DODOchain:
The Omni-Trading Layer3

Jan 2024

Abstract

Amidst the rapid growth of the cryptocurrency market, the decentralization of liquidity and its associated challenges are becoming increasingly central in blockchain and cryptocurrency research and application. The rise of various blockchain ecosystems, particularly those compatible with EVM and non-EVM chains, is highlighting the problems of liquidity segmentation and fragmentation. Such issues substantially hinder improvements in cross-chain asset interoperability and trading efficiency. Although current cross-chain solutions like centralized exchanges, interoperability frameworks (like Cosmos, Polkadot), and asset/token bridges have partially addressed these concerns, they continue to grapple with critical challenges related to further dispersion of liquidity, security flaws, and subpar user experiences.

This paper analyzes the current market dynamics, explores the fundamental causes of liquidity fragmentation and its market impact, and assesses the limitations of existing cross-chain technologies and solutions. Building on this, the paper introduces DODOchain, a Layer 3 solution focused on omni-chain trading. DODOchain integrates advanced cross-chain technology, efficient market-making algorithms, and a flexible Layer 3 architecture to create a platform that bridges EVM and non-EVM ecosystems. This platform is designed to deliver a one-stop, seamless, efficient, and secure trading experience for users. Core to its trading hub, DODOchain employs PMM market-making and efficient routing algorithms, leverages AltLayer to access Arbitrum Orbit for effective trade execution, and ensures the security of omni-chain trading with EigenLayer as a data availability and decentralized verification network. Furthermore, DODOchain introduces innovative incentive mechanisms and a participatory governance model, encouraging extensive community participation to drive the ecosystem's continuous growth and prosperity.

The study offers a fresh perspective on the application of blockchain technology to solve liquidity fragmentation and presents a new framework and path of practice for the cryptocurrency market. The launch of DODOchain signals a step towards a more efficient, open, and decentralized cryptocurrency market, significantly contributing to the integration and interconnectivity of diverse blockchain ecosystems, thus enhancing overall market liquidity and asset utilization.

Introduction

In the current blockchain ecosystem, fragmented liquidity and high cross-chain costs represent two prominent challenges. The decentralization within the EVM ecosystem has led to the dispersal of funds and resources across different chains, resulting in liquidity segmentation. Meanwhile, non-EVM chains such as Bitcoin and Solana are rapidly evolving, establishing unique ecosystems but often lack technical compatibility with EVM, further exacerbating liquidity fragmentation. Cross-chain technologies, though attempting to share liquidity through tokenization of assets or direct inter-chain communication, face multiple challenges, including liquidity dispersion and security vulnerabilities in cross-chain bridges. DODOchain, as a novel Layer 3 solution, is committed to integrating liquidity across all chains through its core trading components, offering a comprehensive omni-chain trading experience.

DODOchain has realized a Layer 3 architecture through Arbitrum Orbit, aimed at enhancing cross-chain functionality and user experience. By integrating the technologies of AltLayer and EigenLayer, DODOchain has created a seamless, efficient, and secure environment for omni-chain trading and liquidity sharing. AltLayer's Rollup-as-a-Service, enhanced by the restaked rollup mechanism, fortifies network security and decentralization while promoting cross-chain interoperability. EigenLayer's core submodule, EigenDA, brings efficient data processing capabilities and security reliant on Ethereum. With Arbitrum Orbit as its foundation, it allows for customized Layer 3 solutions that support high transaction throughput and low network fees, thereby improving transaction efficiency and user experience. DODOchain's goal is to establish a permissionless omni-chain trading platform that enables users to freely issue, trade, and manage assets across various blockchain ecosystems.

Background

Current Market State

The dispersion of market liquidity is a significant issue facing the cryptocurrency sector, with ongoing innovation in blockchain technology introducing new chains and ecosystems that bring both opportunities and unprecedented challenges. In this multifaceted environment, the decentralization of the Ethereum (EVM) ecosystem and the emergence of non-EVM chains inherently lead to the segmentation and complexity of market liquidity.

Impact of EVM Ecosystem Decentralization on the Market

The decentralization of the EVM ecosystem is characterized by an increasing number of blockchains adopting Ethereum-compatible virtual machines, allowing developers to use the same smart contracts and tools to build applications across different chains. While this compatibility has spurred innovation, it has also resulted in liquidity dispersion. As more chains join the EVM ecosystem, resources initially concentrated on Ethereum begin to spread to other chains, including a growing number of Layer 2 rollups. Each chain develops its own ecosystem with unique user groups and assets, which tend to keep assets within the ecosystem, causing liquidity fragmentation. Despite their technical and performance differences, these chains face a common issue: how to effectively manage and utilize dispersed liquidity while maintaining ecosystem diversity.

Challenges and Rise of Non-EVM Chains

Simultaneously, non-EVM chains like Bitcoin, Solana, and Near are rapidly growing, building distinctive ecosystems and technical architectures. These chains are often not compatible with EVM, meaning their assets and services are technically challenging to interoperate with Ethereum and its derivatives. This further intensifies liquidity fragmentation as asset transfers and exchanges across different chains become more complex and costly. Particularly, established cryptocurrency ecosystems like Bitcoin, despite their substantial market value and user base, still face significant interoperability challenges with the EVM DeFi ecosystem.

Cross-chain technologies aim to solve interoperability issues between chains, allowing assets and data to be transferred and exchanged securely and efficiently across different chains. The market currently features a variety of cross-chain solutions, such as bridges, side chains, and locking mechanisms, attempting to share liquidity between chains through tokenization of assets or direct inter-chain communication.

These solutions face several key issues:

1. **Liquidity Dispersion:** Although cross-chain technology enables asset transfer between different chains, it does not fundamentally resolve the issue of liquidity dispersion. The liquidity of the original chain is still impacted when assets are transferred to a new chain, and the problem of liquidity fragmentation persists, constrained by interoperability.

2. **Bridge Security Issues:** Cross-chain bridges are repeatedly exploited by hackers, resulting in the loss of millions in assets. These security breaches not only undermine user confidence but also reveal the limitations of cross-chain technology in protecting asset safety.

3. **Poor Cross-chain Transaction Experience:** Due to dispersed liquidity, lack of interoperability, and the variety of existing cross-chain standards, users face extremely complex choices for on-chain transactions, resulting in a degraded experience. Users need to employ multiple cross-chain bridges and protocols to manage and trade multi-chain assets.

