magpie

Litepaper

v1.2 - February 2024

magpiefi.xyz

Vision

We're shaping the future of how people interact with financial systems built on decentralized, fair, and universally accessible technology.

Mission

To empower users of all levels by building a cross-chain infrastructure service that offers a simple, efficient, and secure way to trade, invest, and transact within DeFi.

Overview

DeFi is the very foundation upon which a fair, trustless, and inclusive global economy is being built. Our purpose is to contribute to building this financial system; more specifically, shaping how users trade, invest, or transact.

Magpie protocol is a cross-chain liquidity aggregator that enables seamless cross-chain swaps with near-instant finality and cost efficiency on many of the top blockchains. Magpie uses bridges on the backend for communication and asset transfer, making for an extremely fast, secure, easy, and gas efficient solution.

Compared to other options in DeFi, when a user swaps using Magpie, they **don't** need to visit the corresponding bridge, learn how to use it, spend a bunch of gas on transfers, and time waiting, only to then have to find a DEX to make a swap. While in some ways similar to 0x, Paraswap, and 1inch, the advantage of Magpie

comes in its user experience, security, ease-of-use, and speed, all while providing users with the best prices on tokens both within-chain and cross-chain.

Problems in DeFi

DeFi solves a lot of issues, but that doesn't mean it isn't without its issues. Currently, there are no options out there for a permissionless, non-custodial, chain-agnostic cross-chain swap solution in which users are free to cross-chain swap or bridge any asset they wish with the same wallet.

Liquidity Aggregation

One of the hottest topics in the space, with TVL (Total Value Locked) increasing by 50% since January of 2023. While this is great in theory, in practice there are some problems, namely, that it's fragmented with liquidity spread across mostly the ten largest chains, but then further fragmented between hundreds of exchanges within those chains. This leads to capital inefficiency and higher costs to users, in both gas and time, with no fast and efficient way to bridge and cross-chain swap their assets.

At the beginning of the 2021 bull run, 96.8% of TVL was on Ethereum, with the remaining 3.2% being spread between about five chains. Now Ethereum makes up about 57% of TVL in DeFi with the other 43% spread between over one hundred other blockchains, 120 of them with over $100m in TVL. This causes quite the fracture between blockchains and exchanges for users to find what they want, quickly, and for a good price. It even becomes an issue within the same chain, liquidity spread across ten or even fifty exchanges, creating a need for users to

use liquidity or DEX aggregators to find the token and price they want.

Bridges

Most often not enough of a solution by themselves, bridges require users to need a DEX or DEX aggregator to complete the swap after using, as they're generally limited to stablecoins and native currencies, while Magpie is not. There are also too many bridges, each with their own unique user interface, limitations, system to learn, and time to bridge. Some apps (DEXs) or liquidity aggregators link to seven or more bridges, each for a different chain, that users would need to learn, navigate, use, and, in some cases, need a new wallet for. These apps allow deposits from a single chain only, forcing users to leave the app to bridge their funds, having to do a lot of hard work, paying a lot of gas fees, all just to be able to use the app they want to get to. In order to purchase assets on the new chain, users need that chain's native token, such as ETH, in order to complete any swaps on the destination chain, meaning users have to first purchase and bridge the native token and trade it for the token they want, adding another layer of complexity to the process.

Bridge Security

By using bridges, users are entrusting their tokens with the security of the bridge, not being able to keep them in their own wallets. This has been the cause of many exploits which have cost users over $1 billion dollars USD in the past couple of years. Magpie helps solve this problem by abstracting away bridge use for users and selecting the route which provides the best price.

User Experience

Requiring the use of so many different bridges and DEXs across multiple blockchains increases the price users are forced to pay, the time it takes to learn each system, and the time spent before they can make the swap for the token they want. Cost and time for approving, swapping, bridging, and sending all leads to opportunities lost, extra fees, and just complicates the process. It's not easy to use and it needs to be, as these issues keep a lot of retail users away and discourages many users from within the crypto space from participating in branching out within the DeFi ecosystem as well. As prices and available tokens can differentiate between exchanges and chains, it just exacerbates the issue in finding a place to swap or stake while getting what the user wants.

