# RaumFi - zk based Decentralized Exchange on Starknet & Polygon

Raum Network Team

**Abstract.** This technical whitepaper explains the core of Raum Network covering the feature that allows traders to swap tokens, add liquidity and remove liquidity from a given token pool.
A decentralized exchange (DEX) is a platform that enables peer-to-peer trading of cryptocurrencies without the need for intermediaries. Unlike centralized exchanges, DEXs operate on a blockchain network, making them more secure and transparent. This whitepaper aims to provide an overview of the current state of decentralized exchanges, their benefits and drawbacks, and a proposal for a new DEX that addresses the challenges faced by existing platforms. Our goal is to create a decentralized exchange that combines the security and decentralization of existing DEXs with user-friendliness and some new functionality.

## 1. Introduction

Raum-Fi is a decentralized exchange protocol that allows users to trade tokens without intermediaries or centralized authorities. Raum-fi introduces a new automated market maker (DEX) system that allows for more efficient trading and liquidity provision on Starknet. Starknet is a Layer 2 scalability solution for Ethereum that enables fast and cheap transactions.

### 1.1. Overview

Starknet is a Layer 2 scaling solution that uses zero-knowledge proofs to validate transactions off-chain, before committing them to the Ethereum blockchain. Starknet enables fast and cheap transactions, which makes it an ideal platform for decentralized exchanges like Uniswap.

### 1.2. Design

The Uniswap-like swap on Starknet will follow the same basic design as Uniswap v2. It will have a pair of tokens, which will be traded against each other based on the constant product formula. The design will leverage the benefits of Starknet to provide fast and cheap transactions, as well as better scalability and throughput.

The swap will consist of two smart contracts: the Factory contract and the Pair contract. The Factory contract will be responsible for creating new pairs, while the Pair contract will manage the exchange of tokens.

The Factory contract will be deployed on the Starknet mainnet, while the Pair contracts will be deployed on Starknet. This design allows for fast and cheap transactions, while still benefiting from the security and stability of the Ethereum blockchain.

The Pair contract will be responsible for maintaining the price of the tokens, as well as managing liquidity provision. The constant product formula will be used to calculate the price of the tokens, and liquidity providers will be incentivized to provide liquidity by earning fees from trades.

A portion of the trading fees will be distributed to liquidity providers. This incentivizes users to provide liquidity, which in turn provides better liquidity and more efficient trades.

### 1.3. Conclusion

The constant product formula will be used to maintain the price of tokens, while liquidity providers will be incentivized to provide liquidity by earning fees from trades. By deploying the Pair contracts on Starknet, the swap will benefit from the fast and cheap transactions enabled by the Layer 2 scaling solution, while still benefiting from the security and stability of the Ethereum blockchain.

## 2. Why Starknet

**2.1 Security (Zero-knowledge):** Starknet is built on top of Ethereum, which is currently the most secure and battle-tested blockchain. On top of ethereum, Starknet also provides additional layers of security through the use of zero-knowledge proofs.

**2.2 Scalability:** Starknet is designed to scale Ethereum by allowing for off-chain computation, which reduces the load on the Ethereum network. This makes it possible to build complex applications and processes that require a high degree of computational power while keeping gas costs low **(Lower gas fees)**.

**2.3 Fast transactions:** Starknet can process transactions much faster than the Ethereum mainnet, with a target throughput of up to 10,000 transactions per second.

