RAI Finance

The Future of Trading

November 2021

1 Introduction

RAI Finance is a protocol designed for decentralized cross-chain asset exchange. Decentralized Finance (DeFi) has grown exponentially and transactions, services and usage of DeFi have increased significantly and become more widespread. This can be corroborated by the TVL (Total Value Locked) in DeFi protocols, which went from 1B USD in June to 10B USD in October. [1]. While DeFi allows peer-to-peer transactions and the security of non-custodial assets, it does so at the cost of liquidity and a diverse asset selection which is traditionally enjoyed by centralized service providers. RAI Finance introduces this with its layer 2 scalability as a swap protocol, improved automated market making functionality and cross-chain asset support, bringing to DeFi both liquidity and diversity of assets. This will be facilitated via SOFI, a native token as the incentive layer for user's liquidity contribution and governance on protocol architecture iterations.

2 About Us

Group of experts in cryptocurrency, trading and decentralized finance are among the community that contribute to the RAI Finance protocol. Additionally,core developer contributors include the team who built innovative cryptocurrency trading platforms such as League of Traders[2], a social trading platform that allows users to emulate the trading strategies of experienced and high profile traders and DEXEOS[3], the first ever DEX (Decentralized Exchange) on EOS. Our goal is to simplify the trading process for retail users and bring new assets and liquidity into the DeFi Ecosystem.

[1] https://defipulse.com/

[2] https://leagueoftraders.io/

[3] http://dexeos.io

3 The Current DEX Ecosystem

Since the launch of the Ethereum chain, DEXs have been a major innovation allowing users to maintain collateral of their digital assets as opposed to delegating that to a centralized exchange when exchanging, thus mitigating exposure to a centralized party's vulnerabilities. However, even with the clear advantages and lessons from numerous devastating exploits of centralized financial services (eg. The Kucoin Hack of over $250M USD), DeFi applications still struggle to onboard the masses keeping it far from competing with, let alone expanding its impact to the realm of traditional finance. All the while centralized platforms hold the majority of the trading volume and asset generation.

3.1 Unsustainable Network Fees

Gas fees on Ethereum have skyrocketed throughout the past several months with the increasing on-chain transaction volume, pricing out retail's small value transactions. This can be seen with a transaction costing an average of $3-4 and up to $15 on Uniswap during periods of high on-chain volume, and more intricate automated market-making (AMM) algorithm based exchanges like Balancer costing even more. This could lead to a situation where no new participants enter the DeFi space since they are priced out. To reach a level of ease and adoption that rivals the traditional finance system, DeFi applications need to handle a similar volume of transactions while keeping fees low. While many solutions have been offered for helping Ethereum scale and handle transactions during periods of high volume, none have come to fruition as of yet.

3.2 Dependent on Single Base Layer Protocol

The vast majority of the activities in DeFi, and locked DeFi assets are found in one main chain, Ethereum. This poses a major problem since the Ethereum blockchain cannot handle the multitude of transactions that stem from these DeFi applications. The Ethereum network has often been congested and gas fees have skyrocketed as a result of the explosive growth of these DeFi applications, as explained in the previous sections. Furthermore, with the possibility of flash loans, more and more attacks are being conducted on vulnerable contracts (eg. Eminence [4]), leading to a loss of faith in DeFi applications.

3.3 Lack of Diversity Among Asset Types

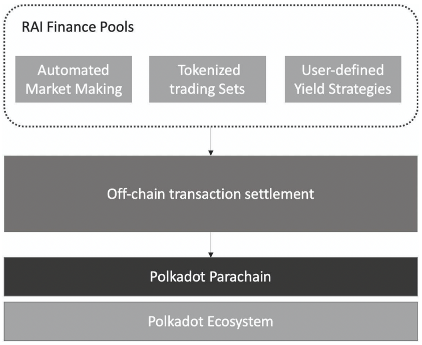
The types of assets supported by blockchains are limited to the parameters defined by the current protocols. ERC20 tokens and single-chain transactions are the main supported option when it comes to Ethereum based DEXs. An example of this can be seen with Maker, Compound, Curve and Aave having several billion dollars locked in their smart contracts yet only supporting vanilla ERC20

[4] https://cryptotips.eu/en/news/bizarre-15-million-eminence-hack-an-unfinished-project-by-andre-cronje/

assets. DeFi is still far from the numerous financial products and services that are found in the traditional market. As additional blockchain-based asset classes continue to emerge, improved liquidity and markets will be needed to flourish them. While ETH-bridges from other chains might allow the tokenization of other assets, challenges remain with respect to the scalability of these proposed ideas.