4. **Asset Explosion and Ecosystem Diversification:** The ongoing expansion and diversification of the cryptocurrency market lead to an influx of new assets and tokens, complicating liquidity management. Each ecosystem has a wide range of assets internally, while asset flow between ecosystems is limited by the development and adoption of cross-chain technology, causing overall market liquidity to become increasingly segmented.

5. **Value Capture by the Chain Layer:** Current blockchain architectures often result in the value generated by DApps (decentralized applications) being captured by the underlying chain, not the DApps themselves. This phenomenon limits the potential for DApp development and innovation. With the exploration of Layer 3 (L3) technology, which builds an application layer on existing chains, there is hope to offer DApps more value capture mechanisms and greater flexibility, but this also increases the complexity and challenges of liquidity.

Seeking New Solutions

We believe that with the development of modular blockchains and restaking infrastructures, adopting new solutions to realize Omni-Trading is urgent. The development of modular blockchains and restaking infrastructures provides new possibilities for the realization of Omni-Trading. As a Layer 3 focused on Omni-Trading, DODOchain is at the forefront of this innovative wave. Utilizing its core trading components, DODOchain aims to unlock an unprecedented omni-chain trading experience, achieving seamless on-chain asset and information flow.

DODOchain's key innovation lies in integrating advanced technologies such as Arbitrum Orbit, AltLayer, and EigenDA, spanning all chains, including EVM and non-EVM. This not only improves transaction efficiency but also significantly expands trading possibilities, allowing users to freely move assets between different blockchains, whether based on Bitcoin, Ethereum, or Solana ecosystems.

As a pioneering Layer 3 solution, DODOchain's vision is to converge the liquidity of various blockchain ecosystems into a unified platform. This means that no matter which blockchain users' assets are on, they can easily engage in transactions within any chain's range without being hindered by existing technological barriers. In this way, DODOchain not only breaks the current status of liquidity fragmentation but also provides users with a more efficient and convenient trading experience.

Furthermore, the structural design of DODOchain enables it to quickly adapt to changes in new blockchain technologies and ecosystems. As new blockchain platforms and protocols emerge, DODOchain can easily integrate new functionalities and support new chains, ensuring that it remains at the forefront of omni-chain trading technology. This flexibility and scalability ensure that DODOchain can evolve with the development of the blockchain ecosystem, providing users with the most advanced trading tools and services.

Cross-chain Related Work

Cross-chain Infrastructure

Centralized Exchanges: Currently, centralized exchanges play a crucial role in cross-chain interoperability by connecting different blockchains in a centralized manner, offering platforms for asset exchange and information flow. Their main advantage lies in their ability to quickly respond to market demands and flexibly list new assets. Due to their centralized management, they offer an efficient trading experience. However, this centralized nature also means that users must trust the operators of these exchanges, somewhat contradicting the decentralized principle of blockchain. Additionally, centralized exchanges face security risks, including hacks and internal fraud, potentially leading to loss of user assets. Despite their convenience for cross-chain interoperability, the limitations and risks of centralized exchanges prompt the exploration of more secure and transparent solutions.

Interoperability Ecosystems: Projects like Cosmos and Polkadot attempt to address inter-blockchain communication by creating interoperability hubs. These projects enable asset and information flow between sidechains or parachains built on their platforms. For instance, Cosmos implements inter-blockchain communication through the IBC protocol. Polkadot, through its unique relay chain and parachain structure, allows different blockchains to securely share information within a unified network. This method provides a relatively decentralized

approach to cross-chain communication, emphasizing interoperability within the ecosystem. However, its limitation is mainly applicable to interoperability within the ecosystem, and interoperability outside the ecosystem still relies on other technological means.

Wrapped Assets and Token Bridges: In cross-chain technology, token bridges and wrapped assets are crucial for connecting different blockchains and facilitating asset transfers. By creating wrapped assets, which are tokens issued on a target chain representing assets from an original chain, asset transfers between blockchains are enabled. This process often involves complex smart contracts to ensure the security and accuracy of transactions. However, each cross-chain asset transfer requires establishing new smart contracts, and as blockchain technology evolves, these contracts may need adjustments, increasing maintenance costs and complexity. Moreover, building and maintaining token bridges requires significant technical resources and expertise, with each new bridge posing a unique engineering challenge. Changes in underlying blockchain protocols necessitate updates to all related bridges to ensure the accuracy and security of cross-chain transactions. This not only increases operational complexity but also limits the scalability and economic efficiency of cross-chain interoperability solutions. Despite the potential offered by token bridges and wrapped assets for cross-chain asset transfers, the technical and operational challenges they face are evident.

Cross-chain Communication Initiatives: Several infrastructure efforts build on previous explorations, such as Layer0, Wormhole, and Axelar, focusing on cross-chain messaging services and connecting multiple ecosystems. However, they often rely on the honesty of specific validating nodes or require the underlying blockchains to adopt specific protocols, limiting their widespread application.

Layer0: LayerZero is an open-source, immutable messaging protocol for creating Omnichain applications that interact across blockchains. It achieves seamless blockchain interactions by deploying smart contracts on each chain, combined with decentralized verification networks (DVNs) and executors. LayerZero offers a method that separates message verification from execution, allowing developers more flexibility in controlling their applications' security settings and independent operation. Moreover, it supports the transmission of arbitrary data, external function calls, and tokens while maintaining full autonomy and control of the application, not limited to asset exchanges. LayerZero aims to provide a universal, third-party-independent security framework, enabling the construction of various types of cross-chain applications, not just asset exchanges. However, the decentralized level of LayerZero is not high, as DVNs are not entirely permissionless and still require trust in some entities.

Wormhole: Wormhole enhances the security and reliability of cross-chain transactions through a network of guardian nodes composed of top global verification companies. These guardian nodes run full nodes, not light nodes, of each participating chain, providing comprehensive validation of each transaction and strengthening resistance to consensus attacks or hard forks.

Besides supporting cross-chain asset transfers, Wormhole also handles cross-chain calls for arbitrary messages, supporting a wider range of applications. The project's governance and monitoring mechanisms, along with its comprehensive open-source and auditing history, further highlight its focus on security. However, Wormhole's performance and stability heavily depend on the operation of its guardian node network, and network failures or attacks may affect its overall functionality. Additionally, while on-chain governance enhances transparency, it also introduces governance risks, particularly in scenarios of low participation or tendencies towards centralization, potentially impacting the system's fairness and security.

