Ponder Whitepaper

Version: 1.0

DISCLAIMER AND NOTES

For the avoidance of any doubt, Ponder including but not limited to the overall project, the website, all its software including the PNDR Token, any smart contracts and user interfaces that are going to be developed and/or deployed in the future ("Ponder Platform") as presented in this conceptual paper is a pure software comparison tool and aggregator and it is not (not it is required to be) an active licensed or regulated or exempted financial, or payment or digital asset service of any kind and in any jurisdiction. Any terminology used in this document, on the website or within any app or in general in the Ponder Platform is intended only as a basic reference, without any effective or legal meaning of the same terms in a financial environment, and/or any other regulated framework. The PNDR Token itself is a strictly utility token in any jurisdiction and is not and can not be considered as a security or otherwise a regulated token of any kind, is not in any way e-money and/or a fiat or asset backed stablecoin, whether global or limited in scope. This document taken by itself is not, nor it can be construed as a contract, an investment contract or a contractual agreement of any kind, it is not an invitation or offer to invest in any of the legal entities developing, fostering or managing the Ponder Platform, in the Ponder Platform itself or to acquire or use the PNDR Token in any way with any expectation of future profit, whether or not arising from the effort of others. Any user intending to use any aspect of the Ponder Platform declares to have received appropriate technical, administrative and legal advice before and after reading this document, the website and using any part of the Ponder Platform (including any tokens therein) and accepts that there is an inherent high risk in acquiring or using any kind of blockchain and/or crypto token, platform, software, interface and acknowledges with full disclaimer for any of the persons or entities mentioned within this document or in any way directly or indirectly connected to the Ponder Platform, including any legal entity directly or indirectly connected, that there can be any kind of damage suffered, including total loss.

Foreword

This document will attempt to outline the idea and implementation details for the "Ponder" solution being proposed to compare, contrast and choose the best service providers when dealing with digital assets across chains.

Introduction

Web3 is the new frontier of tech where every day we see innovative solutions making headlines with billions being poured in by venture capitalists. As more solutions are built, be it a bridge, NFT marketplace or simply another borrowing and lending platform, it adds a layer of complexity to end users' experiences. Given how counterintuitive the current UX is in Web3 space the additional complexity adds to the already existing problem of users' ability to navigate the space and find the best products for their needs at the cheapest cost. It can be overwhelming to a new user to understand solutions such as bridges or DeFi protocols let alone try to use them to their advantage.

This is why we built “Ponder”, simply put; a comparison engine that scans across chains and protocols while hiding cryptocurrencies complexities through a simple, intuitive and clean UI/UX for a range of Web3 services, starting with bridges.

Background

Highlight the background of why Ponder was even thought of as a solution. Outlook of growing services and growth in the space. Problem statement and solution.

Problem

In today’s cryptocurrency world, there are numerous bridge providers, DeFi protocols and NFT marketplaces. Each solution has its advantages and disadvantages. This can be overwhelming for end users. Given the current complexities and hurdles already in place in Web3 in terms of UI/UX, the growing number of services will perpetuate this experience as the space becomes even more technical and more brutal to explore. There are many smart and innovative technological solutions for bridging, borrowing/lending, and dealing with NFTs but without a true comparison site, it is becoming increasingly complex and confusing on deciding, even discovering which of these solutions one should use. As the number of bridges is expected to grow by multitudes in 2023 onwards, along with the new frontier of DeFi and NFT dApps coming online, it is evident that a fully integrated comparison tool is required to allow users to pick and choose the best options out there without having to navigate a wide range of dApp websites and doing manual comparisons.

Solution

Ponder will build a fully integrated comparison product that allows its end users to compare and choose the best option whether it's bridging, borrowing/lending

or dealing with NFT Marketplaces. Ponder will plug into partners' solutions at both SmartContract and API levels to provide a seamless and fluid user experience where users can carry out their actions all within a single intuitive interface. Ponder is synonymous with its Web2 counterparts such as "PriceGrabber" from the US or "CompareTheMarket" from the UK.

Ponder will in phases attempt to compare various bridges, DeFi solutions, NFT Marketplaces and more, to provide a detailed breakdown to the end user on options available allowing users to make an educated choice while saving them money and time.

Ponder Ecosystem

Ponder will be built in multiple phases, with each phase attempting to simplify and cover different aspects of Web3(and DeFi) to provide its end users simplicity and abstraction thus improving user experience while building an inclusive solution for all providers' new and existing across the space.

Ponder Roadmap

Ponder encompasses many phases and products within each phase. Having a realistic timeframe and giving high-level visibility(transparency) of what is set to be achieved is crucial. Ponder aims to cover all of its phases detailed in the previous section within a 24-36 months time frame. Given phases such as “DAO Transition'' is dependent on many dynamic variables such as user maturation, market share, and general Web3 maturity it is relatively a hard phase to set a strict time frame for, however, the roadmap below aims to set realistic timeframes and the dates at a high level across the board.

Given phases like “DAO Transition'' is dependent on many dynamic variables such as user maturation, market share and general Web3 maturity. It is a relatively hard phase to set a strict time frame for, however, the roadmap below aims to set realistic milestones and dates at a high level across the board.