# 3 .Technical Architecture

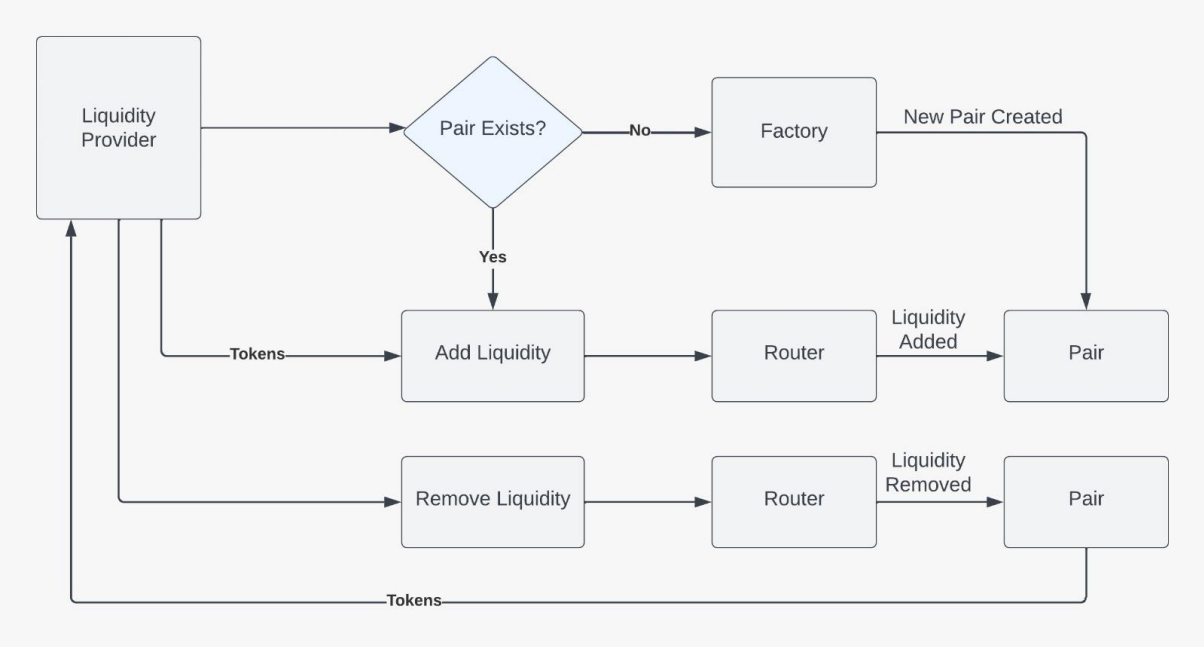
## 3.1 Key smart contracts

**3.1.1 Factory** - The factory contract acts as a blueprint for creating new liquidity pools. It holds a mapping of all the pools, and users can interact with this contract to create new pools or add liquidity to existing pools.

**3.1.2 Router** - This contract acts as an intermediary between the user and the pools. It receives the trade requests and routes them to the correct pool based on the tokens being traded. It also handles the calculation of the prices and the transfer of funds.

**3.1.3 Liquidity Pool** - Each pool is represented by a separate smart contract that holds the reserves of the tokens being traded. This is where the actual trading takes place. When a user wants to trade, they submit an order to the pool, and the price is determined by the ratio of the token reserves in the pool.

## 3.2 Liquidity Provider Flow:-



### 3.3 User Flow:-


## 4. Feature List

- **4.1 Swap tokens from a given pool**
- **4.2 Add/Remove Liquidity from a pool**
- **4.3 LP Token**
- **4.4 Fees based on tier**
- **4.5 RN staking***
- **4.6 Locked/Variable Staking***
- **4.7 Liquid Staking***

**Will be introduced in future iterations and deployment*

## 4.6 Locked and Variable Staking

### 4.6.1 Introduction

Staking is a process in which token holders lock their tokens in a smart contract in order to support the network and earn rewards. There are two types of staking: lock staking and variable staking. Lock staking involves locking tokens for a set
period of time, while variable staking allows users to stake and unstake their
tokens at any time. This whitepaper will explore the differences between lock staking and variable staking, as well as the advantages and disadvantages of each approach.

### 4.6.2 Lock Staking

Lock staking involves locking tokens in a smart contract for a set period of time. During this time, the tokens are not available for trading or transfer. Lock staking is commonly used in proof-of-stake (PoS) consensus algorithms, where token holders stake their tokens to support the network and earn rewards.

One of the advantages of lock staking is that it provides a predictable and stable source of income for token holders. Since the tokens are locked for a set period of time, token holders can accurately calculate their expected rewards. This makes lock staking a popular option for investors who are looking for a low-risk investment with a predictable return.

However, one of the disadvantages of lock staking is that it can be difficult to predict market conditions. If the market value of the staked tokens decreases during the lock-up period, the investor may end up with a lower return on investment than expected.

### 4.6.3 Variable Staking

Variable staking allows users to stake and unstake their tokens at any time. This gives users more flexibility and control over their tokens. Users can stake their tokens when they believe the market conditions are favorable, and unstake their tokens when they believe the market conditions are unfavourable.

One of the advantages of variable staking is that it allows for greater flexibility and control over the tokens. Users can adjust their staking strategy based on market conditions, which can help to maximize their returns. Additionally, variable staking can help to promote liquidity in the

market, since users are not required to lock up their tokens for a set period of time.

However, one of the disadvantages of variable staking is that it can be less predictable than lock staking. Since users can unstake their tokens at any time, the rewards for variable staking can be more volatile than lock staking. Additionally, variable staking may not be suitable for investors who are looking for a low-risk investment with a predictable return.

