RAI Finance

The Future of Trading

August 2020

1 Introduction

RAI Finance is a protocol designed for cross-chain asset exchanges. WIth the increased traffic in the blockchain space and the value of cryptocurrency monetary policy being understood, the adoption of decentralized financial (DeFi) applications has also naturally risen. 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 changes this with the introduction of its layer 2 scalability as a swap protocol, improved automated market making functionality and cross-chain asset support, bringing DeFi both liquidity and diversity of assets. This is facilitated via RAI, a native token as the incentive layer for user liquidity contribution and governance on protocol architecture iterations.

2 About Us

RAI Finance is led by a group of experts in cryptocurrencies, trading and decentralized finance. We have built complex cryptocurrency trading platforms like League of Traders [1] a social trading platform that allows users to copy the trading strategies of experienced and high profile traders and Dexeos[2], the 1st DEX on EOS. Our goal is to simplify the trading process for retail users and bring new assets and liquidity into the DeFi Ecosystem.

3 Problems with Current Decentralized Liquidity Protocols

Since the beginning of Ethereum, decentralized exchanges (DEX) have been a major innovation allowing users to maintain custody of their digital assets as opposed to delegating that to a centralized entity when exchanging, thus mitigating centralized exchange vulnerabilities. However, even with the clear advantages and lessons from numerous devastating exploits of centralized alternatives, 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 exchanges and service providers hold the majority of the trading volume, asset generation, and even see traditional adoption.

1 https://leagueoftraders.io/
2 http://dexeos.io/

3.1 Lack of Volume and Liquidity

Dex volume has made significant strides since the start of the year with a report from DappRadar[3] publishing that the overall DEX trading volume has surpassed all of 2019 reaching US$2.5 billion in the first five months of 2020. In spite of this, it's still just a fraction of overall trading volume and to put it in overall trading volume and to put it in context, Binance one of the largest centralized exchanges reported on April 29th, 2020 a 24hr trading volume of $11 billion USD[4]. On the other side the top DEX, Uniswap, held 30% of the May 2020 trading volume albeit with a low 1000-2000 active user count with a key bottleneck, for Uniswap and DEXs as a whole, being the low volume and liquidity.

3.2 Slow and Expensive Transactions

The current gas fees on Ethereum have skyrocketed 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 on Uniswap based on July 2020 data, and more intricate automated market-making algorithm based exchanges like Balancer costing even more. With this stands the chance of the Ethereum network facing even higher fees and congestion as increased liquidity mining participants could result in a standstill like state for DeFi applications. If DeFi had adoption and reach to a level of that of the global financial system, such an event would have disastrous implications.

3.3 Limitations in the Asset Classes

The degree of assets available and blockchains supported are limited to the parameters defined by the current protocols. This can be seen with ERC20 token, single-chain transactions being the main supported option when it comes to Ethereum based DEXs. As additional blockchain-based asset classes continue to emerge, improved liquidity and markets will be needed to support them. An example of this can be seen with Maker, Compound, and Aave having hundreds of millions of dollars locked in on-chain lending, one of the rapidly growing DeFi verticals. Furthermore, DeFi has also seen the rise of crypto insurance and bonds but is still far from markets facilitating the exchange of Repos (Repurchase Agreements) or asset securitization.

3.4 "Centralized" Base Layer Protocol

The vast majority of the activity in DeFi, and locked DeFi assets are found on one chain, Ethereum. This poses a major problem since the Ethereum blockchain can not handle the multitude of transactions that stem from these applications. The Ethereum network has often been congested and gas fees have skyrocketed as a result of the activity of these DeFi applications. Also, this DeFi base layer centralization has inherent risks, especially as Ethereum moves to a Proof-of-Stake system. The security threat is shown in an analysis by Dragonfly Capital,[5] where if the lending facilities provide better returns as compared to staking, the protocol vulnerability would grow as users follow returns to lending over staking.