Zetachain: Zetachain is a novel cross-chain product designed to connect smart contract blockchains (such as Ethereum and Solana) with non-smart contract blockchains (such as Bitcoin and Dogecoin), facilitating seamless asset and information interoperability. Zetachain utilizes multi-party signatures (TSS) and cross-chain smart contracts to manage and update the states of external chains in a relatively decentralized manner without relying on centralized third parties. However, Zetachain also relies on trust in the signatories.

Axelar Network: Axelar is based on a proof-of-stake (PoS) consensus mechanism, processed by a decentralized network of validators handling cross-chain messages. Axelar supports a wider range of applications through its own blockchain and a series of APIs, not limited to asset exchanges. It is built using the Cosmos SDK, allowing developers to build cross-chain dApps on any blockchain. Additionally, Axelar introduces quadratic voting mechanisms to prevent the concentration of power, while enhancing network security through measures such as key rotation and code audits. Its validator network is public, and the larger the collective, the stronger the security. Axelar aims to provide a universal platform supporting cross-chain asset transfers, smart contract calls, and other functions, but this also brings complexity and high performance demands on participating nodes.

Cross-Chain DEX

Cross-chain transactions are revolutionizing how users understand and engage with digital asset trading. This process involves asset transfer between different blockchain networks, enabling users to seamlessly exchange assets across independent chains. With the rapid evolution of blockchain technology, an increasing number of exchanges are beginning to support cross-chain transactions, resolving the issue of fragmented and disjointed asset liquidity across chains through infrastructures such as cross-chain bridges and aggregators. Nevertheless, considerable challenges remain: most cross-chain trading projects operate within their ecosystems, like EVM and Cosmos ecosystems, and some achieve inter-operability through aggregating cross-chain bridges and liquidity but do not facilitate omni-chain transactions. As a result, liquidity remains scattered, and the security of cross-chain transactions is still not guaranteed. Some cross-chain transaction products attempt to build their own network of validators, but the decentralization

and dispersion of these networks are limited, and their security may even be lower than that of the cross-chain protocols themselves.

Cross-chain swap by building a small decentralized protocol: Managing cross-chain assets through self-built networks of validators is one way to facilitate cross-chain transactions, as seen with ChainFlip and Symbiosis. ChainFlip is a decentralized cross-chain trading protocol that allows users to exchange assets across chains directly from personal wallets without relying on wrapped tokens, centralized exchanges, or synthetic assets. The protocol is supported by a network of validators, employing Multi-Party Computation (MPC) and Threshold Signature Scheme (TSS) to ensure fund safety and facilitate trustless transactions. ChainFlip's architecture comprises a settlement layer and an accounting layer, with the core being its state chain and Just-In-Time Automated Market Maker (JIT AMM) functionality, providing an efficient and secure cross-chain exchange solution. However, reliance on a validator network could pose security issues, and the JIT AMM essentially settles market maker orders and does not effectively access omni-chain liquidity sources.

Symbiosis, as a decentralized exchange aggregator, supports EVM and non-EVM technologies and provides boundless liquidity across different blockchains through fully decentralized, interoperable, and non-custodial practices. It facilitates cross-chain exchanges through smart contracts and an off-chain relay network, utilizing stablecoins and WETH as intermediary tokens to find optimal exchange paths, managing liquidity pools through AMM to ensure efficient exchanges. Although Symbiosis introduces a liquidity provider incentive mechanism to maintain high liquidity, its reliance on a relay network design also brings added complexity and potential security challenges.

Cross-chain swap by aggregating different bridges and liquidity sources: Aggregating cross-chain bridges or different DEX liquidity to enable cross-chain transactions is a common method, exemplified by Jumper and XY Finance. Jumper, the frontend UI for LIFI technology, itself a bridge and Decentralized Exchange (DEX) aggregator, provides a one-stop solution for cross-chain asset transfer. LIFI's core advantage lies in its adaptability to a multi-chain future, solving the challenges faced by DeFi applications, wallets, and other protocols during asset transfers. In addition, LIFI significantly reduces the complexity for other developers integrating cross-chain functionality through its APIs and SDKs, optimizing the user experience for cross-chain transactions. While its smart contracts are open-source, LIFI chooses to keep parts of its API private to maintain a competitive edge, and its backend must remain centralized due to data processing needs, posing a challenge to the decentralization ethos.

XY Finance, through its X-Swap and yBridge platforms, offers a cross-chain trading and liquidity pool protocol that supports seamless token exchanges across different blockchains and yields for users providing liquidity. Its underlying technological infrastructure includes

developer-friendly APIs and a user interface that simplifies cross-chain transactions. Furthermore, XY Finance uses its consensus mechanism and settlement chain; although the network currently operates centrally, there are plans to introduce external nodes to enhance system security. XY Finance's API functions as a multi-bridge aggregator, supporting multiple decentralized exchanges and bridging protocols, optimizing the management of cross-chain liquidity. Despite its unique "rebalancing mechanism" and "reward system" designed to address liquidity shortages, the network's partially centralized operations may spark discussions on security and the principles of decentralization.

Cross-chain transaction products designed through aggregation methods are limited by the aggregation mechanism itself, which cannot offer customized services or integrate liquidity sources at the base layer, and the security of aggregated cross-chain bridge sources cannot be guaranteed.

Reliance on a Specific Cross-Chain Protocol: Relying on a specific cross-chain protocol, then building liquidity pools or aggregating liquidity, is another way to achieve cross-chain transactions. For instance, Xswap leverages Chainlink's CCIP protocol, while Interswap relies on the Axelar Network. XSwap is a cross-chain DEX implemented using Chainlink's Cross-Chain Interoperability Protocol (CCIP), providing a streamlined cross-chain exchange experience through aggregated liquidity. XSwap's user interface is designed for simplicity, aiming to reduce the complexity of cross-chain transactions while offering tools for third-party projects to integrate cross-chain liquidity transfers, further enhancing the ability of single-chain applications to handle cross-chain messages. Although XSwap relies on Chainlink's secure protocol to ensure the safety of user assets during exchanges, it still faces limitations in chain transaction speed and fees, as well as the centralization risks associated with depending on a single external protocol (Chainlink CCIP).

InterSwap is a cross-chain trading and liquidity management platform that provides a one-click, seamless cross-chain exchange experience by integrating Axelar's cross-chain communication technology. Utilizing Axelar's General Message Passing (GMP) and GMP Express messaging features, InterSwap aims to become the first cross-chain liquidity layer on Axelar to achieve unified liquidity, reducing the risks associated with traditional bridging while increasing capital and user inflow. InterSwap offers a rapid (less than 20 seconds) and convenient (one-click exchange) cross-chain exchange experience, with a trustless zero-layer protocol ensuring transparent and seamless transactions. However, InterSwap's success heavily depends on the performance and security of the Axelar platform.