✅	***Phase 1 = Q1 2024***	Bridges
✅	***Phase 2 = Q1 2024***	Swap Aggregator
🛠️	***Phase 3 = Q2 2024***	DeFi, (Re) Staking Protocols, RWA Markets
🛠️	***Phase 4 = Q4 2024***	NFT Marketplace Aggregator, Ordinals and BRC20s
🛠️	***Phase 5 = Q1 2025***	DeFi Insurance, DePIN, Ramps and Wallets
🛠️	***Phase 6 = Q2 2025***	Investment DAOs

Phase 1 - Bridges

This first phase will attempt to use multiple bridge providers via multiple infrastructure providers to allow the flow of funds across both EVM and non-EVM chains. The first iteration will focus on digital currency/token flow.

Phase 2 - Swap Aggregator

The second phase will utilise architecture and integrations from the previous phase to start integration for swap providers across the space. The aim is to allow end users to bridge and swap within the Web3 world, providing the users with an intuitive and easy-to-understand dashboard whilst covering key information comprehensively.

Phase 3 - DeFi, (Re) Staking Protocols, RWA Markets

Building on the success and architecture of the previous two phases, this phase will start focusing on direct comparison and integration of various DeFi protocols, (re)staking protocols, RWA markets and more. The aim of this will be to allow end users to; bridge, search, compare, swap (where necessary) and finally execute DeFi and (re)staking operations such as PoS participation, EigenLayer AVS securing, yielding, liquidity mining, lending, borrowing and a lot more.

Phase 4 - NFT Marketplace Aggregator, Ordinals and BRC20s

Designed to query, compare and present direct buy/sell of NFTs across the space on various chains including Ordinals and BRC20 inscriptions on BTC network at the lowest fees and the best prices. While providing full-scale data analytics for search collections and individual NFTs allowing end users to make an educated and well-informed decision before executing a trade.

Phase 5 - DeFi Insurance, DePIN, Ramps and Wallets

The fifth phase will be the start of the “end game” for Ponder as it attempts to warp in offerings from across the space to provide its users ability to compare service and offering not only at the access layer but going down to infrastructure layer by integration DePIN offerings. As well as comparing fiat ramps and even wallets allowing users to make an educated decision based on various parameters and traits each service provider may offer.

Phase 6 - Investment DAOs

Built on the success and comprehensive outlook provided by earlier phases, Ponder will strive to aim for alternative angles of investment opportunities for its end users. Ponder will integrate and compare several Investment DAOs that are existing today to allow users to discover, compare and enter various investment DAOs.

Foundations of Web3

Bridges

Within the blockchain space, bridges refer to the conduit through which value can be transferred between two blockchain ecosystems. These bridges are fundamental to enabling flows of information and tokens between blockchains. Due to the structural differences between L1s, they are not able to inherently communicate with other ecosystems. This is why bridges are fundamental to connecting and growing blockchains and ultimately the monetary system in which they create.

There are a variety of ways to classify the different types of bridges based on their internal mechanisms, ways of reaching consensus and the function in which they serve. As there is a multitude of ways to differentiate bridges, each bridge will incorporate multiple classifications. Some examples of bridge classification are

One-way (unidirectional) bridges - A general distinction of bridges, meaning users can only bridge assets to one destination blockchain but not back to its native blockchain.

Two-way (bidirectional) bridge - As opposed to one-way bridges, two-way bridges will allow asset bridging in both directions.

Custodial bridge - Require users to place their trust in a central entity to properly and safely operate the system.

Non-custodial bridge - Operate in a decentralised manner, relying on smart contracts to manage the crypto locking and minting processes, removing the need to trust a bridge operator.

Multichain bridge - Exchange many tokens in a large number of networks. Multichain crypto bridges can also interact with many cryptocurrency wallets.

DEXes

Decentralised exchanges (DEXes) are blockchain protocols that function as peer-to-peer cryptocurrency marketplaces that facilitate direct transfers of value without the need for a trusted intermediary. The advent of DEXes has allowed cryptocurrency participants to execute trades and transfers in a permissionless way that aligns with the core values of decentralised finance (DeFi).

There are various components and mathematical formulas that create the foundational logic of the DEX. Below is a breakdown of these aspects.

Automated Market Maker (AMM) - An underlying SmartContract that operates on and serves as the engine for DEXes by using formulas to automate trading token pairs efficiently and provide liquidity for transactions with the use of liquidity providers.

Proactive Market Maker (PMM) - Developed in-house by DODO, it is a type of AMM that improves capital efficiency, lowers impermanent loss and reduces slippage for participants on the DEX. These protocols aggregate liquidity and gather accurate price data with the use of on-chain oracles. PMMs can make one-sided deposits and withdrawals, change the price curve whenever desired and can provide precise liquidity at any given price point.

Constant Product Market Maker (CPMM) - Introduced by Uniswap, this iteration of an AMM uses a specific formula to establish continual liquidity within the DEX. CPMMs utilise the mathematical function:

$$(Rx - \triangle x)(Ry + (1-f)\triangle y) = k$$

Within the formula, **Rx** and **Ry** represent the reserves of each token, **f** is the transaction fee, and **k** is the constant. This equation produces a range of prices for the two tokens following the available quantities of each particular token.