### 4.6.4 Conclusion

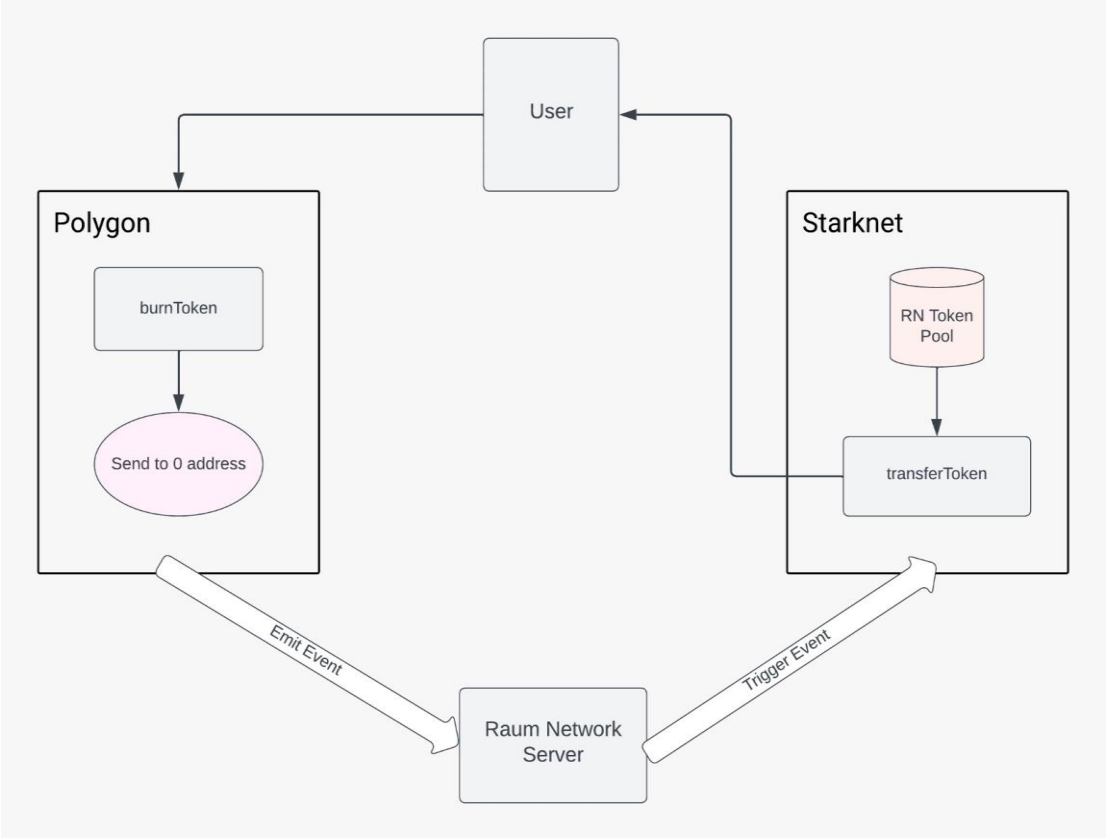
Lock staking and variable staking are two different approaches to staking. Lock staking involves locking tokens in a smart contract for a set period of time, while variable staking allows users to stake and unstake their tokens at any time. Both approaches have their advantages and disadvantages, and the choice between lock staking and variable staking will depend on the individual investor's risk tolerance and investment goals. Ultimately, the decision to stake tokens should be based on a thorough analysis of the market conditions and the potential risks and rewards of each approach.

## 5. Transfer the token from polygon to Starknet

Currently, Raum network tokens are available on polygon, but the users who want to use our DEX need to bridge the tokens to Starknet. Currently, we provide our intermediary server to capture the burn event and trigger the send event. Please refer to the following diagram for more details:-

**Detailed steps:-**

i. The user calls the burnToken() function of our smart contract on the polygon chain, passing the parameters like Starknet address.
ii. Our smart contract burns the RN token(send to 0 address) and emits an event to our centralised server.
iii. The server triggers the call to transferToken() function of our smart contract on the Starknet chain.
iv. User receives money from our pools.



## 6. References


[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf

[2] Vitalik Buterin et al. Ethereum white paper, https://whitepaper.io/document/5/ethereum-whitepaper

[3] Ethereum: A secure decentralized generalized transaction ledger, https://ethereum.github.io/yellowpaper/paper.pdf

[4] DeFi : Decentralized finance (DeFi), https://ethereum.org/en/defi/

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

[6] Lido.fi, https://lido.fi/

[7] Rocketpool, https://rocketpool.net/

[8] Superfluid staking, https://docs.osmosis.zone/osmosis-core/modules/superfluid/

[9] Staking, https://www.coinbase.com/learn/crypto-basics/what-is-staking

[10] Rollup-centric Ethereum roadmap, https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698