DODO's Trading Gene

As a decentralized trading platform driven by the Proactive Market Maker (PMM) algorithm, DODO is characterized by its highly capital-efficient liquidity pools that support single-token liquidity provision. This reduces impermanent loss and minimizes slippage during trades. The core PMM algorithm is an inventory management strategy. As the quantity of an asset decreases, the PMM algorithm automatically raises the price of that asset, anticipating buying back the missing inventory from the market. Using the Price Curve Simulator tool, we can visually comprehend how the price changes when the quantity of pool tokens varies. The sensitivity of price changes to inventory amounts is abstracted by DODO through the 'k' parameter; the larger the value, the steeper the curve, heightening the price's sensitivity to inventory levels and thus the trading slippage. Conversely, a smaller 'k' value results in a smoother curve, less price sensitivity to inventory, and reduced slippage. It's through the PMM design that we've been able to iteratively evolve DODO's versions.
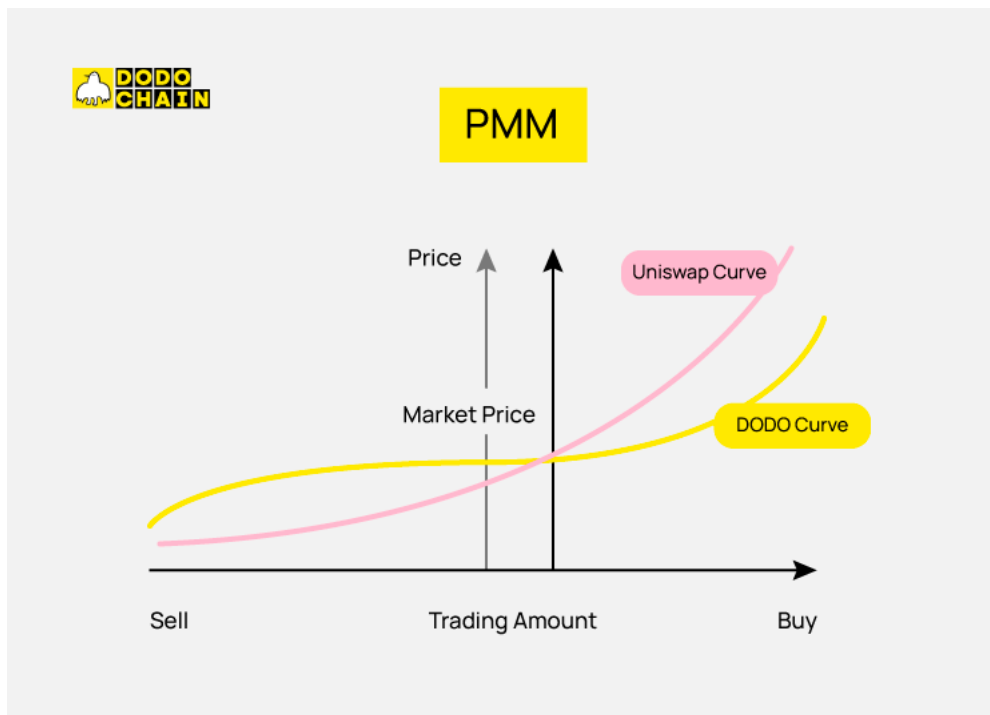
DODO V1: Launched in August 2020, the first version of DODO's product line introduced concentrated liquidity around oracle prices to enhance capital efficiency. This mechanism was intended to offset impermanent losses by collecting sufficient trading fees. Additionally, it segregated buy and sell liquidity, enabling LPs to deposit and withdraw a single asset rather than two. Presently, DODO V1's stablecoin trading pools remain among the most active and high-volume on the exchange. These pools have achieved notable capital efficiency and low transaction fees, continuously providing the market with stable and abundant liquidity.

DODO V2: Rolled out in February 2021, V2 introduced a completely permissionless system. This significant upgrade democratized the creation of funds and market-making strategies, allowing anyone to contribute to the ecosystem. As a complement to V1, V2 expanded DODO's functionalities and scope. It added three different types of liquidity pools to meet the diverse needs of various tokens:

- DODO Vending Machine (DVM): Customized liquidity pools suitable for assets that are not widely traded but still require market liquidity.

- DODO Private Pool (DPP): Catering to mainstream tokens, DPP provides a more personalized liquidity environment, allowing more control over trading strategies and parameters.

- DODO Stable Pool (DSP): Specially designed for stablecoins, DSP ensures efficient and stable liquidity management, meeting the unique requirements of stablecoin trading pairs.

DODO V3: Launched in 2023, V3 is designed for professionals, maintained by LPs (Liquidity Providers) and SPs (Strategy Providers). LPs contribute funds to the pool, while SPs contribute strategies. Both LPs and SPs share the fee revenue. SPs must provide collateral, which will be deducted first if the strategy performs poorly. From the perspective of strategy providers, DODO V3 also serves as a leveraged market-making tool.

In addition to the multi-version pools built around the PMM, infusing DeFi with liquidity, DODO X, as a routing algorithm, offers aggregated trading functionalities to front-end traders. A distinctive feature of DODO X is its coverage of nearly all on-chain liquidity, not only from DODO pools but also from other various sources, including renowned platforms like Uniswap. Moreover, DODO X integrates quotations from third-party aggregators such as 1inch and 0xAPI and has designed a powerful proprietary routing algorithm to ensure that users receive the most competitive exchange rates on the market.
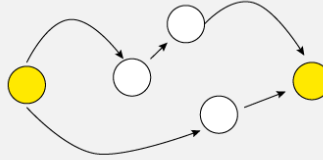
With the industry's growth, particularly around the numerous Layer2 ecosystems of Ethereum, DODO has been deployed on 15 EVM-compatible chains, leading to fragmented liquidity. Managing assets and trading steps has become cumbersome for front-end users. Against this backdrop, DODO has chosen to continue evolving towards omni-chain trading by constructing DODOChain, a Layer3 infrastructure. In conjunction with DODO's own liquidity advantages, it aims to build a liquidity aggregation hub that links numerous Layer2 and non-EVM ecosystems, offering users more convenient, cost-effective, and rapid omni-chain trading products.