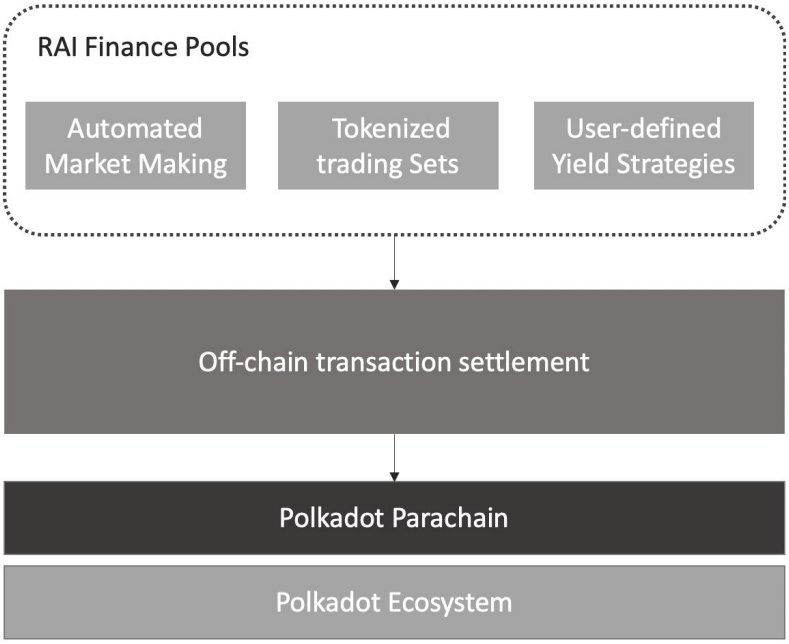
3 https://dappradar.com/blog/dex-trading-volume-exceeds-2-5-billion

4 https://cointelegraph.com/news/binance-trading-volume-reaches-all-time-high-amid-bitcoins-price-surge

5 https://medium.com/dragonfly-research/how-defi-cannibalizes-pos-security-84b146f00697

4 RAI Finance Protocol

RAI Finance is a protocol designed to provide DeFi with a wider range of assets, a higher amount of liquidity, and a diverse set of financial use cases. When this feature set is combined with the cross-chain compatibility of the Polkadot ecosystem, it eliminates fragmentation across the existing DeFi ecosystem by bringing a complement of new assets and a higher amount of liquidity to decentralized finance. This is the next step for DeFi to break through its current limitations.



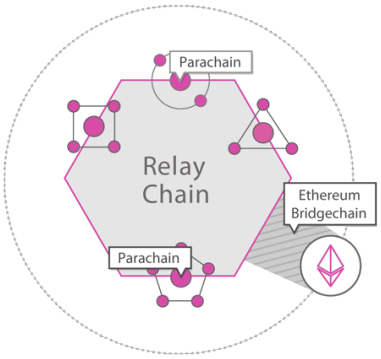
The protocol architecture layers secure off-chain transactions with on-chain settlements to enable complex computations and more efficient transactions without giving up the security and decentralization of blockchain. This added complexity and speed opens up opportunities for market-making and automated trading that are traditionally reserved for centralized exchanges.

4.1 Secure Off-chain Transactions

RAI Finance utilizes secure off-chain transactions to improve the scalability of its automated market-making and yield strategies. By using 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 a majority of the work off-chain lowers the cost and time of each individual swap, and enables a larger variety of previously out-of-bounds market use cases. As a result, trades and calculations for automated trades can be performed and validated off-chain in real-time, with final settlements done on-chain.

4.2 Cross-chain Asset Capability

In order to reach a wider variety of asset classes, Rai Finance will be built on a parachain and integrated into the Polkadot ecosystem. This enables the protocol to leverage the cross-chain compatibility of the Polkadot relay chain to increase the number of supported assets. Interoperability distinguishes RAI Finance from many of the other popular liquidity protocols that are on Ethereum and are solely limited to ERC20 tokens. Furthermore, as RAI Finance evolves, the smart contract capability of the Polkadot ecosystem 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 utilize a variety of automated market-making (AMM) agents to provide liquidity to different digital markets, with the objective being to choose automated market-making algorithms to maximize profit for different pairings. It has been shown that the same market-making techniques, like the product rule, perform well for mean-reverting assets and correlated pairings, but they do not perform well for uncorrelated and inverse correlated pairings.