Price Issues

Gas prices and dealing with gas in general are some of the reasons that many retail users stay away from DeFi, with the price of transactions scaling with both the price of the native gas token and activity on the chain, prices can quickly skyrocket during bull markets. While this may not be as big of a deal for those with hundreds of ETH, when retail users can swap on a CEX for between a few cents and dollars, it becomes incredibly difficult to get them over to DeFi when transactions on ETH range wildly, with the average transaction for January of 2024 being between $5-10, but during the bull run from January of 2021 to May of 2022, the average gas price was around $40, and some days could even reach $200 for an asset swap. Even on the low end, swapping for $5 adds up over time, especially if you're trying to actively trade. Swapping, sending, staking, & bridging costs money.

Price disparity between exchanges or chains also makes it even more difficult to navigate through DeFi, where it isn't uncommon to see prices that are 1-5% different across chains on smaller tokens.

The Solution: Magpie Protocol

The easiest and simplest way to describe Magpie Protocol is that it facilitates cross-chain swaps without users needing to bridge assets by themselves. Magpie accomplishes this by sending messages using a data transfer protocol like Wormhole bridge to initiate and help execute a swap across chains. How will we solve the issues above? We'll give a short version of how we're tackling each problem as well as in depth descriptions of our architecture and further down.

Liquidity Aggregation

Magpie aggregates liquidity from the top DEXs and AMMs across all of the blockchains we're on: ETH, Polygon, BNB Smart Chain, Avalanche, Arbitrum, Optimism, Polygon zkEVM, and Base, with zkSync, Mantle, Gnosis, Celo, Manta Network, and Movement lab currently being worked on. This encompasses a large portion of all of the total value locked within AMMs in DeFi, allowing our unique aggregator to provide users with fast execution, response times, high order throughput, and the best prices both inter- and cross-chain.

Bridges

Magpie takes away the need for users to use a bridge themselves as Magpie Protocol aggregates liquidity from the largest bridges, meaning users don't need to worry about receiving synthetic tokens or learning how to bridge to each and

every chain, it's all built into the swap process with Magpie. All the user needs to do is select their starting and destination chain, we take care of everything else.

Bridge Security

Magpie Protocol is a non-custodial and trustless solution that uses bridges for both data and value transfer, in which the protocol & relayer does not have any central control over the funds that belong to users, making it much more secure than using traditional bridges.

User Experience/Onboarding

Magpie makes a large component of onboarding into DeFi as easy as can be. One app, one page, one interface, and incredibly easy-to-use. The Magpie team has already done all of the work and research for users, from aggregating DEX and Bridge liquidity, taking out the need to bridge to go cross-chain, finding the best prices, to figuring out where to buy the token. With Magpie Protocol's dApp, users can just choose which blockchain they're on, which one they want to go to, any two assets they want to swap, and we'll do the rest.

Price Issues

While we cannot change gas prices, we can help users get what they want, when they want it, for the best possible price. Magpie does this by facilitating users to swap on- or cross-chain between all of the major blockchains and DEXs. Our unique order routing algorithm will find the best path available to get the assets needed, even pulling from multiple sources if necessary.

magpie

The Process

Magpie aggregates both DEX and Bridge liquidity on all of the most popular chains to initiate swaps for the desired token. This results in users receiving their tokens very quickly, for much less gas, and not being limited to swapping stablecoins or the chain's native gas token like with most bridges.

There are four steps to the process:

1. Users select their pair and chain of choice.
2. They initiate the swap on the source chain.
3. Magpie swaps user assets to an asset which is supported by the bridge, deposits that asset to the bridge, it uses the bridges to send a swap instruction message to complete a token swap on the destination chain.
4. The bridge releases funds on the destination chain then the relayer, after confirming the message, completes the cross chain swap on destination chain which sends the chosen asset to the user's wallet.

The following infographic shows the steps involved for the end user while Magpie takes care of the complexities of aggregation and route calculation.

