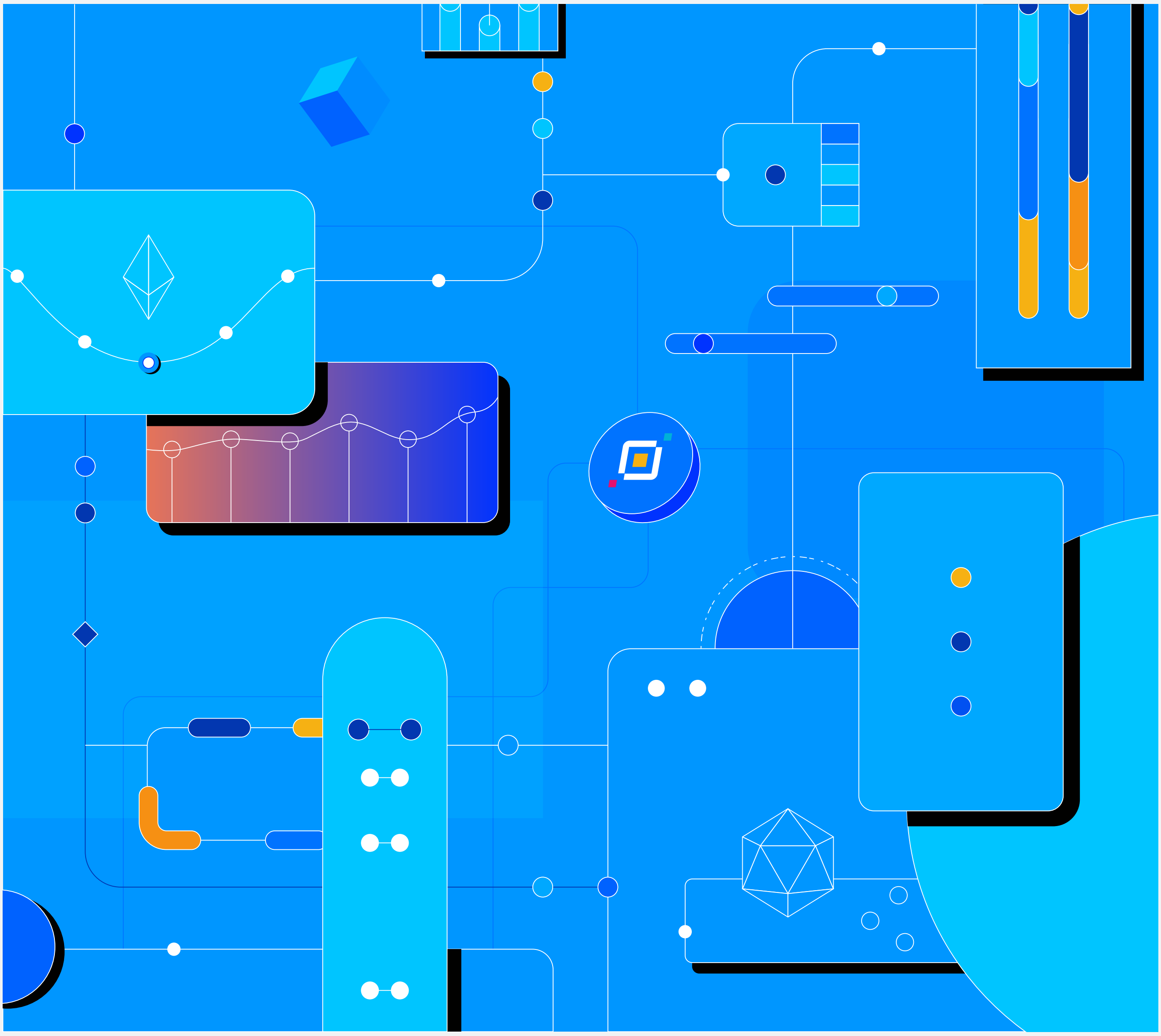
www.platon.network

PlatON

PlatON AppChain Technical Whitepaper

LatticeX Foundation /

Sep 2023



Abstract

With the gradual proliferation of blockchain technology, an increasing number of industries are dedicating themselves to exploring opportunities for development and constructing next-generation applications in the Web3 domain. However, a single blockchain network alone cannot fully meet the specific needs of different industries and application scenarios. These industries and application scenarios lack universality; some require higher performance, some demand stronger privacy protection, some necessitate specific underlying technologies (such as zero-knowledge proofs), and others require improved cross-chain interoperability, and so forth. In cases where public chains are unable to fulfill these particular requirements, the concept of Application Chains (AppChains) has emerged, aiming to provide specialized, efficient, and secure solutions for the development of applications in specific industries and scenarios.