4 RAI Finance Protocol

RAI Finance is a protocol designed to provide a wider range of assets, a higher amount of liquidity, and a variety of financial accesses for the DeFi ecosystem. For example, when combined with the cross-chain compatibility of the Polkadot ecosystem, this feature set provides decentralized financing with new assets and more liquidity, eliminating fragmentation across the existing DeFi ecosystem. This is the next step for DeFi to break through its current limitations.



The protocol architecture provides layering for secure off-chain transactions with on-chain settlements to enable complex computations and more efficient transactions without losing the security and decentralization of blockchain. This increased complexity and speed can provide opportunities for market making and automated trading that are traditionally exclusive to centralized exchanges.

4.1 Secure Off-chain Transactions

RAI Finance improves the scalability of automated market making and yield strategies through secure off-chain transactions. By leveraging Zero-knowledge Proofs for trustless computation and cryptographic accumulators for immutable data storage, it is possible to provide a layer 2 solution that supports scalability, transparency, and privacy in transactions. Bringing most of the work off-chain reduces the cost and time of each individual transaction and enables a larger variety of previously out-of-bounds market use cases. As a result, transactions and computations for automated trade can be performed and validated off-chain in real-time, with final settlements being made on-chain.

4.2 Cross-chain Asset Capability

In order to reach a wider variety of asset types, RAI Finance will be able to integrate with various blockchains like Polkadot, Polygon and other blockchains making it fully cross chain. Interoperability differentiates RAI Finance from many other popular liquidity protocols running on Ethereum and limited only to ERC20 tokens. Furthermore, as RAI Finance evolves, its EVM compatible smart contract capability allows for the integration of unique assets and non-fungible tokens (NFTs).

5 RAI Finance Pools

5.1 Automated Market-Making Variability

RAI Finance liquidity pools can manage a variety of automated market-making (AMM) services to provide liquidity to different digital markets, with the objective being to choose automated market-making algorithms to maximize revenue for different asset pairs. It has been proven that the same market-making techniques, such as product rule, perform well for mean-reversion assets and correlated pairings, but they do not perform well for uncorrelated and inverse correlated pairings.

5.2 Constant Function Market-Makers

Constant Function Market-Makers(CFMM) have obtained popularity in DeFi markets and, as a result, There have been various CFMMs implemented in DeFi liquidity protocols such as Uniswap, Balancer, and Curve. We give a brief introduction here. For a two-sided pool with reserve asset quantities x and y, we fix a function $f(.,.)$ and a constant k

$$f(x,y) = k \tag{1}$$

For constant-product pools with equal weights, we have:

$$f(x,y) = xy \tag{2}$$

For Balancer pools with two assets, it is possible to adjust weights for the reserve assets:

$$f(x,y) = x^a y^b \tag{3}$$

For Curve pools with a basket of n assets, each with reserve amounts x_i, let $S = \sum x_i$ and $P = \Pi x_i$. We have:

$$\alpha\delta^{n-1}S + P = \alpha\delta^n + (\frac{\delta}{n})^n \tag{4}$$

In essence, to simplify the above expression, we can write the following:

$$f(S) + g(P) = k \tag{5}$$

Here functions f and g are chosen specifically tuned to the properties we want for our AMM. Protocols like Curve and Shell use combinations of these rules to offer unique AMM algorithms for different use-cases. In particular, Curve has proved to be incredibly effective for stablecoin swaps with extremely low slippage (0.5%). Hypertuning AMM parameters described above, as well as changing not just functions of S and P. In general, we can have infinitely many functions:

$$f(x_1, ..., x_n) = k \tag{6}$$

One interesting alternative would be to have the function f be chosen from a family of functions $F = f_i, F : i \to f_i$ where i captures the properties of the basket of assets in some way. For example, for stablecoins whose volatility (over the past 3 months, say) is low, we can have a function like Curve. On the other hand, we can have a more sensitive function such that the following holds:

$$f_i \propto \sigma_i \tag{7}$$

Where σ_i is a measure of the variance of the assets parameterized by i. For example, we can set:

$$\sigma_i = max(Var(x_1), ..., Var(x_n)) \tag{8}$$

This allows the slippage to be sensitive to the volatility of the underlying assets in the pool.