Constant Sum Market Makers (CSMM) - A variation of an AMM, this formula creates the best possible outcome when attempting to minimise price impacts during trades, but has the drawback of not providing infinite liquidity. The equation is expressed with the following function:

$$(Rx - \triangle x) + (Ry + (1 - f)\triangle y) = k$$

Within the formula, **Rx** and **Ry** represent the reserves of each token, **f** is the transaction fee, and **k** is the constant. Although similar to CSMM, the formula plots a straight line when graphed as opposed to a concave curve on the CSMM graph. The downside is that this formula creates large arbitrage opportunities for traders to drain the liquidity if off-chain prices for the tokens aren't in synchronisation. Due to this fact, this particular mode is very limited in its use case.

Constant Mean Market Makers (CMMM) - Made popular by Balancer, this type of AMM allows for more than the standard two assets (50:50 ratio) liquidity pool system. This formula can establish a balanced weight of up to eight different assets within a single pool. This equation can be expressed by the following simplified example:

$$(x * y * z)^{(⅓)} = k$$

Within the formula, **x** represents “token 1”, **y** is “token 2”, **z** is “token 3”, and **k** is the constant. The fraction within the formula will always be 1 divided by **x**, with **x** being the number of tokens. In this example, there are three tokens (x, y, z), thus (⅓).

Virtual Automated Market Makers (vAMM) - Launched by Perpetual Protocol, it essentially takes the CPMM model created by Uniswap and keeps all of the aspects of the formula, but changes the **k** (constant). In this formula, **k** represents not the constant actual liquidity but rather a SmartContract that holds all of the assets that are backing this AMM variation. The “virtual'' component of the vAMM, refers to the fact that what is being swapped in the AMM is virtual synthetic assets, similar to derivatives.

Staking

Cryptocurrency staking refers to the process in which token holders lock up their tokens for some time in exchange for more tokens in the form of interest at the end of a fixed or dynamic period. There are a few separate types of staking structures that can vary greatly depending on the purpose they are serving for the protocol. Some forms of staking are used simply to give the participants rewards while others are used as fundamental aspects of consensus. The definitions below describe the variations.

PoS Staking - A form of staking that creates a consensus mechanism which can validate cryptocurrency transactions on a blockchain. Stakers are rewarded with a portion of the transaction fees for validating the blocks and securing the network. This method is in contrast to the Proof of Work consensus mechanism which was popularised by Bitcoin.

Delegated PoS Staking - This variation on PoS staking allows token holders to essentially vote by pooling tokens together to delegate nodes which operate the validation system on the blockchain. Combining tokens and creating nodes, increased the probability of being selected to perform the necessary work to validate the network and earn the rewards. This simplifies the validation aspect of token holders who want rewards but don’t have either the time, resources or knowledge needed to operate a node themselves.

Soft Staking - This distinction within cryptocurrency staking refers to the time in which you can unstake the tokens. With soft staking, there are no set lock-up periods. Users can withdraw their tokens from the staking SmartContract at any time. This gives participants more flexibility but generally fewer rewards.

Hard Staking - The inverse of soft staking, this distinction within cryptocurrency staking has a set and defined period in which a user must keep their tokens

within the staking SmartContract to receive full rewards. In some cases, rewards can simply be “slashed” or reduced if users exit before the required time is complete. In other cases, users are simply unable to exit until the time is completed.

Re-Staking - Restaking, as exemplified by EigenLayer's Advanced Validation Services (AVS), enables the use of staked assets to secure additional networks without un-staking. Users can lend their staked assets' security to validate transactions on other blockchains within the EigenLayer ecosystem, compounding their rewards without the need to withdraw their original stake. This innovation enhances network security and interoperability, allowing stakers to maximise their investments' utility and rewards across multiple protocols seamlessly.

DeFi

Decentralised Finance or DeFi for short, is a component of blockchain technology that focuses on combining the core tenets of blockchain and the traditional finance (TradFi) industry. This general term applies to several practical use cases and platforms within cryptocurrency. DeFi aims to build a better financial system that is permissionless, trustless, sovereign and secure. Ultimately the goal of DeFi would create a system that cuts out the middlemen or gatekeepers who currently have control of who can participate in monetary transactions. This democratisation would allow for more participation across the global ecosystem. The following terms below explain the different aspects of DeFi.

Lending/Borrowing - This vital part of DeFi allows cryptocurrency users to either lend their tokens in exchange for interest or borrow tokens from a protocol or counterparty with fast settlement times. Due to the differences inherent to blockchain technology, these systems differ from lending and borrowing in traditional finance. For example, the borrower must provide collateral for loans generated on the platform. This ensures the system can stay solvent and that users have the incentive to pay back their loans. This avoids the need for “know your customer” (KYC) on some platforms, which is required for all regulated banks in the traditional finance world. Additionally, these transactions can take place much quicker within DeFi and generally take only a few minutes to complete, which benefits lenders and borrowers alike.

Yield Farming - Similar to staking, yield farming (aka farming) allows users to earn rewards for depositing assets into liquidity pools in exchange for token rewards. The main distinction between the two is that farming requires at least two different tokens to be added to the pool simultaneously. While this method of earning interest can be more lucrative, it can also be riskier due to issues such as impermanent loss. This means that when prices are volatile the change in token prices can cause an individual's share of the liquidity pool to be less

valuable than when it was deposited. Although the price can increase back to the original price if the market moves to the price the tokens were deposited at, thus “impermanent” loss.

