequent triggers in a short span and execute only once.

## 3.2.6 IDO (Initial DEX Offering)

IDO is a token sale mechanism at the onset of a token's listing on ICDex, authorized by the owner (DAO) and set up by the Funder of the base token. Only trading pairs created through the owner (DAO) can initiate IDO.

### **Configuration:**

- Opening IDO: The Owner (DAO) uses the IDO\_setFunder() method to start IDO, set participation thresholds, and designate the Funder.
- Funder Configuration: Funder uses the IDO\_config() method for setup, including IDO timing, whitelist, tiered supply rules, and participation limits.

### **Tiered Pricing Framework:**

• The Funder determines the total supply for IDO and sets multiple price levels for tiered supply, with purchases prioritizing the lowest priced tiers on a first-come, first-served basis within set limits.

### **IDO Timeline:**

- Setting IDO Times: The Funder sets IDOOpeningTime, marking the trading pair's launch, and IDOClosingTime, indicating the start of official trading.
- **Pre-IDO Adjustments:** Up to 24 hours before IDOOpeningTime, the Funder can modify IDO settings if no orders exist.
- Order Placement Before IDOOpeningTime: The Funder places Sell-side LMT orders based on the tiered supply data, with the option to set whitelists and participation limits.
- **IDO Active Period:** From IDOOpeningTime to IDOClosingTime, users can buy tokens within the participation limit through Buy-side FOK orders.
- **Post-IDOClosingTime:** Any unfilled orders are canceled, and normal trading begins.

### **Participation Limits:**

- Whitelist Mode: If used, only people on the whitelist can buy and optionally limited to a certain amount.
- **Non-Whitelist Mode:** Without a whitelist, any eligible account can participate in IDO.
  - Eligibility for Participation: The eligibility criteria for IDO participation are determined as follows:

1). If the ICDexRouter sets the participation threshold at zero (threshold=0) during IDO activation, it implies that all users are eligible for participation.

2). Conversely, if the ICDexRouter establishes a non-zero threshold (threshold>0), a user's eligibility is contingent on their trading volume in specified pairs, converted to USD, sur-passing this threshold. Should a user's

trading volume fall short of the threshold, the Funder has the discretion to assign a whitelist quota to the user, thereby granting eligibility.

 Participation Limit:
 Eligible participants are entitled to purchase tokens up to a predefined limit. In cases where a user has been allocated a whitelisted quota, this specific quota takes precedence, dictating the maximum number of tokens they can acquire.

## 3.2.7 Orderbook Automated Market Maker (OAMM)

The Orderbook Automated Market Maker (OAMM) serves as a liquidity pool for trading pairs, employing a grid strategy in the order book to automate market making. This approach is akin to that of a traditional AMM.

#### Settlement:

When liquidity is added or removed, both the Net Asset Value (NAV) and the shares are recalculated. This calculation involves fetching the liquidity asset amount each time and adhering to the following formula as a guideline:

NAV / shareUnitSize \* shares = total liquidity

#### Grid strategy for market-making:

ICDexMaker uses a grid strategy for market-making, recognized for its simplicity and effectiveness.

We've taken inspiration from the AMM model of Uniswap, which uses a variant of this grid strategy where-in the grid interval is infinitesimally small. To ensure decentralized, long-term execution, strategy parameters are set as relative values, minimizing the need for manual adjustments. Key parameters include:

- gridspread = #Geom(gridSpread). The grid spread is configured as a ratio (ppm).
- gridamount = #Percent(null). The quantity (amount) of orders traded per grid is configured as #Percent and is specified as null, indicating that the proportion takes the value ppmFactor.

ppmFactor: Default grid order amount factor, initialized when the strategy is created.

$$ppmFactor = 1000000 * \frac{1}{n} * \left(n * * \left(\frac{1}{10}\right)\right)$$

Where n is (n1 + n2) / 2 and n1, n2 is be-tween 2 and 200. n1 is the number of grids between the latest price and the lowerLimit, and n2 is the number of grids between the latest price and the upperLimit.

### **Liquidity Limit**

ICDexMaker initially adds liquidity without a cap. Once the token1 balance in total liquidity hits `threshold`, a liquidity limit rule is activated. A user's liquidity cap (measured in token1) = the user's token1 volume in the current pair \* volFactor.