Solution

## Technical Structure

DODOchain — The Omni-Trading Layer

DODOchain's technical architecture takes a unique approach to tackling the array of challenges encountered in cross-chain trading, especially concerning the issues with self-built asset cross-chain protocols. Traditional self-built cross-chain protocols often gravitate towards centralization of the validator network due to their inability to support public chain-level throughput, thus increasing operational costs and reducing both the system's decentralization and security. To overcome these barriers, DODOchain employs modern blockchain infrastructure improvements and the trend towards modularity, utilizing the EigenLayer restaking solution's validator network, also known as AVS (Arbitrary Verification System), for its validation nodes. This design not only optimizes the decentralization of the validator network but also enhances the network's security and efficiency.

Through AltLayer technology's integration with Arbitrum Orbit, DODOchain chooses to build an L3 solution on Arbitrum Orbit, achieving efficient order execution and liquidity aggregation. This layered design enables DODOchain to maintain high performance and low latency when handling trillion-level transaction volumes and mass order settlements.

Security is paramount in cross-chain transactions, and DODOchain's underlying security mechanisms are provided by the AVS restaking network. This security mechanism ensures a high degree of network safety and defense, allowing users and developers to enjoy a level of security comparable to L1. Additionally, DODOchain uses EigenDA (EigenLayer Data Availability) to guarantee data availability, ensuring all data on L1 is reliable and timely. Similar to aggregated cross-chain trading protocols, DODOchain introduces Trusted Bridges as the entry and exit points for user assets crossing chains, balancing efficiency and security. This fundamentally transforms DODOchain into an omni-trading platform capable of seamless asset and information flow between different blockchains.

The introduction of Trusted Bridges will also consolidate fragmented ecosystems, achieving seamless connectivity between EVM and non-EVM ecosystems. In terms of liquidity integration, DODOchain will incorporate DODO's own efficient trading hub, aggregate omni liquidity, and leverage efficient PMM market-making algorithms and routing networks to market and settle orders, resolving the fragmentation of liquidity between chains and between EVM and non-EVM ecosystems.

DODOchain's technical architecture not only demonstrates innovation in addressing existing cross-chain trading issues but also reflects a deep understanding of future blockchain technology trends. By implementing an L3 solution on Arbitrum Orbit, DODOchain not only enhances transaction efficiency and speed but also provides developers with a more flexible and convenient development environment, guaranteed by AltLayer. This multi-layered and multifaceted technical combination ensures DODOchain's leadership in the field of cross-chain trading, offering users a secure, efficient, and decentralized cross-chain trading platform.
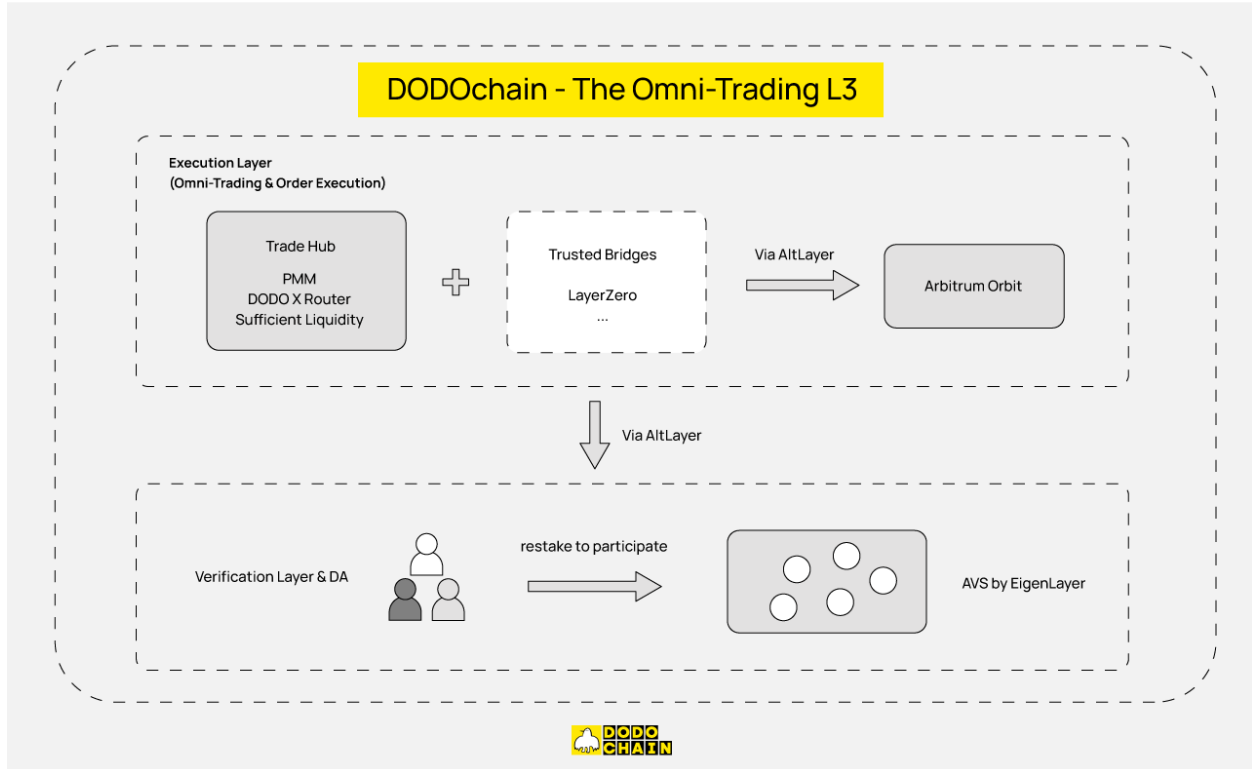
Arbitrum Orbit Empowers DODOchain as a High-Efficiency Execution Layer

Arbitrum Orbit is designed to provide developers with a permissionless route to quickly launch customized proprietary chains using Arbitrum technology. Orbit chains can act as a second layer (L2) chain executing and settling directly to Ethereum, or as a L3 chain executing and settling to any Ethereum L2 chain, such as Arbitrum One. This flexibility in settlement layers makes Arbitrum Orbit an ideal choice for efficient execution.

Arbitrum Orbit utilizes the Arbitrum Nitro technology stack, which supports interactive fraud proofs, advanced compression techniques, EVM+ compatibility through Stylus, and continuous technological improvements. This ensures that Arbitrum Orbit not only has advantages in execution efficiency and speed but also supports flexibility and convenience in the development environment.