Conducting in-depth research and analysis of diverse application requisites, we have formulated a comprehensive protocol for the application chains solution. Our objective is to establish a universally applicable, dependable, standardized, and flexibly adaptable framework. This framework aims to address the specific technological challenges and pain points encountered by distinct industries, thus rectifying the current deficiencies within the blockchain infrastructure. Our endeavor is to furnish various industries within the Web3 domain with blockchain solutions that are not only more efficient, secure, and credible but also possess the capability for seamless integration. By affording robust technical support, our aspiration is to facilitate the expeditious deployment of applications across assorted sectors within the Web3 landscape. Ultimately, our initiatives endeavor to catalyze innovation and foster advancement within the era of the digital economy.

The structure of the rest of this article is as follows. Session 1 introduces the current status and issues of the Web3 infrastructure. Session 2 provides a brief description of the opportunities and challenges of application chains in the Web3 era. In Session 3, we will focus on introducing a complete set of protocols and frameworks for building application chains based on PlatON. This includes the PlatON Appchain Extension Protocol (PAEP), efficient consensus mechanisms, customizable development, security considerations, usability, and other aspects. Session 4 introduces the comprehensive infrastructure and accompanying tool set for PlatON application chains. Session 5 involves the analysis of practical application scenarios. Finally, Session 6 outlines the ecosystem development road map for PlatON application chains.

Contents

1 / Trends of Web3

1.1 Diverse Development of Public Blockchain Landscape

The continuous emergence of new applications and users has also driven the rapid development of underlying infrastructure. With technological advancements and the growth of the ecosystem, public blockchains have evolved from Ethereum's initial dominance to the current state of 'diversity and competition,' which is the essence of Web3. In the decentralized realm, fundamental infrastructures like public blockchains should neither be nor can they be perpetually monopolistic. Within this diverse landscape, emerging chains that are making a mark or in the process of development also have the opportunity and potential to continue expanding in the public blockchain arena.

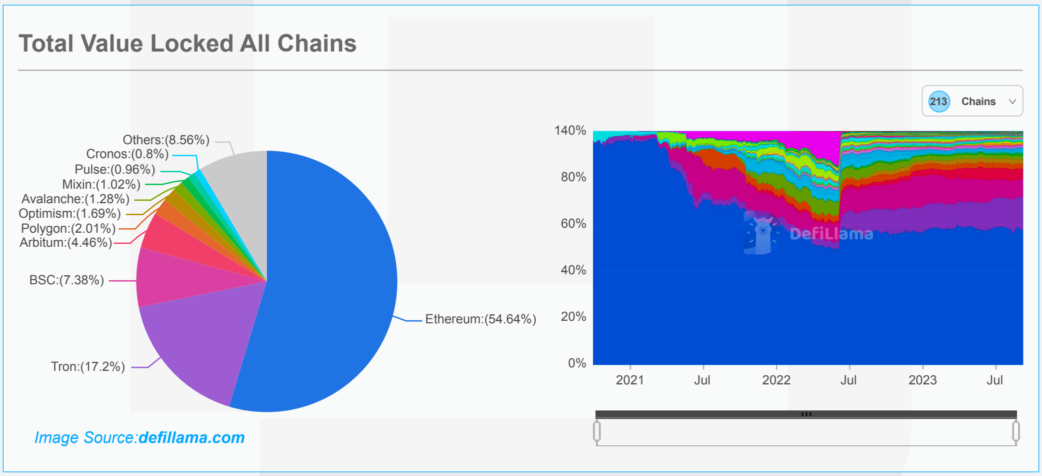


Figure 1 TVL Data Statistics (sourced from Defillama)

From the TVL statistics provided by Defillama, it is evident that Ethereum still maintains its dominant position within the WEB3 ecosystem. However, emerging chains are also showing strong growth momentum. These new public chains can be categorized into the following three types:

EVM-Compatible Chains

The objectives of these public chains are clear. They do not forge new development paths, they instead attempt to address Ethereum's shortcomings within its existing ecosystem using different technologies. This may include improving high performance, faster transaction confirmation times, lower energy consumption, and more. While each of these public chains has its distinct features, their decision to follow the Ethereum community indicates that surpassing Ethereum's influence in actuality is a challenging task.