Derivatives - This type of cryptocurrency asset is fundamentally the tokenized version of derivatives from traditional finance. Both DeFi and TradFi derivatives are financial contracts that are used by buyers and sellers to trade the underlying asset instead of the asset itself. These contracts are generally satisfied once a particular set of requirements are met, such as a certain length of time or the price of the token. This asset class can be divided into two major subcategories, which are “futures contracts” and “options contracts.”

Futures contracts - These assets create an agreement that represents an individual’s right to sell or buy a token in the future at a specific predetermined price point. For example, to buy BTC for $30,000 in 5 months, regardless of the current price at that future date. The main difference between futures and options is that a future is legally binding meaning the investor must execute the agreed terms at the end of the period whereas options are not obligatory.

Insurances - Similar to how traditional insurance operates, crypto insurance protects an individual or group against potential cryptocurrency losses associated with a variety of negative impact factors, such as theft, data breaches, or human error. Policies can be obtained via crypto insurance companies and can vary in price depending on the value of the funds being secured.

NFTs

NFTs, or Non-fungible Tokens, function similarly to traditional tokens in cryptocurrency but with a key distinction: each token is unique and cannot be traded one-for-one with any other NFT due to its distinct characteristics. These tokens are indivisible and possess unique metadata that differentiates them from others, allowing for immutable proof of existence and ownership on the blockchain. This concept extends into the Bitcoin network through innovations like Ordinals and BRC20 inscriptions. Ordinals inscribe data onto individual satoshis, creating unique digital artefacts or NFTs within Bitcoin, while BRC20 enables the creation of tokenized assets, similar to Ethereum's ERC-20 tokens but on the Bitcoin blockchain. These developments allow for a diverse range of applications, from digital art to more complex financial instruments, integrating NFTs into DeFi borrowing and lending protocols. As the technical infrastructure around NFTs expands, their functionality evolves beyond mere tradable assets, encompassing everything from digital representations of art to tokenized versions of real-world assets like property deeds, clothing, and identification.

Investment DAOs

DAO stands for Decentralised Autonomous Organization. A DAO is a type of organisation that is run using blockchain technology and SmartContracts, allowing it to operate autonomously and without the need for a central authority. Investment DAOs are a specific type of DAO that is focused on investing, typically in blockchain-based projects or other forms of cryptocurrency. Investment DAOs are often open-source and decentralised, allowing anyone to participate and potentially earn a return on their investment. However, it is important to note that investing in a DAO carries significant risks, as with any other form of investment, and it is important to carefully research and evaluate any potential investment before committing funds.

Zero-Knowledge

Type of proof in which a prover can convince a verifier that they know a certain piece of information, without actually revealing the information itself. This is often achieved through the use of mathematical concepts, such as number theory, to create a proof that is both short and easy to verify but is also completely unlinkable to the original information. The idea behind zero-knowledge proofs is that they allow for the verification of a statement without actually revealing any sensitive information. This can be useful in many different situations, such as in cryptography, where zero-knowledge proofs can be used to prove that someone has the correct decryption key without actually revealing the key itself.

Optimistic Roll-ups

Optimistic roll-ups are a type of blockchain technology that assumes posted transactions are valid unless proven otherwise through the submission of a fraud-proof. This "innocent until proven guilty" approach allows for efficient processing of transactions, as only invalid transactions need to be further verified. In case of an invalid transaction, a dispute resolution system is used to verify fraud proofs, detect fraudulent transactions, and disincentivize bad actors from submitting invalid transactions or incorrect fraud proofs.

ZK Rollups

"Zero-knowledge" roll-ups, or ZK-rollups, are a specific type of roll-up technology that makes use of a cryptographic concept called zero-knowledge proofs to efficiently verify transactions without revealing sensitive information. In the case of ZK-rollups, multiple off-chain transactions are bundled into a batch, and a cryptographic proof called a ZK-SNARK (succinct non-interactive argument of knowledge), is generated to go along with the batch of transactions. This proof is then used to verify the transactions on the main blockchain (layer 1), using a "guilty until proven innocent" approach. This means that transactions are only

accepted on the main blockchain after the ZK-SNARK proof has been validated. This is in contrast to "optimistic" roll-ups, which take an "innocent until proven guilty" approach to validation.

zk-STARK vs zk-SNARK

ZK-STARK and ZK-SNARK are both types of zero-knowledge proofs, which are a type of cryptographic proof that allows a prover to convince a verifier that they know a certain piece of information, without revealing the information itself. The main difference between ZK-STARK and ZK-SNARK is in their underlying technology and implementation.

ZK-STARK, which stands for Zero-Knowledge Scalable Transparent Argument of Knowledge, is a relatively new type of zero-knowledge proof that is based on a type of mathematical proof called a "transparent argument of knowledge." ZK-STARKs are considered to be particularly efficient and scalable and do not require a trusted setup (a one-time, potentially vulnerable process that is needed to generate certain types of zero-knowledge proofs).

ZK-SNARK, which stands for Zero-knowledge Succinct Non-Interactive Argument of Knowledge, is a more established type of zero-knowledge proof that has been used in several blockchain projects. ZK-SNARKs are based on a type of mathematical proof called a "non-interactive argument of knowledge," and are considered to be particularly short and easy to verify. However, ZK-SNARKs do require a trusted setup.