Arbitrum Orbit allows developers to configure multiple components of a chain, including throughput, privacy protection, Gas tokens, governance, pre-compiled contracts, data availability layers, etc., offering limitless possibilities. Developers have ownership of their own Orbit chain and can decentralize its ownership, validation, and other dependencies. This not only enhances the network's security and transparency but also allows for flexible adjustment and optimization of chain operations according to community needs. These features mean that developers can customize their own Orbit chain according to their needs and target markets. DODOchain uses this feature of Arbitrum Orbit to custom develop an L3 suitable for omni-trading, including improvements to Data Availability (DA), choices of Gas Token, and customization of trading-related contracts, greatly enhancing DODOchain's execution efficiency to support mass order settlement and liquidity integration.

EigenLayer as DA and Validation Layer

EigenLayer introduces a novel collective security mechanism that allows modules to secure themselves by restaking ETH rather than their own tokens, with a specific focus on Ethereum validators. These validators can set their beacon chain withdrawal credentials to the EigenLayer smart contract and opt into new modules built on EigenLayer. To participate, validators need to download and run additional node software required by these modules, which can impose extra punitive conditions on validators who opt in. This restaking mechanism rewards validators with additional income for providing security and validation services to the selected modules, thereby deeply transferring cryptoeconomic security.

For example, participants restaking through EigenLayer for a data availability layer module would be paid each time the module stores data. Re-stakers are subject to punitive conditions. Restaking thus significantly broadens the scope of blockchain applications that can pool decentralized network security, opening up more opportunities for security leasing to virtual machines, consensus protocols, and middleware.

EigenLayer offers an open market mechanism that manages how its pooled security is taken up and consumed by AVS. Validators can choose whether to join each module established on EigenLayer. Modules must provide sufficient incentives for validators to allocate their re-staked Eth to them. Validators will also help determine which modules deserve this additional pooled security considering the potential for extra punitive risks. DODOchain will operate as one such module, with AVS providing validation services and security assurance, thus securing data availability and a safe decentralized network backed by high-value staked amounts.

To understand EigenLayer's mechanism and its impact on DODOchain's security, consider an AVS protected by $8 million in re-staked ETH containing a total of $2 million in locked value. To seize that $2 million would require a minimum cost of $4 million (50% of the $8 million). This is because if an attack occurs, the attacker would see at least $4 million of their re-staked

ETH penalized and slashed. In this scenario, the cost of the attack outweighs the gain, making it uneconomical and thus secure. If the same group of stakers also re-stakes in other AVSs, it's more complex. In the simplest case, the exact same group of re-stakers participates in another 10 AVSs, each with $2 million locked. The total potential profit from attacking these re-stakers is $20 million, but the total stake value is only $8 million. Once an attack occurs, the punitive mechanism can only slash $8 million, making the application economically insecure. Therefore, the number of AVS validation sets a re-staker is involved in is crucial, and efforts will be made to ensure economic security.

DODOchain overcomes the centralization and security challenges of self-built cross-chain protocols and communication nodes by integrating EigenDA and the AVS validator network.

AltLayer as an Efficient Development Tool

AltLayer introduces the concept of Restaked rollups, simplifying the creation process of rollups by using existing rollup technology stacks (such as OP Stack, Arbitrum Orbit, ZKStack, Polygon CDK, etc.) and enhancing network security, decentralization, interoperability, and finality through EigenLayer's restaking mechanism.

Restaked rollups of AltLayer are created on demand and consist of three vertically integrated Active Validation Services (AVS) for specific rollups, compatible with any underlying rollup technology stack. These AVSs provide key services including verifying the correctness of rollup states, speeding up finality, and decentralizing order through three modular components: VITAL, MACH, and SQUAD.

AltLayer also offers a versatile, no-code Rollups-as-a-Service (RaaS) launchpad, enabling developers and non-technical users to create customized rollups with just a few clicks within minutes. The RaaS supports multi-chain and multi-VM worlds and provides for EVM and WASM, different rollup SDKs, various shared ordering services, and different DA layers, among other modular services.

The market demands a universal and neutral protocol to meet these rollups' different fundamental needs for decentralized verification, rapid finality, cross-rollup interoperability, and flexible decentralized sorting. AltLayer addresses these needs by constructing a set of AVS, also offering dApp builders flexibility in selecting AVS operators, reward rules, adherence to protocols, and corresponding punitive rules. DODOchain will utilize AltLayer's infrastructure to better customize AVS-related rules and more swiftly integrate into Arbitrum Orbit.
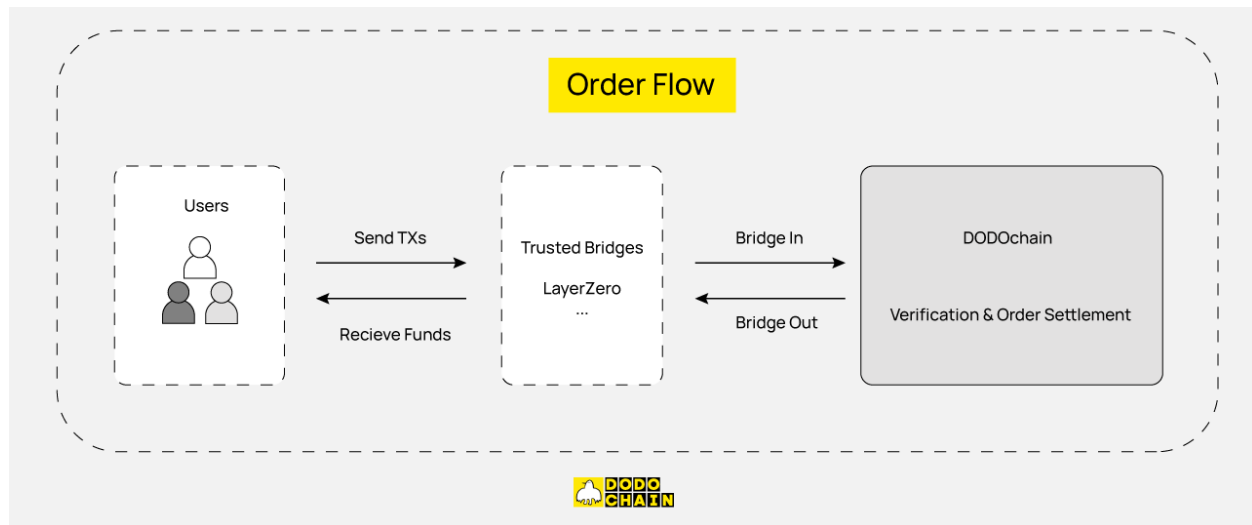
Cross-Chain Swap

Cross-chain bridges serve as critical components connecting different blockchain networks, with their core function being the secure and reliable transfer of assets and information. Typically, this involves considerations on several technical levels:

- **Cryptographic Signatures and Verifications:** To ensure the security of transactions, cross-chain bridges commonly use cryptographic technologies such as multi-signature wallets and smart contracts to verify transactions. These technologies ensure that assets can only be transferred cross-chain when specific conditions are met, adding a layer of security to transactions and preventing unauthorized access and potential double-spending issues.