Constant Function Market-Makers

Constant Function Market-Makers (CFMM) have gained popularity in decentralized finance, and as a result, there have been a variety of different CFMM implementations in liquidity protocols like Uniswap, Balancer, Curve. Constant function market-makers utilize an equation that takes in the quantity of each reserve currency (R). This equation is then set equal to an initial value (k), and each trade must change the number of reserve currencies in a manner that maintains this equality. There are a variety of different simple CFMMs, including the

Product, Sum, and Mean rule, and protocols like Curve and Shell have used combinations of these rules to provide unique AMM algorithms. These protocols show that there is still much more room for improvement in the Automated Market-Making space, with the boundary for this progress being computational complexity and the hypertuning of AMM parameters like the weights of reserves (*w)* and the initial value.

Constant Sum Rule	$\sum_{i=1}^{n} R_i = k$
Constant Product Rule	$(R_a)(R_b) = k$
Constant Mean Rule	$\prod_{i=1}^{n} R_i^{w_i} = k,$

Logarithmic Market Scoring Rule (LMSR)

Along with constant function market-makers, OmniSwap liquidity pools can utilize additional market-making functions like the Logarithmic Market Scoring Rule (LMSR). Unlike CFMMs which are tied to a constant (*k*), the LMSR uses a reward function (*C*) to determine beneficial trades. Any trade that improves the reward function is accepted. This methodology is used in traditional finance and in prediction markets for uncorrelated assets.

$$C(P_W, P_L) = b * \ln(e^{\frac{P_W}{b}} + e^{\frac{P_L}{b}})$$

Different algorithms are better suited for certain assets since they contain different assumptions about the price relationship between the assets being quoted. The goal of the RAI Finance protocol is to provide an AMM that is optimized for the different relationships between asset pairings. The flexibility of algorithms is essential to bringing more assets for users to trade efficiently while also maximizing profit and minimizing risk for liquidity providers.

5.2 Unique Assets

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

Tokenized Sets and NFT's

Along with automated market-making, the RAI Finance protocol has the capability to use smart contracts and zero-knowledge computation (ZKP) in the implementation of self-balancing token sets and in the creation and exchange of unique non-fungible tokens (NFTs) associated with insurance, loans, and property ownership. In contrast to other protocols like Compound and Dai, the underlying computational processes can be implemented off-chain with ZKP which adds transparency and security without compromising on the complexity and privacy.

User-defined Yield Strategies

The transparency of computation and privacy of implementation provides the foundation for enabling user-defined yield strategies. Using ZKP, users can define and transparently publish trading strategies without giving away the implementation behind their proprietary algorithms. RAI Finance pools that base their trades on these algorithms have the assurance that they are all receiving the same strategy and do not require the user to provide the 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 yield strategies.

For example, one can tokenize a trader's performance/strategy on RAI Finance so that everyone can easily access and invest in these traders. Users stake RAI based on their confidence level of their trading/farming strategy, which impacts how much RAI they receive if other users choose their strategy. Those who want exposure to that user's strategy stake RAI which is directly correlated to the exposure of their selected strategy. Any user can get exposure to these assets without being forced to learn the intricacies of trading and/or using these assets or risk financial loss due to inexperience.

6 RAI Finance Token (RAI)

RAI, the native token for RAI Finance is an essential component to the protocol and employs many functions in the ecosystem. The following utilities reflect the current status of the token that can be subject to change based on future governance proposals.

Transaction Fee Burn

Each transaction on RAI Finance requires a transaction fee of 0.02%. The transaction fee is split where 50% of the fee goes to the providers of the liquidity pool and the other 50% goes to a RAI burn.

Liquidity Pool Staking

In order to discourage liquidity pools of fake and scam tokens, RAI must be staked in order to create a new liquidity pool.

Asset Generation

Both users that generate assets based off of their trading or yield farming strategies and users who invest in these strategies must stake RAI which correlates directly with their exposure.

Governance

RAI functions as a governance token for the protocol where token holders will vote on parameters such as but not limited to transaction fee burn, liquidity mining ratio, pool staking fees, etc.

Liquidity Incentives

A major portion of RAI is allocated to attract and reward users for providing liquidity on the protocol. AMM variability ensures users can maximize their profit by selecting the best liquidity pool while also receiving RAI.

7 Conclusion

RAI Finance improves upon existing DeFi liquidity pools by enabling superior liquidity and diversity of assets through layer 2 scalability as a swap protocol with AMM flexibility and cross-chain asset support through the Polkadot ecosystem. On top of that, RAI finance will be able to support future innovative financial products and seamlessly incorporate them into the protocol to garner increased liquidity.