Ponder Implementation

Ponder is designed to be modular and extensible by default. There are several moving components within the Ponder architecture and additionally given the speed of change and evolution in Web3, the architecture has to be easily extensible to cover today's and tomorrow's trends, thus, stay relevant as a comparison engine for the Web3 no matter the trends and changes the future may bring. The Ponder team has chosen modular architecture for its engine and integration due to:

- *Improved maintainability*: Modular architecture makes it easier to update, maintain, and modify individual components or modules without affecting the rest of the system. This can reduce the overall cost and effort of maintaining the system and can make it easier to introduce new features or improvements.

- *Increased flexibility*: Modular architecture allows different components or modules to be easily swapped in and out of the system, depending on the specific needs or requirements. This can make the system more adaptable

and flexible, enabling it to be easily customised for different use cases or environments.

- *Enhanced scalability*: Modular architecture allows for the independent scaling of different components or modules, depending on the specific demands and workloads of the system. This can improve the overall scalability and performance of the system and can make it easier to handle large volumes of data or traffic.

- *Improved reliability*: Modular architecture allows for the independent testing and debugging of different components or modules, which can improve the overall reliability and stability of the system. This can reduce the likelihood of system failures or downtime thus improving the user experience.

Shared Components

Before diving into individual phases and their niche, it is important to lay out the blueprint of the entire ecosystem and highlight some of the components shared across all phases. These components serve as the "backbone" of the entire project be it at a B-2-C or B-2-B level.

Ponder Engine

The engine is the main component and backbone of the entire Ponder ecosystem. The idea behind the engine is to serve as the central component where all new providers identified today and in the future will plug into. For example, the engine will plug into several providers such as Socket.Tech, LayerZero and more to allow for a wide spectrum of options and compare products across the space. Given the engine will serve as "glue" code across different providers and options it must be built with scalability and extensibility in mind. The engine will connect to providers via both direct SmartContract integrations and Interoperability Protocols like LayerZero to offer the most comprehensive outlook on services individuals need.

Ponder API

The main integration point of any service provider is by default its API suite. Ponder strives for both B-2-C and B-2-B integrations across the industry. Given the long-term vision of offering Ponder's feature set as a service to anyone who wishes to utilise the framework, subject to PNDR token payments, will be able to plug into the API and start utilising its product suite for both Web2 and Web3 end users. Ponder API will be initially utilised by Ponder's frontend platform but with time public facing endpoints along with industry-standard API documentation will be made available for anyone to use. Ponder API will serve

as a wrap(abstraction) layer to Ponder Engine and end users (developers) can simply call endpoints in both REST and GraphQL standards.

Transaction Indexer Module

The module is used to watch, process and index all blockchain transactions that end users at both B2B and B2C levels may execute via Ponder. This means that it creates an index or database of all of the transactions that Ponder users have executed on the blockchain, making it possible to quickly and easily search and query the blockchain to find specific transactions or to gather information about the state of the blockchain at a particular point in time.

The indexer module will be plugged into each chain that is supported to allow for the watching events to push out notifications across the board wherever required. The module will be built as an independent microservice with scalability in mind as the number of transactions and events to watch will grow exponentially.