- **Asset Transfer Mechanisms:** Different cross-chain bridges employ various asset transfer methods, but typically, cross-chain transactions use a lock-and-release mechanism. When assets are transferred from the source chain to the target chain, they are first locked on the source chain and then an equivalent amount of tokens is minted or released on the target chain. This process, automated by smart contracts, ensures the atomicity of transactions and prevents the loss of funds on either chain.

- **Data Availability (EigenDA) and Verification (AVS):** Cross-chain bridges rely on EigenDA and the AVS validator network for the data availability and security of asset transfers. EigenDA ensures the integrity and timeliness of cross-chain transaction data, while the AVS validator network provides additional security for cross-chain bridge operations through the restaking mechanism of EigenLayer.

- **Inter-Blockchain Communication Protocols:** Effective inter-blockchain communication protocols are necessary for transferring information and assets between different blockchains. These protocols are designed to consider compatibility with various blockchains, including EVM and non-EVM chains.

The core technologies that DODOchain employs to execute cross-chain transactions include multiple key components and processes. First, it ensures the security of transactions through cryptographic signatures and verifications, such as multi-signature wallets and smart contracts, which permit asset transfers across chains only under specific conditions, thereby enhancing transaction security and preventing unauthorized access and double-spending. Next, it uses a lock-and-release mechanism where assets locked on the source chain are correspondingly minted or released on the target chain, with smart contracts automating the process to ensure atomicity and prevent the loss of funds. Additionally, DODOchain relies on EigenDA and the AVS validator network to guarantee data availability and security, with the restaking mechanism of EigenLayer providing extra security for cross-chain operations. Inter-blockchain communication protocols ensure effective transfer of information and assets between different blockchains,

accommodating compatibility with EVM and non-EVM chains. Within DODOchain, the cross-chain bridge is closely integrated with components like the DODO Core Trading Hub and Layer3 architecture, calculating the optimal trade path and price, selecting the appropriate cross-chain bridge, and settling transactions quickly and efficiently on the target chain with the help of Arbitrum Orbit technology stack, achieving efficient and secure cross-chain transactions.

LayerZero

LayerZero is an open-source cross-chain messaging protocol designed to facilitate interoperability between Omnichain applications. It operates by deploying specific smart contracts on each chain and utilizing a decentralized verification network (DVNs) and executors (Executors) to enable smooth communication between chains. DVNs provide a mechanism to verify the authenticity of messages on the target chain, ensuring the security and trustworthiness of cross-chain messages. LayerZero uniquely separates the verification from execution, providing developers with greater control over the security settings and independent operation of their applications. Capable of handling arbitrary data, external function calls, and token transfers, it ensures applications maintain autonomy and control throughout their operations, not limited to asset exchanges alone. LayerZero aims to serve as a universal framework that offers a third-party-independent and secure environment, supporting the development of various cross-chain applications beyond just asset exchanges.

DODOchain will initially use LayerZero as its cross-chain bridge, utilizing its efficient, stable, and secure features to provide omni trade services, with plans to incorporate more cross-chain bridges to ensure a superior omni trade experience in the future.

The Implementation of Omni-Trading

Omni-Trading aims to provide a seamless, intuitive, and efficient cross-chain trading experience. Users can exchange assets between different blockchain platforms (whether EVM-compatible or non-EVM-compatible) with simple operations. This process is supported by three core components: the DODO Core Trading Hub, Trusted Bridges, and Layer3 architecture.

- **The DODO Core Trading Hub**, with its efficient market-making algorithms, ensures liquidity and optimal pricing for trades, regardless of the chain on which the assets reside.

- **Trusted Bridges** act as the conduit for transactions, optimizing cross-chain trade paths by selecting the safest and most efficient cross-chain bridges, reducing the complexity and cost for users.

- **Layer3**, with the help of Arbitrum Orbit, realizes efficient order execution and liquidity integration, ensuring speed and efficiency in transactions. The introduction of EigenLayer also enhances the security of cross-chain trading.

DODOChain will also implement DODOV3, maintained by Liquidity Providers (LPs) and Strategy Providers (SPs). LPs contribute funds to the pool, while SPs provide strategies. This version's technical enhancements based on the PMM algorithm include:

- **Decoupling sell curves from buy curves.** When liquidity on one side is depleted, the other side's curve does not automatically shift to replenish it. Each side independently follows the PMM algorithm.
- **Price truncation.** SPs can set truncation prices, allowing the curve to move within a certain price range to better concentrate liquidity.
- **Hybrid coin pools:** By using Virtual USD (VUSD) as an intermediary and building sell and buy curves with actual tokens, any two types of tokens can be exchanged, allowing a single pool to accommodate many different tokens, helping market makers save on capital.