Note: Threshold and volFactor are defined at the creation of ICDexMaker. This mechanism is in place because, in popular market-making pools with many users adding liquidity, the yield decreases. To prioritize higher-contributing users, the liquidity cap is based on the user's trading volume in the pair.

### LP Yield

LPs may benefit from adding liquidity to the liquidity pool, but it is risky and does not result in a stable gain or may result in a loss. Possible gains include:

#### • Grid Spread Gain:

By opening a grid strategy in the trading pair, ICDexMaker profits from the spread between grids during price fluctuations. However, unidirectional price movements can lead to imbalances in token quantities, affecting spread gains. Therefore, grid spread gain is correlated with the trading pair's volatility.

• Vip-Maker Rebate:

As a Vip-maker, ICDexMaker earns a trading fee rebate, which con-tributes to the liquidity pool.

#### • Withdrawal Fee from Liquidity Removal:

LPs are charged a withdrawal fee when re-moving liquidity, which is added to the pool.

#### • Liquidity Mining/Airdrop:

This is a potential benefit. ICDexMaker does not inherently provide liquidity mining or token airdrops; these require the development of an additional liquidity mining canister.

# 4. Governance

ICLighthouse DAO represents a novel approach to governing and operating the dApp, ICDex, intended to function as a public good without ownership by any specific entity. The DAO's operational oversight is facilitated through the utilization of SNS canisters and an SNS subnet, providing a secure and reliable infrastructure for dApp governance. The establishment of this DAO and its associated activities hinge on the successful approval of proposals submitted to the NNS (Network Nervous System), which is the governance framework of the IC blockchain and has been operational for several years.

The process of initiating the ICLighthouse DAO involves submitting a proposal to the NNS, outlining parameters such as neuron specifications, parameters for decentralized sales, and initial token distribution. Upon acceptance of this proposal, the NNS will commence the de-centralized sale of ICL tokens based on the specified parameters, transferring governance control to the public and raising funds to be allocated by the community through the SNS-treasury. The sale of ICL tokens is designed to decentralize governance control and encourage broader community participation.

After the successful establishment of the ICLighthouse DAO (SNS), control of the existing ICDex canister will transition from the founding development team to the SNS, ensuring that only the SNS has the authority to modify the ICDex platform. This approach underscores the DAO's commitment to decentralized governance and enhances trust and security among users.

### 4.1 Governance Structure

ICLighthouse DAO adheres to the governance structure of the SNS:

- The ICL token is deployed by the SNS system. The ICLighthouse DAO SNS cannot modify the token's key characteristics through proposals but can follow SNS system up-grades to update the token's WASM version.
- Canisters of the dApp transfer control to the ICLighthouse DAO SNS. Management per-missions for the dApp are exercised through proposal initiation, or by granting/modifying certain operational rights to specified accounts via proposals.

Given the specific nature of DeFi projects, which often require timely intervention by governors, the SNS proposal mechanism might not always be timely. Therefore, we have designed the DAO Board (ICDAO) system as a complement to the SNS, enabling rapid response to DEX-related matters. The DAO Board (ICDAO), controlled and upgraded by the SNS, is authorized only for functions with lower security implications.



#### ICLighthouse DAO Governance

ICLighthouse DAO Whitepaper

## 4.2 DAO Board Governance

The DAO Board's functions and responsibilities within the ICLighthouse DAO are governed and managed by the SNS, meaning the SNS authorizes the DAO Board to handle certain aspects of dApp governance through Lightning Governance Proposals (LGPs), facilitating rapid responses to time-sensitive matters.

Members of the DAO Board, known as Keepers, are selected from holders of neurons with the highest ICL lock-up, or directly appointed by the SNS. The number of Keepers, typically set at 17 (with 5 appointed as team members by the SNS), is determined by the SNS.

Individuals who own neurons and aim to become Candidate Keepers must register with the DAO Board. This registration necessitates a dissolution delay exceeding one month for their neurons. Every 48 hours, the DAO Board queries the SNS for neuron information of all Keeper candidates, ranking them based on voting power and an engagement score (0 to 1) for selection. When the SNS appoints a new Keeper, the total number of Keepers may temporarily exceed the set limit until the next update.

Keepers are responsible for processing LGPs designated by the SNS. They cannot upgrade dApp canisters, only API specified in the DAO Board code. This mechanism is intended to constrain the DAO Board's authority.