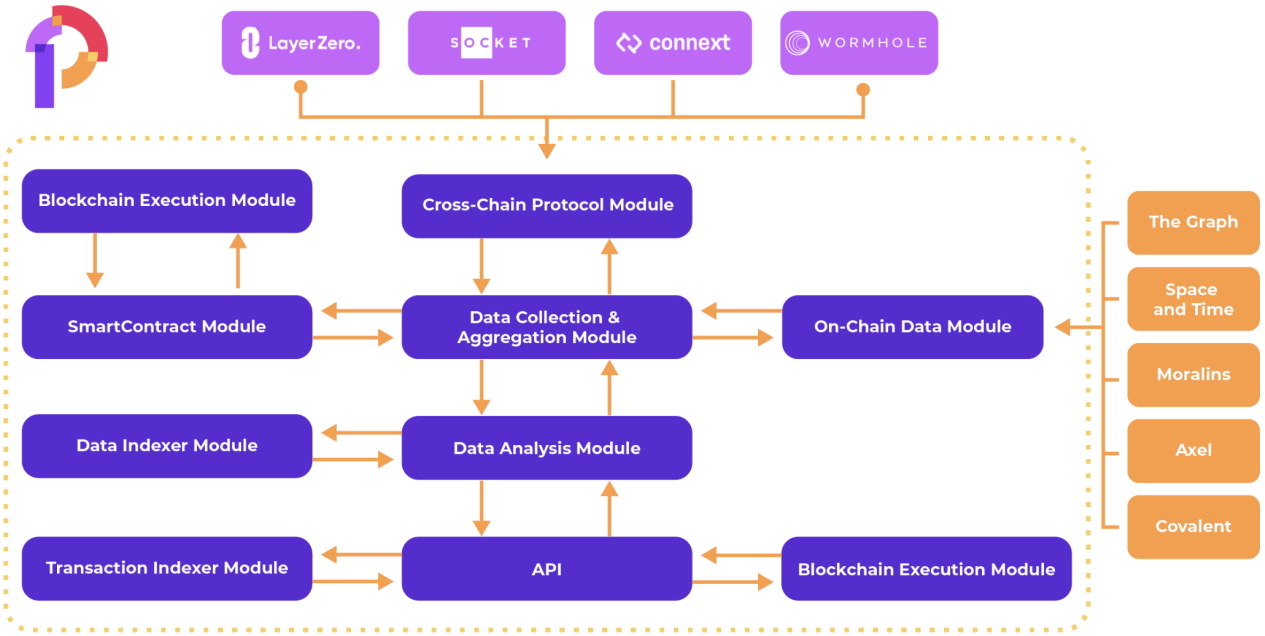
Blockchain Execution Module

One of the key shared components of Ponder across its architecture is the blockchain execution module. The module is responsible for direct RPC and Web3 integration and broadcasting of transactions on relevant chains depending on the end user's commands. The module essentially serves as Ponder's interface to all blockchains that are supported and wherever possible is directly integrated with private RPCs and MEV-protected RPCs to allow for instantaneous broadcasting and privacy.

deBackend

A decentralised Backend is the overall structuring and release of both the *engine* and the *Ponder API*. Both components will be wrapped up and released on a centralised provider like AWS initially but Ponder team's end goal is to decentralise the infrastructure hence the name "*deBackend*" through providers like 4everland, dFinity, IPFS, Arweave and more. Ponders end goal is to become decentralised as per philosophies the founders believe in and operate on its chain eventually where each node will run both the engine and the API to collect, aggregate, analyse and serve comparison data to its end users.

Along with deployment changes from centralised to decentralised, the long-term vision is to open-source the code behind the engine to allow engineers around the globe to extend and improve the feature set and earn PNDR tokens in return for their efforts.



Phase 1 - Bridges

The initial goal of Ponder through the MVP will be to compare and contrast major existing bridges and will aim to grow its integration list continuously.

Ponder will plug into all the major audited liquidity providers such as AnySwap, Stargate etc wherever possible at the SmartContract level to have native support for each solution. Based on values entered by the end user, multiple bridge providers will be queried in real-time to get an overview of the following vital data which will help the end user make an educated decision.

- Cost of Transfer
- Bridging Fee
- Time Required
- Trust Score
- Route Overview
- Ponder fee

The solution will allow the execution of trades to bridge assets in real-time through our UI rather than directing users to the actual bridge provider UI. This will ensure that individuals can request quotes, compare results and execute all in a single flow without ever leaving Ponder.

Phase 2 - Swap Aggregator

Phase two will build on the strengths and capabilities of phase one and the Ponder engine. The end goal here is to allow for cross-chain and truly interoperable trading without any friction. Ponder engine will be extended to support a wide range of DEXs across several chains, starting with EVM chains

and will strive to offer end users the best swap rates and minimal cost. The end goal of phase two is to address fragmented liquidity across chains thus lower slippage, increasing throughput and overall creating a more liquid Web3 ecosystem. The engine will directly plug into several exchanges at the SmartContract level and the API level via its interoperable protocols like LayerZero, Socket.Tech while providing a comprehensive outlook to its end-user on data points such as;

- Exchange Rate
- Fee structure
- Slippage
- MEV Protection
- ZK Relays (Private Transactions)
- Availability of Liquidity
- Risk Scores

Phase 3 - DeFi, (Re) Staking Protocols, RWA Markets

As part of efforts to build a comprehensive comparison engine for Web3, Ponder will aim to integrate itself directly with DeFi protocols across chains allowing end users to enter and exit DeFi positions and even move positions across chains all from a single hub. Phase three will begin with integrations of some of the largest DeFi protocol integrations starting with AAVE, Compound, Liquity and several more blue-chip names within the space.

DeFi generally speaking has many moving parts that tend to plug into each other one way or another. This is in line with the concept of “lego blocks of money”. DeFi is a collective effort with no intermediaries in between. However, the problem with DeFi and in general Web3 is the complexity and speed of evolution that has become a burden on end users to keep up with and spot the new trends. As well as finding the most lucrative offerings and of course security reassurance. Ponder will work as an abstraction layer with extensibility and scalability in mind considering the speed of development and progress in this space.

Ponder will aim to provide an abstract with minimal complexity for end users to;

- Find and enter staking options such ash PoS on Ethereum
- Find and enter options to restake into EigenLayer AVS’
- Find and enter RWA markets to lend their funds to real world businesses and more
- Find and enter most lucrative DeFi Money Markets

Ponder will hide all complexities behind these offerings, simplifying the flow for the end user and allowing everyone regardless of their experience to be able to

generate yield in various forms. Some obvious complexities Ponder will mask are:

- Deposit Collateral
- Withdraw Collateral
- Loans
  - Create/Issue Loan
  - Payback Loans
  - Liquidate Loans
  - Enter or Exit Lending Pools
  - Liquidation Data
- Query credit limit or “line of credit” for a given wallet
- Health Factor of a Given Wallet (Credit Score)

The end goal for phase three will be to bring all (complex and non-complex) data available on-chain together and present it as bitesize abstract views for individuals and institutions to analyse and execute trades without ever having to “shop around” on multiple platforms.