5.3 Logarithmic Market Scoring Rule (LMSR)

Introduced first by Hanson in the late 90s/early 2000, the LMSR gives a scoring rule for prediction markets. The idea was to elicit information from participants and adjust scores/weights for assets accordingly. Scoring rules have a longer history, however, going back to the early 1900s. Here we introduce a few basic scoring rules:

$$Brier/Quadratic : Q(r, i) = 2r_i - \sum r_j^2 \tag{9}$$

Another interesting scoring rule is the spherical scoring rule:

$$S(r, i) = \frac{r_i}{||r||} \tag{10}$$

The logarithmic scoring rule offered by Hanson is:

$$L(r, i) = ln(r_i) \tag{11}$$

The logarithmic cost function is given as:

$$C(q_1, ..., q_n) = bln(e^{\frac{q_1}{b}} + ... + e^{\frac{q_n}{b}}) \tag{12}$$

In a pool with two assets (1 and 2), the corresponding price function (for asset 1, say) for the LMSR above would be:

$$\begin{aligned} p(1) &= \lim_{\Delta q_1 \to 0} \frac{C(q_1 + \Delta q_1, q_2) - C(q_1, q_2)}{\Delta q_1} \\ &= \frac{e^{\frac{q_1}{b}}}{e^{\frac{q_1}{b}} + e^{\frac{q_2}{b}}} \end{aligned} \tag{13}$$

In fact, Hanson showed that any proper scoring rule can be converted into a market maker. A scoring rule is proper if the highest expected reward is obtained by reporting the true probability distribution. RAI Fiannce will tune its market maker functions to be sensitive to the assets in any specific pool. In addition, the function can be chosen across a large set of functions that satisfy the conditions for a scoring rule.

Different algorithms are more suitable because specific assets contain different assumptions about the price relationship between the assets being quoted. The goal of the RAI Finance protocol is to provide an AMM optimized for the different relationships between asset pairs. Algorithm flexibility is essential to maximize profits and minimize the risk of liquidity providers while securing more assets for users to trade efficiently

6 Unique Assets

RAI Finance is designed to support the creation of unique assets that do not currently exist in the liquidity pools. These include and are not limited to tokenized trading strategies, yield generating strategies and future financial strategies.

6.1 User Defined Trading and Yield Strategies

The transparency in calculation and privacy of implementation provide the foundation for enabling user-defined yield strategies. With ZKP, users can define and publish transaction strategies transparently without giving up implementing proprietary algorithms. In contrast to other protocols like Compound and Dai, the underlying computational processes can be implemented off-chain with ZKP, enhancing transparency and security without compromising complexity and privacy. As an example, consider the case of depositing X USD into a contract that can be unlocked at any time by the user. Operations can be conducted off-chain, with zk-proofs being published on-chain, so that veracity and integrity is preserved, while transactions can be made quickly and efficiently. All of the RAI Finance pools that trade based on these algorithms are under the same strategy and have the assurance that users do not have to provide computational resources for said strategy. Strategies within the ecosystem can then be assessed according to metrics like maximum and average drawdown, win rate, profit/loss ratio, and the lifetime of the strategy. Through these metrics, it is possible to create a reputation-based market from which users can select trading and yield strategies.

6.2 Token Sets and NFTs

The RAI Finance protocol implements self-balancing token sets where users are able to follow a trader's performance/strategy on RAI Finance so that everyone can easily access and invest in these traders. The capability to use smart contracts and zero-knowledge computation(ZKP) can eventually extend to create and exchange unique non-fungible tokens (NFTs). The implementation of self-balancing token sets can mirror that of SET protocol [5], where a vault small contract stores mappings to ownership of certain assets. As an example, consider a strategy by a trader that starts with USD and buys ETH when the ETH/BTC ratio is <0.025 and sells ETH when the ETH/BTC ratio is >0.035. The values of the ratio are obtained via oracle access. A RAI user can buy the performance of this strategy through a vault that uses an AMM to swap between ETH and USD depending on the conditions of the strategy. The vault can be redeemed for the equivalent amount of USD if a user ever wants to withdraw their funds from the vault.

7 RAI Finance Token (SOFI)

SOFI, the native token for RAI Finance is an integral component to the protocol and constitutes many functions in the ecosystem. The following utilities represent the current status of the token that may change in accordance with future governance proposals.

- **Governance** - SOFI token has a governance function for the protocol where token holders will vote on parameters but not limited to transaction fees, liquidity mining, vault management, etc.
- **Protocol Fees** - RAI Finance requires a % fee for each transaction utilizing the protocol which is subject to community governance.
- **Network Incentives** - A portion of SOFI is allocated to attract and reward users and traders for providing liquidity on the protocol. AMM variability ensures users can optimized their liquidity by selecting the best liquidity pool while also receiving SOFI.

8 Conclusion

RAI Finance improves upon current DeFi liquidity pools by enabling superior liquidity and diversity of assets through layer 2 scalability as a swap protocol.

[5] https://www.setprotocol.com/pdf/set_protocol_whitepaper.pdf

In addition to offering AMM flexibility and cross-chain asset support through chains like the Polygon or Polkadot ecosystem, users can use its social trading features without being forced to learn the intricacies of trading and/or using these assets.