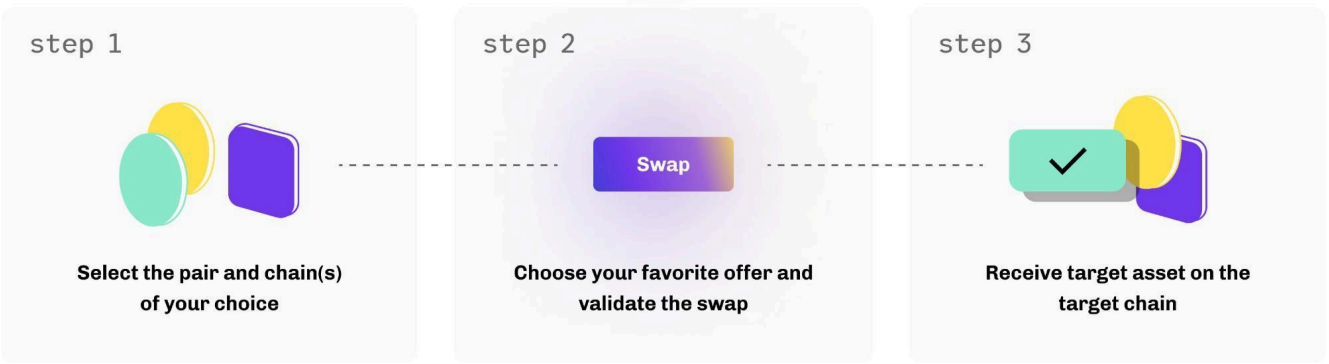


Fig.1: The user-experience is straightforward for the traders.

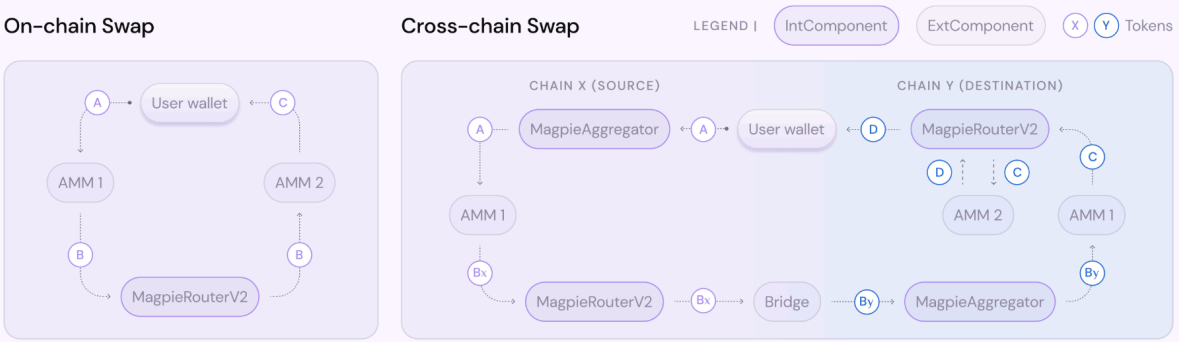
With that said, let's dive into the following components of Magpie Protocol and how they work: Architecture, Aggregator, Services, Liquidity, and Major Benefits. If you're interested in a more detailed description, follow us on our social media to be alerted as soon as the much more detailed whitepaper is released.

Architecture

The user chooses their pair and chains of choice. Once chosen, Magpie swaps user assets to an asset which is supported by the bridge, deposits that asset to the bridge, then it uses the bridges to send a swap instruction message to complete a token swap on the destination chain. Magpie sends a message through the bridge relayer messaging system. Once the bridge releases funds on the destination chain then the relayer completes the cross chain swap which sends the chosen asset to the user's wallet. Image below shows the flow of the system.

magpie

How it works under the hood.



Aggregator

The Magpie Aggregator calculates the route for swapping from one token to another. It uses an advanced proprietary routing algorithm which finds the most efficient paths for a token swap by splitting the order between different protocols (DEXs) and bridges to get the maximum amount of tokens for the user.