DAO Board voting follows a "one person, one vote" rule, distinguishing it from SNS proposal voting. For LGPs, different passing thresholds are set: 50% for LGPs without financial risk and 75% for those with potential financial losses.

Participation evaluation for Keepers involves scoring them from 0 to 1 for each LGP, with an average score determining their participation rating. New Keeper candidates start with a default score of 0.5. The advantage of being a Keeper includes becoming an RPC provider for the icRouter, entailing rewards from the icRouter.

### **SNS Proposal Principles**

• Security as a Top Priority:

Always place the utmost emphasis on security in all aspects of the SNS.

- Focus on Long-Term Value:
   Prioritize initiatives that promise enduring value to the ecosystem.
- Token Listings Strategy:
  - Standard Procedure: Project teams are expected to form pairs and enhance their standing through operational excellence.

- Expedited Listings: Tokens that promise significant user influx or introduce unique pairings to the ecosystem may be fast-tracked via SNS proposals.
- Utilization of ICP in the Treasury:
  - Main Uses: Allocate primarily for bolstering security and liquidity.
  - Funding Policy: The founding team is committed to not withdrawing ICP for development expenses.

#### • Neutral Approach to Projects:

- Equitable Treatment: Maintain impartiality towards both emerging and established projects.
- Fair Resolution: Address issues within dApps through just and balanced rules.
- Slight Advantage: Projects on the SNS might receive a slight edge, acknowledging their role in enriching the IC ecosystem.

#### • Fee Rate Strategy:

- Balanced Approach: Consider the average fees in the DEX industry while being mindful of on-chain resource limitations.
- Avoiding Congestion: Avoid setting excessively low fees to prevent transactional bottlenecks.

#### • IDO Proposal Voting:

• Developer Stance: The development team will generally refrain from participating in voting on IDO proposals.

#### • OAMM Creation Proposals:

- Holders of #NEPTUNE, #URANUS, #SATURN NFTs can initiate an OAMM, but must spend a specified amount of ICL as a fee.
- Non-NFT holders initiating an OAMM are required to spend ten times the specified amount of ICL as a fee.
- Voting Policy: The development team will usually abstain from voting, except for the first project-side proposed OAMM, which will receive unanimous support.

#### • VIP-maker Qualification Proposals:

- Acquisition Method: Typically granted through #NEPTUNE NFT binding.
- Voting Tendency: Favor proposals granting VIP-maker status to OAMMs established by the SNS treasury, while generally opposing others.

# **5.** Tokenomics

The ICLighthouse DAO Token (ICL) is the governance token of the ICLighthouse DAO and also serves as the utility token for the project ICDex. ICL is an ICRC1 token issued on the IC network, used for governance, as gas for dApps, and for ecosystem incentives, among other purposes.

#### Tokenomics



The goal of this economic model is to embody a decentralized utility-focused deflationary model in reality.

#### **Token Information:**

Name:	ICLighthouse DAO
Symbol:	ICL
Token Standard:	ICRC1
Decimals:	8
Total Supply:	Approx. 210,000,000 (The supply without SNS voting rewards is 200,000,000)

## 5.1 Token utility

The ICL token will be utilized for governance, as gas for dApps, to incentivize contributors to the dapp and DAO, and to establish reserves for security and long-term development.

The uses of ICL reserved in the SNS treasury include the Eco-Incentive Reserve, Risk Reserve, and Strategic Reserve.

### **Participation in Governance**

ICL enables community governance of dApps through the SNS system. For more details, please refer to the '4. Governance' section.

### Used for gas in the dApp

To maintain the economic balance of the dapp ecosystem, conserve on-chain computational and storage resources, and prevent certain types of attacks, dApps have implemented a mechanism that uses ICL as gas for certain functionalities. This includes, but is not limited to, specific rules that may change due to dapp upgrades or DAO governance:

- Creating trading pair (TP) fee: The user creates a trading pair and will be charged creatingPairFee (initial value is 5000 ICL).
- Creating order-book automated market maker (OAMM) fee: The user creates an order-book automated market maker and will be charged creatingMakerFee (initial value is 50 ICL).
- Trading fees: Traders are charged in ICL or other tokens as fees when conducting transactions in trading pairs. The fee structure includes:
- Maker-fee: When a trade order is filled, the maker pays a fee based on the amount of the filled order, and its rate is currently 0% by default. A negative value means that the maker receives a commission (Vip-maker rebate).
- Taker-fee: When a trade order is filled, taker pays a fee based on the filled amount, and fee rate is currently 0.5% by default. Taker-fee after subtracting Vip-maker rebate is used as gas consumed by dapp.
- Cancelling-fee: An order canceled within 1 hour of placing it will be charged a fee (Taker\_fee \* 20%) if nothing is filled, this fee is limited to a range from `token fee \* 2` to `token fee \* 1000`.
- Strategic order fee:
  - Pro-order fee: When configuring a pro-order strategy, traders are charged a fixed amount of ICL as a fee (poFee1) and the fee for updating the strategy is poFee1 \* 5%. Vip-maker is not be charged poFee1. When the strategy is triggered and the new trade order is closed, the trader is

charged the amount of tokens (token0 or token1) he receives multiplied by the rate (poFee2) as a pro-trade fee.

2) Stop-limit-order fee: When configuring a stop-limit-order strategy, traders are charged a fixed amount of ICL as a fee (sloFee1) and the fee for updating the strategy is sloFee1 \* 5%. Vip-maker is not be charged sloFee1. When the strategy is triggered and the new trade order is closed, the trader is charged the amount of tokens (token0 or token1) he receives multiplied by the rate (sloFee2) as a stop-limit-trade fee.

It is suggested (but not mandatory) that 30% of the gas fees collected by the dapp be allocated to the Risk Reserve, 10% to the Eco-Incentive Reserve, 10% to the Strategic Reserve, and the remaining 50% be converted to ICL and transferred to a burn address for destruction.

#### **Eco-incentive**

The DAO incentivizes contributors who improve the dapp ecosystem and DAO governance through rewards or airdrops, including:

- Contributor rewards or airdrops
- Trading mining rewards
- Liquidity rewards
- Trading competition rewards

Funds from the Eco-Incentive Reserve in the SNS treasury are withdrawn and used as per the operational plan through proposals.

#### **Other Reserve Uses**

The Risk Reserve in the SNS treasury is solely for compensating user asset losses due to dapp security incidents.

The Strategic Reserve in the SNS treasury is used for purposes beneficial to the project's development, such as providing liquidity, partnership rewards, and future financing for the core team.

## 5.2 Initial token allocation

Total supply is approx. 210,000,000 ICL (The supply without the SNS voting rewards is 200,000,000), The initial allocation of ICL is as follows:

	Supply	Percentage	Note
Voting Rewards	10,000,000	4.762%	Will be minted during
	, ,		future governance.
Treasury	76,100,000	36.238%	
- DRC20 Swap & NFT Airdrops	4,200,000	2%	Conversion for
1 1	, ,		DRC20 ICL holders
			and NFT airdrops.
- Eco-Incentive Reserve	25,200,000	12%	For eco-incentives
			such as trading
			mining, liquidity
			rewards, airdrops,
			community
			contributions, and
			more.
- Risk Reserve	21,000,000	10%	For security and risk-
			related expenditures.
- Strategic Reserve	25,700,000	12.238%	For liquidity and
			future financing.
Early Investors	29,400,000	14%	
- Early contributors & donors	14,700,000	7%	
- Seed round	14,700,000	7%	
Team	31,500,000	15%	
SNS Swap	63,000,000	30%	
Total	210,000,000	100%	

#### **Token allocation**



#### Voting Rewards (4.762%)

The total amount of voting rewards for SNS governance is expected not to exceed 4.762% (10,000,000 ICL) of the total supply. These rewards are not minted at the start of SNS. Once SNS governance begins, the initial voting rewards are set at 2.43%. The reward rate will decrease quadratically from 2.43% to 0% over a span of 6 years.

#### Treasury (36.238%)

The ICL held in the SNS Treasury accounts for 36.238% (76,100,000 ICL) of the total supply. The allocation includes DRC20 swap & NFT airdrops of 4,200,000 ICL, 25,200,000 ICL for the Eco-Incentive Reserve, 21,000,000 ICL for the Risk Reserve, and 25,700,000 ICL for the Strategic Reserve.