Phase 4 - NFT Marketplace Aggregator, Ordinals and BRC20s

Phase 4 of Ponder introduces a groundbreaking approach to navigating the complex world of NFTs, including the innovative additions of Ordinals and BRC20s on the Bitcoin network. This phase marks a significant leap beyond traditional crypto assets, as Ponder integrates with NFT marketplace APIs and smart contracts to offer comprehensive quotes for both collections and individual NFTs. The platform's capability extends to executing monetary transactions, providing users with a seamless and efficient trading experience.

Expanding its utility, Ponder will incorporate data from analytics platforms like CryptoSlam, DeFiLlama, Dune, NFTBank.ai, hiro.so (Ordinals) and more. This integration aims to deliver detailed insights on volume, social presence, and a broad array of metrics, enabling users to make well-informed decisions. The inclusion of Ordinals and BRC20 inscriptions brings a novel dimension to Ponder's service offering, allowing users to explore and transact with unique digital artefacts and tokenized assets directly on the Bitcoin blockchain.

The ultimate goal for Phase 4 is to facilitate a sophisticated comparison and analytics framework for exotic assets, enabling users to find the best rates across different markets for buying or selling. This integration sets the foundation for cross-chain movement of NFTs and establishes a vital link to Phase 3's DeFi integration. With platforms like Paribus considering NFTs as collateral, Ponder aims to bridge the gap between DeFi and NFTs, providing a comprehensive experience that encompasses the full spectrum of digital asset interaction and management.

Phase 5 - DeFi Insurance, DePIN, Ramps and Wallets

Phase 5 of Ponder represents a significant leap towards a holistic digital finance ecosystem, offering nuanced comparison tools for fiat ramps, wallets, DeFi insurance, and notably, Decentralised Physical Infrastructure Networks (DePIN). This stage is meticulously crafted to cater to the diverse needs of users in the rapidly evolving DeFi and Web3 spaces.

In the realm of fiat ramps, Ponder meticulously evaluates crucial aspects like transaction speeds, costs, and regulatory requirements, presenting users with a clear, concise comparison. This enables a seamless transition between fiat and digital currencies, optimising for efficiency and compliance.

For wallet services, the platform delves deep into analysing various features such as transaction fees, security measures between custodial and non-custodial options, and the innovative concept of account abstraction. This comparison empowers users to choose wallets that align with their security preferences, usability expectations, and financial objectives.

Addressing the vital need for security in DeFi investments, Ponder integrates with a range of insurance providers. It offers personalised quotes, thus fortifying users' investments against potential vulnerabilities in the DeFi sector. This approach mirrors traditional insurance models, adapting them to the unique risks and opportunities of digital finance.

DePIN, as a cornerstone of Phase 5, receives a dedicated focus. Ponder navigates through the complex landscape of decentralised cloud services, edge computing, and blockchain-based storage solutions. By comparing various DePIN providers, Ponder illuminates key considerations such as operational costs, scalability options, and the technical robustness required for running sophisticated applications, from decentralised web hosting to AI-driven analytics. This enables developers and businesses to make informed decisions, choosing infrastructure solutions that not only reduce costs but also enhance performance and reliability in a decentralised manner.

Through Phase 5, Ponder aims to streamline the complex decision-making processes inherent to engaging with DeFi and Web3, ensuring that users are equipped with comprehensive, easy-to-understand comparisons. This initiative underscores Ponder's commitment to elevating user experience, offering clarity and confidence as users navigate the multifaceted digital finance landscape.

Phase 6 - Investment DAOs

The rise of decentralisation has given the scope and ability to build the foundation block of DeFi a new paradigm of interacting with money and utilising it to invest and yield without the bureaucracies and the obstacles

present in TradFi. With such a shift innovation quickly followed and new forms of funds and groups came together to propose the idea of “Investment DAOs”.

A DAO, or Decentralised Autonomous Organization, is a type of organisation that is run using blockchain technology. A DAO operates without a traditional hierarchical structure or central leadership and instead relies on a network of users who interact with each other and with the DAO using a set of rules and protocols that are encoded on the blockchain.

An investment DAO is a specific type of DAO that is focused on investing. This could involve investing in traditional assets such as stocks, bonds, and real estate, or more novel assets such as cryptocurrency or other blockchain-based assets. Investment DAOs are typically run by a group of users who collaborate to make investment decisions and manage the assets of the DAO. These users may be rewarded for their contributions to the DAO, typically in the form of a share of the profits generated by the DAO's investments.

Today there are 100s of DAOs in web3, some with a minimal entry ticket size of $100k in native assets while others go as low as $1000. While some have fees and annual renewals others are “free” once you enter as a membership. Of course, each investment DAO specialises in assets, some may focus heavily on NFT collections while others in real-world assets. Given such a wide range of DAOs and their novelty, it is a hard space to navigate and find relevant DAOs. As such Ponder will aim to simplify the research, comparison and entry to these DAOs with phase six. Ponder will integrate directly into these DAOs at the SmartContract level to allow for easy investing and tracking of funds while minimising all friction.