Ultimately, DODO V3 utilizes two types of funds pools: a Vault for providing liquidity and a Pool for strategy operation. LPs can deposit assets into the Vault for stable returns, while SPs can devise strategies to call funds from the Pool for above-average returns, achieving an integrated design.
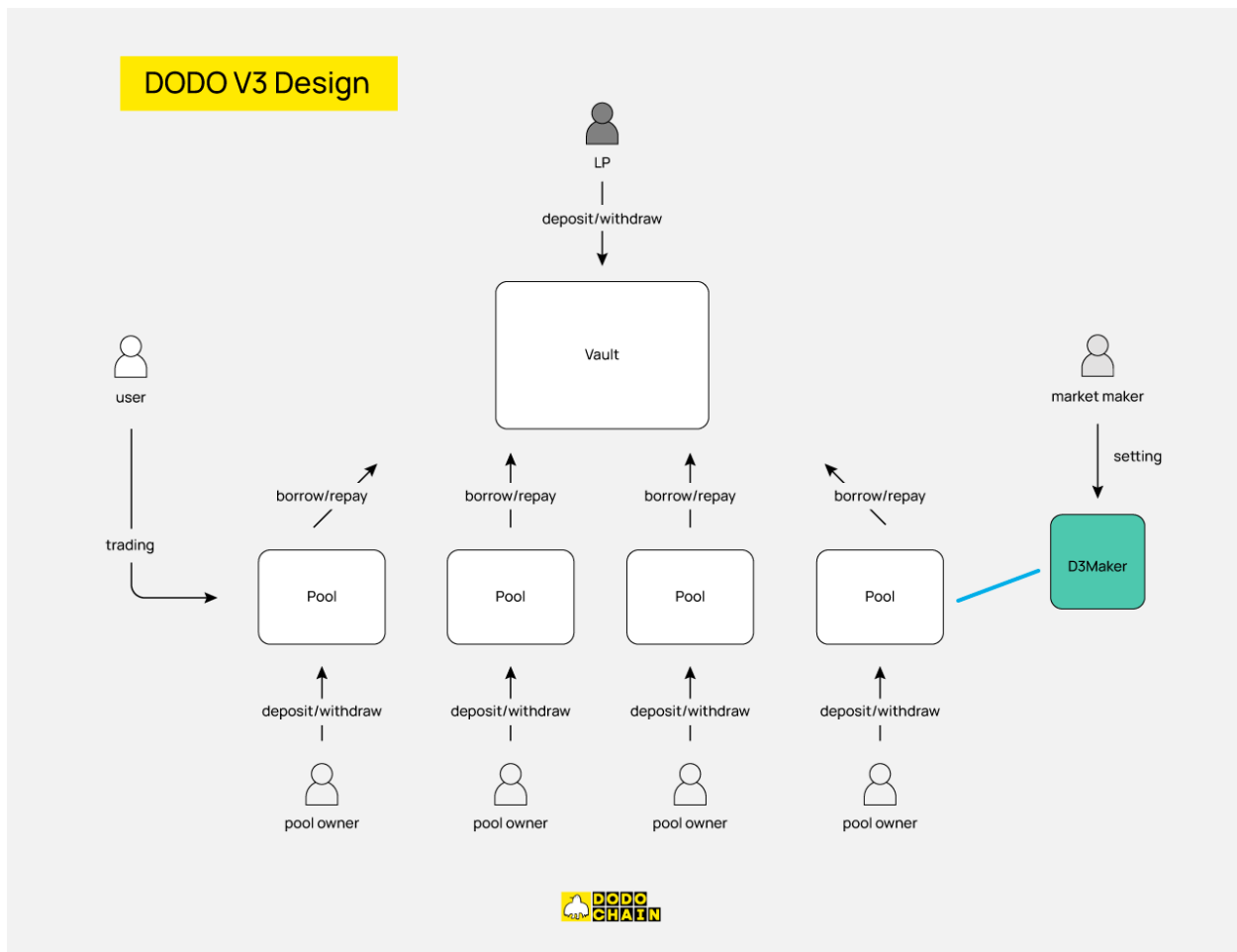
Thus, the deployment of DODO V3 greatly enhances the DODO Core Trading Hub, providing DODOChain with superior and more efficient liquidity. Coupled with the open market-making algorithm, it effectively serves as a liquidity hub.

The trading process begins with the user initiating a transaction. Once the user selects the asset and amount to be exchanged, the DODO Core Trading Hub immediately calculates the optimal trade path and price. Next, the Bridge Aggregator intervenes, selecting the most suitable cross-chain bridge for the transaction based on the bridge's security, efficiency, and current network conditions.

Once a cross-chain bridge is selected, the transaction is packaged and sent to the corresponding bridge. The security of the bridge's operations is thanks to DODOchain's technical architecture, particularly the data availability and security ensured by EigenDA and the AVS validator network. This means that users' assets are fully protected even during the cross-chain process.

After the assets cross the chain, the Layer3 architecture ensures that the transaction is quickly and efficiently settled on the target chain. Arbitrum Orbit, serving as an efficient execution layer

with its flexible configuration and optimized technology stack, provides support to DODOchain, enabling it to handle high-frequency and large-scale cross-chain transactions. Ultimately, once the transaction is successfully settled on the target chain, users can freely withdraw or further operate their assets.

DODOchain Roadmap

Q2 2024

- **Core Infrastructure Development**
    - Complete the launch of the DODOchain mainnet.
    - Confirm auxiliary chain information, advance business development, and build a documentation center to support community and developer access.
- **New Website and Staking Features Launch**
    - Launch a new DODOchain website to enhance the communication of the brand story and vision.
    - Introduce staking features (supporting Arbitrum, BTC Layer2s).

Q3 2024

- **Cross-Chain Trading and DODO v2 Support**
    - Integrate the DODO core trading hub to enable omni trade functionalities.
    - Develop and implement cross-chain bridge solutions to support secure and efficient asset flow on DODOChain.
- **Expanded Support for Arbitrum and BTC Layer2s**
    - Strengthen support for Arbitrum and BTC Layer2s, enhancing DODOchain's interoperability and ecosystem liquidity.

Q4 2024

- **Solana Support**
    - Expand support to non-EVM chain Solana, increasing DODOchain's cross-chain coverage.
- **Enhanced Features and Ecosystem Growth**
    - Continue to advance feature enhancements for DODOchain (such as omni-trading) to improve transaction efficiency and user experience.
    - By executing key milestones and plans, increase DODOchain's TVL and promote the healthy growth of the ecosystem.

References

https://whitepaper.io/document/715/dodo-whitepaper

https://docs.mayaprotocol.com/white-paper/readme-1-1

https://docs.eigenlayer.xyz/eigenlayer/overview/whitepaper

https://docs.axelar.dev/axelar_whitepaper.pdf

https://docs.arbitrum.io/launch-orbit-chain/orbit-gentle-introduction

https://docs.altlayer.io/altlayer-documentation

https://layerzero.network/publications/LayerZero_Whitepaper_V2.1.0.pdf

https://solana.com/solana-whitepaper.pdf

https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

https://polkadot.network/whitepaper/

https://github.com/wormhole-foundation/wormhole/blob/main/whitepapers/0007_governor.md

https://www.zetachain.com/whitepaper.pdf

https://chainflip.io/whitepaper.pdf

https://docs.symbiosis.finance/

https://docs.li.fi/

https://docs.xy.finance/

https://blog.chain.link/introducing-the-cross-chain-interoperability-protocol-ccip/