*Note: The implementation of these Treasury plans requires completion through formal proposals.* 

- 1) DRC20 swap & NFT(2%): Before the launch of SNS, 2% (4,200,000 ICL) of the total supply is airdropped to the community. This includes 2,962,000 ICL for the airdrop plan of the NFT collection 'ICLighthouse Planet Cards' and approximately 1,238,000 ICL already airdropped for early community activities (to be converted to ICRC1 tokens after the launch of SNS). This ICL is not subject to a lock-up period, but requires technical development, which will be completed within 3 months after the launch of SNS.
- 2) Eco-Incentive Reserve (12%): The ICL in the Eco-Incentive Reserve is used for ecosystem incentives in conjunction with operational activities. The maximum quarterly distribution for the first three years should not exceed 0.5% (1.05M ICL) of the total ICL supply, and thereafter, the quarterly distribution should not exceed the lesser of 0.5% of the total supply and the quarterly burn rate (total\_supply \* min(0.5%, burn\_rate)).
- 3) Risk Reserve (10%): This balance will be maintained long-term, with a portion of the trading fees continuously transferred to this account. In the event of a security incident, if the ICP in the Risk Reserve is insufficient to cover losses, a proposal can be made to auction the ICL in the Risk Reserve to continue compensating users.
- 4) Strategic Reserve (12.238%): This balance will also be maintained longterm, with a portion of the trading fees continuously transferred to this account. Approximately 50% of the ICL in the Strategic Reserve can be used to provide liquidity after listing on trading pairs. It also offers financial support for significant external partnerships, future fundraising for the core team, and other strategic initiatives.

### Early Investors (14%)

Prior to the launch of SNS, 14% (29,400,000 ICL) of the total supply of ICL was allocated due to early-stage fundraising for the project, divided into two parts:

- Early contributors & donors (7%): During 2020-2021, in the initial phase of the project, donations and contributions for work services were accepted from specific entities. This resulted in the allocation of 7% (14,700,000 ICL) of the total supply, distributed across five neurons with dissolve delays of 0 months, 3 months, 6 months, 9 months, and 12 months.
- Seed round (7%): In 2023, the team completed a seed round of financing targeted at specific entities. This led to the allocation of 7% (14,700,000 ICL) of the total supply, distributed across three neurons with dissolve delays of 0 months, 3 months, and 6 months.

#### Team (15%)

The amount of ICL allocated to the development team accounts for 15% of the total supply (31,500,000 ICL), with a vesting period of 6 months. It is divided into nine neuron distributions with dissolve delays of 0 months, 3 months, 6 months, 9 months, 12 months, 15 months, 18 months, 21 months, and 24 months.

#### **SNS Swap (30%)**

The amount of ICL allocated for the SNS Swap account for 30% (63,000,000 ICL) of the total supply, divided into five neuron distributions with dissolve delays of 0 months, 3 months, 6 months, 9 months and 12 months.

## **SNS Swap Parameters:**

minimum\_participants: 100
minimum\_direct\_participation\_icp: 200\_000 tokens
maximum\_direct\_participation\_icp: 600\_000 tokens
minimum\_participant\_icp: 1 tokens
maximum\_participant\_icp: 100\_000 tokens
VestingSchedule:
 events: 5
 interval: 3 month
 start\_time: 12:00 UTC
 duration: 15 days
 neurons\_fund\_participation: true

## 5.3 Voting power

At the launch of SNS, Voting Rewards and Treasury do not have voting rights. The initial distribution of voting rights is as follows:



Voting power distribution

Early Investors consist of over 20 early-stage investors and contributors who, from 2020 to 2023, provided the development team with funding and resources. They possess specialized knowledge in blockchain or finance and will vote based on their interests, hence their voting rights are independent of the development team's.

One potential scenario involves an attacker purchasing a significant portion of ICL tokens during the SNS swap and increasing the dissolve delay of all their neurons to the maximum period, in an attempt to gain more than 50% of the SNS voting power. If successful, the attacker could potentially force a proposal to transfer the treasury to themselves.

Assuming a worst-case scenario where the attacker participates in the SNS swap and occupies the entire quota of maximum\_direct\_participation\_icp, the Community Fund will also participate according to the algorithm, accounting for about 25% of the total SNS swap. In this scenario, the attacker would approximately hold 75% of the total SNS swap volume, resulting in a maximum of 48.04% of the total voting rights. This



would not be sufficient to carry out a 51% attack.

## 5.4 Circulating Supply Line

According to the Initial token allocation rules, except for the Treasury, the circulating supply over time is predictable. To forecast the overall circulating supply curve, assumptions need to be made regarding the use of the Treasury and the burning of ICDex gas.

(1) Assume that the Risk Reserve and Strategic Reserve in the Treasury will not be withdrawn.