Fast Response

Magpie aggregator infrastructure is based on microservices, each having its own functions and purpose, they communicate with each other through message broker, we collect on-chain liquidity information of all the supported pools in the pool explorer via the block explorer which is updated whenever it detects any liquidity change event such as add, remove liquidity or swap, Aggregator service has all of the supported AMMs logic implemented within it along with routes discovery and distribution logic such as constant product formula,

balancer-weighted, stable-swap etc. It interacts with the pool explorer to get the liquidity information and calculate amountOut for a given amountIn, storing this on chain information in our database allows us to not directly call any contract functions to get amountOut and allows us to calculate the routes faster since it doesn't depend on getting a response from on chain contracts

Best Price

The infrastructure of Magpie aggregator makes it highly scalable and flexible. For example, if you want to swap tokenA to tokenC, it could be routed through tokenB first before converting it directly to tokenC.

tokenA → tokenB → tokenC

For intermediary token tokenB for other aggregators they most likely use predefined intermediary tokens and will not use any random token, as it will mostly likely be a token with high liquidity such as USDT, USDC, ETH, etc. For Magpie, this tokenB can be any token which allows Magpie to find and capture market inefficiency such as an arbitrage opportunity.

Cross Chain Communication

Magpie establishes interchain communication through a Wormhole Core Bridge where it sends messages from sender chain to the target chain. Wormhole relies upon a set of distributed nodes which monitor state on several blockchains referred to as Guardians, where the current Guardian set can be seen in the Wormhole Explorer.

It is these guardians' role to observe messages and sign the corresponding payloads. Each guardian performs this step in isolation, later combining the

resulting signatures with other guardians as a final step. The resulting collection of independent observations form a multisig, referred to as VAA's in Wormhole, which represents a proof that a state has been observed and agreed upon by a majority of the Wormhole network.

Messages emitted by contracts need to be verified by the guardians before they can be sent to the target chain. Once a majority of guardians reach consensus that an observation has been made, the message is wrapped up in a structure called a VAA which combines the message with the guardian signatures to form a proof. These VAA's are ultimately what a smart contract on a receiving chain must process in order to receive a wormhole message.

Magpie Intents

Magpie Intents represents a notable shift from conventional transactional models, putting the user at the heart of their financial journey, allowing users to initiate transactions by stating their desired outcomes, such as asset swapping or providing liquidity. The process starts when users place a reward on the source chain, demonstrating the seriousness of their intent. This reward acts as an incentive for solvers, creating a fair compensation system for their work.

Solvers use advanced algorithms and strategic thinking to understand user intents and develop the best strategies for achieving the desired results on the destination chain. A reward commitment on the source chain serves as a binding contract that reinforces user intent, ensuring the ecosystem is fueled by authentic, significant transactions.

Fast Execution

Magpie Protocol seamlessly translates intent into action through a well-defined workflow. Users define their intent and lock a reward on the source chain. Solvers

retrieve these intents, strategize optimal solutions on the destination chain, and execute them. The proof of settlement on the destination chain provides a transparent validation of the completed transaction. The protocol also introduces time dynamics, allowing users flexibility in setting lock times, and solvers can strategically manage time through fine payments for extensions.

Magpie Intents aims to redefine the landscape of decentralized transactions. By focusing on user-defined intent and solver creativity, the protocol serves as a testament to the infinite possibilities within DeFi.

Magpie Micro Services

The **Aggregator Service** provides an API endpoint that returns a quotation for a token swap. It calculates the best route to exchange tokens using graph search, based on the data collected by the pool explorer service, which is prioritized based on available liquidity in USD. It performs price impact calculations off-chain based on the collected data in order to find the best deal for the user.

The **Pool Explorer Service** makes sure that our system has all the necessary information from the integrated AMMs on each chain. Accomplishing this in two ways: it subscribes to listen to the pool contract of all the pairs of the AMMs that have been integrated and it updates token reserves of that pool in case of any swap event that it fetches and it gets the pool data from the subgraph of AMMs, and queries the subgraph to get all pairs and their reserve of all the supported AMMs.

Block Explorer

If a service wants to listen to blockchain events, it has to register in Block Explorer

for the event. The Block Explorer goes through all of the blocks and sends event information to subscribers. If there was an error or interruption in running of Block Explorer, or there was a reorg, the Block Explorer goes through the archive blocks and sends the missing information to subscribers.