Governance

Decision-making and governance have become key in Web3 projects and the road to decentralisation. It can be both a blessing and a burden on a project depending on the design structure and incentivisation programme attached to governance to increase participation at large. Given the lessons learnt throughout time and through other protocols governance models, Ponder aims to leverage some of these lessons to raise average engagement time within its community and to keep the level of returns in line with the level of engagement with the protocol itself. Ponder will aim to go beyond simple governance to achieve such results. Before diving into the implementation of governance for Ponder, it is crucial to understand some key concepts the governance module of Ponder implements.

VoteEscrow Model

Curve Finance has introduced a governance model in which token holders can lock up their governance tokens (e.g. CRV) for a predetermined time in exchange for vote escrowed tokens (e.g. veCRV). The length of the lock period can range from one week to four years, and the longer the tokens are locked, the more voting power is issued to the holder as a reward for their loyalty. During the lock period, the locked tokens are not able to be sold or unstaked. However, the locked tokens do decay linearly throughout the lock period, and holders can periodically relock the decayed tokens to extend their lock period and earn the maximum rewards and governance rights.

In addition to receiving voting power, holders of veCRV tokens also receive other perks, such as the ability to select a pool to receive boosted CRV emissions and a share of protocol fees paid in CRV. They also can vote weekly on the allocation of CRV emissions and governance proposals.

Overall, this governance model is designed to encourage long-term commitment from token holders by rewarding them with voting power and other perks based on the length of time they lock their tokens. It also provides some flexibility for token holders, as they can periodically relock their tokens to extend their lock period and earn the maximum rewards.

Quadratic Voting

A voting system designed to allow voters to express their preferences more accurately and to align the outcomes of voting more closely with the preferences of the voters. It is based on the idea that voters should be able to express their preferences more strongly for issues that are more important to them.

In a quadratic voting system, each voter is given a certain number of votes that they can use to express their preferences. These votes can be used in any combination, but the cost of using each vote increases quadratically. For example, if a voter has 10 votes and wants to express a strong preference for an issue, they could use 4 votes for that issue, which would cost them 4 * 4 = 16 votes in total. If they wanted to express an even stronger preference, they could use 8 votes for the issue, which would cost them 8 * 8 = 64 votes in total.

The quadratic voting system is intended to encourage voters to be more strategic in how they use their votes and to better reflect the intensity of their preferences. It has been suggested as a possible alternative to traditional voting systems, such as first-past-the-post or ranked-choice voting, to better align the outcomes of elections with the preferences of voters.

VE(3,3)

The VE(3,3) model is a governance model for decentralised autonomous organisations (DAOs) that use tokens to represent ownership and voting power. It is a variant of the more general VE(n,m) model, which is a framework for designing governance systems in which **n** tokens are required to propose a change to the system and **m** tokens are required to vote on it.

In the VE(3,3) model, a proposal to change the governance of a DAO requires the support of at least 3 tokens to be put to a vote. Once a proposal has been put to a vote, it requires the support of at least 3 tokens to be passed. This means that the VE(3,3) model requires a relatively high level of support from token holders to make changes to the governance of the DAO.

One of the advantages of the VE(3,3) model is that it allows for a relatively high degree of decentralisation, as it requires a significant level of support from token holders to make changes to the governance of the DAO. However, it may also make it more difficult for the DAO to quickly respond to changing circumstances or to make necessary changes to its governance.

Governance on Ponder

The team while designing the governance model looked into various existing governance mechanisms in existence today and attempted to gauge their overall success, failures, shortfalls and advantages.

To push for engagement Ponder will introduce a VE model where it will be compulsory for stakers to vote at least once a month on a proposal of their liking to “claim” their rewards for participating in governance, any member who does not fulfil this obligation will forfeit their rewards for that particular month and the rewards that were forfeited will be put back into the Treasury to be distributed amongst all other stakers who have fulfilled their requirements of voting on proposals actively.

Ponder does not believe in delegation as each individual who is a token holder should be upheld with the responsibility to engage with the platform and governance to push the platform in a direction that benefits everyone. Given delegation entices the model of “stake and forget”, the Ponder team has chosen not to allow for delegation within its governance module.

Token Utilities

✅ **Stake PNDR to run decentralised API node (Roadmap Item)**

✅ **vePNDR Staking - Earn against vePNDR Balance**

Governance
Voting on bridges to integrate
Voting on chains to integrate
Voting on tokens/coins to support
Voting on marketing campaigns
Voting on development and hackathon participation

✅ **Base TX Fee: 0.05% - All TXs; Bridge, Swap, DeFi Position, NFT Buys/Sell/Swaps, Insurance, Investment DAOs**

Ponder Plus:
Min lock amount 40k PNDR for 12 months
0% Fees for the duration of the stake
GAS refunds in PNDR
Early access to beta features
MEV Protection
Personalised Dashboard
Analytics across space on TVLs, Bridges, News, Blogs, Educational pieces, offers from partners

✅ **Usage rewarding**
Generate a volume of $100k+ over x periods to claim an NFT
That has y number of PNDR tokens that can only be withdrawn and staked in governance for a minimum of 12 months thus Ponder Plus

✅ **Earn PNDR**
Report hacks on bridges and DeFi and once confirmed earn a fee for stopping more trade going through a certain provider
Report bad data

✅ **API Subscriptions (B2B)**
Discounts are available when paid in PNDR

✅ **Advertising and Promotion (B2B)**
Monthly payments in PNDR