(2) Assume that the extraction and distribution rules for the Eco-Incentive Reserve in the Treasury follow the description in Section 5.2, 'Eco-Incentive Reserve.'

(3) Assume that the gas generated by ICDex will be burned according to the rules in Section 5.1, 'Used as a gas for dapp,' where 50% will be burned. Based on this, optimistic and pessimistic forecasts can be made.

Optimistic forecast: Starting from the second quarter after the launch of SNS, 0.02% of the total supply of ICL will be burned, maintaining a 100% growth rate for three consecutive quarters, followed by a 50% growth rate for the next four quarters, and then

maintaining that level.

Pessimistic forecast: Starting from the second quarter after the launch of SNS, 0.01% of the total supply of ICL will be burned, maintaining a 30% growth rate for three consecutive quarters, followed by a 10% growth rate for the next four quarters, and then maintaining that level.

Based on the above data assumptions, the predictable ICL supply curve is as follows: Under the optimistic forecast, the maximum circulating supply is 140.37M ICL



Circulating Supply (optimism)



In a pessimistic forecast, the maximum circulating supply is 158.07M ICL, excluding the Risk Reserve and Strategic Reserve from the Treasury.



Circulating Supply (pessimism)



## 5.5 Funding target

Community Direct Participation in SNS Swap ranges from 200K ICP to 600K ICP, and the Community Fund (CF) contributing a portion of the ICP. The ICP raised will be retained in the SNS Treasury and will be used for the risk reserve, providing liquidity, Cycles consumption for dApps, security audits, and other security-related expenses, with no plans for other uses. The founding development team commits not to initiate proposals to withdraw ICP from the treasury for team expenses. The team's costs are covered by early fundraising, personal funds, and if necessary, financing through ICL from the treasury. This approach is to align the goals of the development team with those of the community.

# 6. Roadmap

Note: Fixes and upgrades to existing projects may delay the following development plan.

## 2024 Q1

- Initiate ICLighthouse DAO SNS.
- Convert airdropped ICL (DRC20) to ICRC1 tokens.
- Complete NFT airdrop of ICLighthouse Planet Cards.
- Implement SNS treasury tokens for ICDex market making.
- Develop Eco-Incentive and Risk Reserve canisters; integrate as dApps in ICLighthouse SNS.
- Redesign trading mining feature.
- Develop liquidity mining.

## 2024 Q2

- Finalize trading pair list Aggregator; introduce decentralized listing rules and trading competition features.
- Restructure ICTC module.
- Overhaul <u>IC.house</u> blockchain explorer.
- Refactor icRouter for Bitcoin and Ethereum; reopen for testing.
- Complete icRouter security audit; integrate with ICLighthouse SNS.
- Integrate USDT, USDC; launch related trading pairs on ICDex.

## 2024 Q3

- Develop ICDex-Trader for on-chain quantitative trading.
- Develop and test decentralized trading fund feature.

## 2024 Q4

- Launch decentralized trading fund feature.
- Enhance operational features.

## 2025

- Extend icRouter integration with more blockchains; conduct testing.
- Continue enhancing operational features.

## 2026

• Explore and develop innovative features.

## REFERENCES

- [1] DFINITY Foundation: https://dfinity.org/
- [2] Internet Computer: https://internetcomputer.org/
- [3] Network Nervous System (NNS): <u>https://internetcomputer.org/nns/</u>
- [4] Service Nervous System (SNS): <u>https://internetcomputer.org/sns/</u>
- [5] Uniswap: <u>https://uniswap.org/</u>
- [6] Dydx: <u>https://dydx.exchange/</u>
- [7] Order matching system: <u>https://en.wikipedia.org/wiki/Order\_matching\_system/</u>
- [8] Stop-limit Order: <u>https://en.wikipedia.org/wiki/Order\_(exchange)#Stop-limit\_order</u>

[9] Grid Order: <u>https://www.binance.com/en/support/faq/what-is-spot-grid-trading-and-how-does-it-work-d5f441e8ab544a5b98241e00efb3a4ab</u>

[10] Iceberg Order: <u>https://corporatefinanceinstitute.com/resources/career-map/sell-side/capital-markets/iceberg-order/</u>

[11] VWAP Order: https://en.wikipedia.org/wiki/Volume-weighted\_average\_price

[12] TWAP Order: <u>https://en.wikipedia.org/wiki/Time-weighted\_average\_price</u>