The **Token Provider Service** keeps the token list up to date, whenever there is any pool creation event detected then token service checks whether there is any new token that needs to be added to the token list and adds new token if it is not present in the token list already. It also collects and stores USD price data for all tokens that are emitted by the aggregator service.

Token Manager and Provider

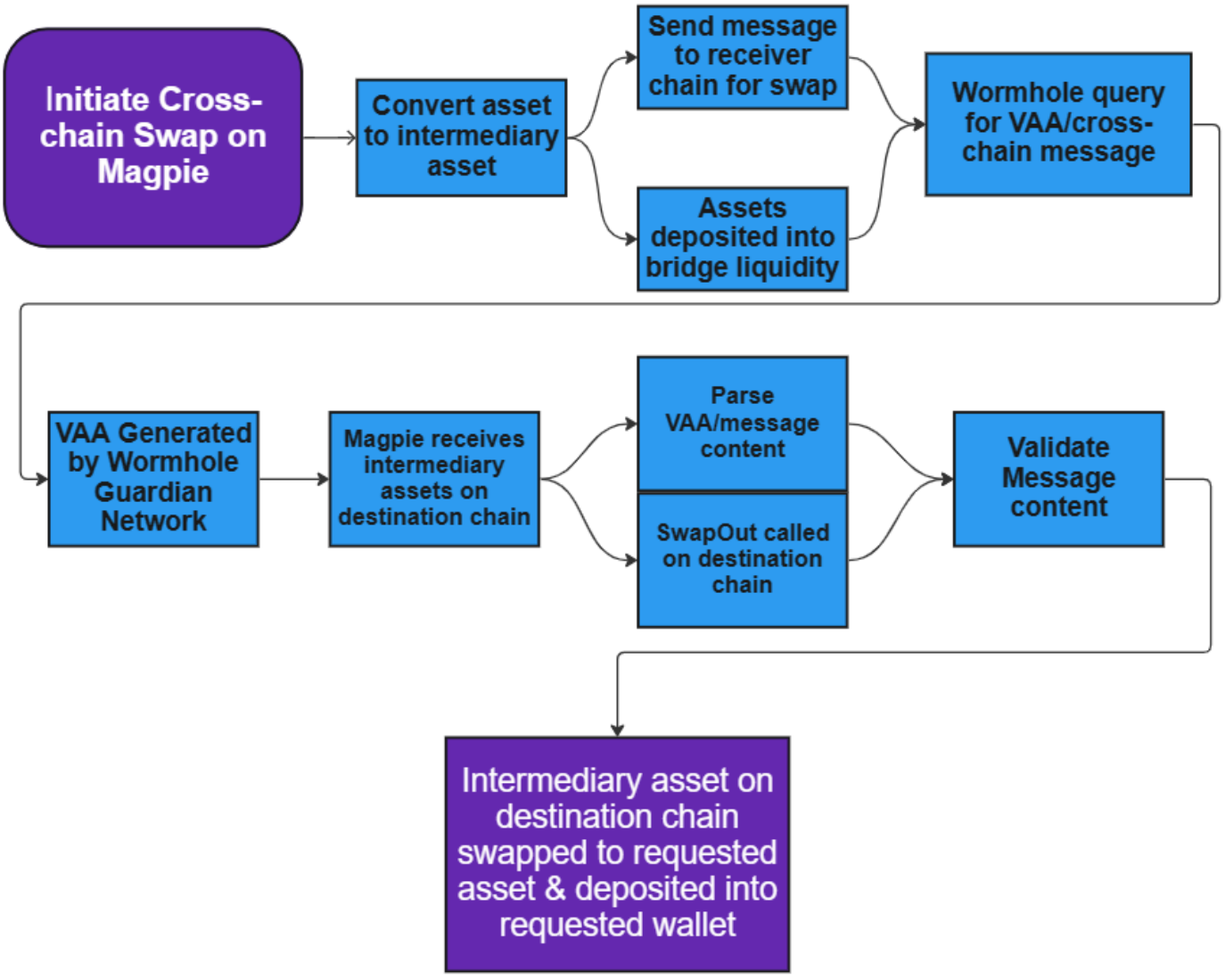
It stores current token information, fetching and serving token icons. The service is fetching token icons from CoinGecko and CoinMarketCap APIs.

The **User Service** keeps track of user balances and transactions, provides an api that is used by frontend user interface to get user swap transaction status. The **Relayer Service**, which is part of the User Service, listens to swapIn event on all supported chains, it queries information from data transfer protocol and bridge then it calls swapOut on the target chain

Finally, the **Message Broker** handles the communication between the services.

magpie

Life Cycle of a Cross-chain Swap through Magpie Protocol



Liquidity Pools

Magpie Protocol aggregates liquidity through various bridges so we have access to large amounts of liquidity on each blockchain that they connect to. Utilizing this, Magpie Protocol's intrachain liquidity aggregator can quickly swap for the token of the user's choice.

Token - FLY

Magpie's native token is FLY and will work as a governance token and rewards share. FLY token will accrue protocol revenues to stakers directly . Protocol revenues come in the form of trading fees and % of the profits will be distributed in a non-native asset to the stakers along with staking rewards.

magpie

Major Benefits of Magpie Protocol

At Magpie, we wanted to help everyone realize the potential of DeFi. Magpie has spent years learning the ins and outs of everything, doing the research and learning for the user, and implementing all that knowledge into the protocol, so that the user doesn't need to. That's what makes Magpie such a great experience, it cuts out the unneeded time wasting involved in a lot of DeFi.

Magpie Protocol is **chain agnostic** in nature, so we are not limited to 0x, 1inch, or other such protocols and can be deployed to and used to bridge *any network to another*, even EVM to non-EVM.

Magpie is **scalable**. By using our unique smart algorithm, low-cost backend system, Wormhole based cross-chain communication, and aggregating billions in bridge and DEX liquidity, Magpie can easily scale to handle new users, while providing them all with the best prices. All of this together results in lower fees (just one swap fee), lower gas, low slippage, and faster transactions (2 block finality). Additionally, Magpie will be adding a solver network with our Intents system to ensure all our users get even better pricing, faster.

At this time, our aggregator and order routing has shown to provide better prices on assets over 85% of the time when compared to 0x based aggregators and exchanges, and better than 1inch over 50% of the time, each percentage increasing in value as trade sizes increase. The larger the trade size using Magpie, the better our router is at finding users the best price.

Magpie has an incredibly **slick user interface** that abstracts away all of the complexities of using traditional bridges and multiple AMMs, making for an amazing user experience. It's as simple as selecting the current chain, token pair, destination chain, and then swapping - it doesn't get any easier. Don't need to

swap cross-chain? Don't worry, Magpie will help find you the best deal on-chain as well.

Magpie works with almost **any asset** and is not limited to stablecoins. Unlike most bridge solutions, liquidity for each and every token that users want to swap for is not required as the protocol handles the swaps on each end through the Magpie Liquidity Aggregation Protocol.

Magpie is **secure and censorship resistant** as it is non-custodial, not relying on any third-party control, there is no need for them to trust anyone else with their assets. Magpie primarily uses Wormhole for data transfer which has 19 Guardian Nodes to verify each and every message sent cross-chain through the Wormhole Guardian Network to make sure the message is secure.

Magpie **APIs** makes it possible for dApps and other protocols to easily integrate with Magpie to make cross-chain yield-farming, NFT buying, or borrowing/lending as easy as ever, and as easy as just a couple of clicks, all in one interface.

Magpie is **more than cross-chain swaps**, it solves the existing issues faced by DeFi protocols and developers to build unified and interoperable apps with shared state and liquidity across different chains; it acts as an infrastructure layer that provides protocol interoperability across chains.

magpie

Magpie's unique selling point is that it uses a unique routing algorithm, routing through any token in order to find the best price for the user, all while abstracting away the complexities of DeFi. By using bridges for both data and value transfer, using relayers to initiate swaps on AMMs on the destination chain, which in turn allows anyone to complete a cross-chain swap without visiting a bridge or DEX.

Find us online

Website: **www.magpiefi.xyz**

Telegram: **https://t.me/magpieprotocol**

Twitter: **https://twitter.com/magpieprotocol**

Medium: **https://medium.com/@Magpieprotocol**