Independent Development Chains

Cosmos and Polkadot have chosen to enhance chain performance through horizontal scalability since their inception. This approach not only improves the chain's performance but also ensures the stability of the entire ecosystem due to the relative independence of sub-chains, safeguarding against single-point failures. New public chains like Aptos, Sui, and Linera, built by former Meta employees, have also captured the attention of top-tier investment institutions. The standout feature of these public chains, besides inheriting some traits from Libra, is the mechanism of parallel execution designed specifically for payments and high-frequency transactions. The entirely new architecture provides these new public chains with a variety of new perspectives, but due to their need for independent ecosystem development, achieving Ethereum's level of influence in the short term remains a challenging endeavor.

Chains Focusing on Specific Areas

These chains primarily concentrate on solving specific problems within a particular field, aiming to bring entirely new solutions to industries such as gaming, DeFi, insurance, etc. Notable examples include dYdX and Immutable X. The development of these specialized chains can mutually empower existing public chains, promoting the overall prosperity of the ecosystem.

1.2 Challenges of Layer1 Chains

Layer1 chains, as general and public infrastructures, cannot be all-encompassing due to their diverse nature. When it comes to practical development, specific application scenarios will always have varying expectations for deeper integration of capabilities at the underlying layer of public chains. However, considering the multitude of users on public chains, rules cannot be changed at will.

As infrastructure, Layer1 is not well-suited for directly hosting specific applications. Taking Ethereum as an example, it falls short in the following three aspects in meeting application demands, especially before the full implementation of sharding.

High Transaction Fees

Expensive transaction fees significantly limit the usage of Layer1 for both users and developers. In cases of extreme congestion on the Ethereum network, the transaction fee for a simple transfer could soar to hundreds of dollars. Even when the network is less congested, transaction fees still deter many users.

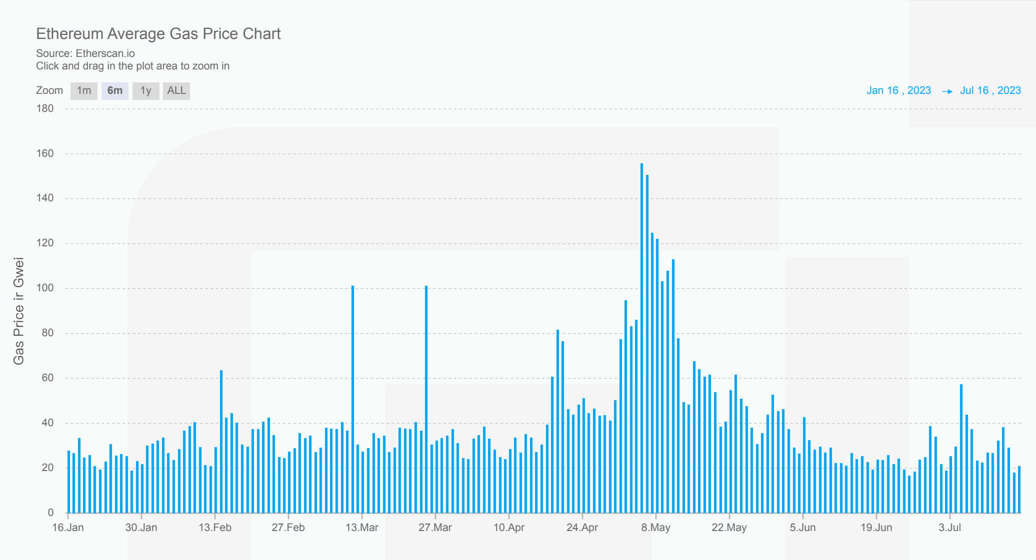


Figure 2: Average Gas Price on Ethereum (sourced from Etherscan)

Low Throughput

Even after the completion of Ethereum's "The Merge," which significantly reduced energy consumption, its daily transaction processing capacity remains limited. As shown in the chart below, Ethereum can handle less than 1.2 million transactions per day, with an average TPS of less than 14 transactions per second.

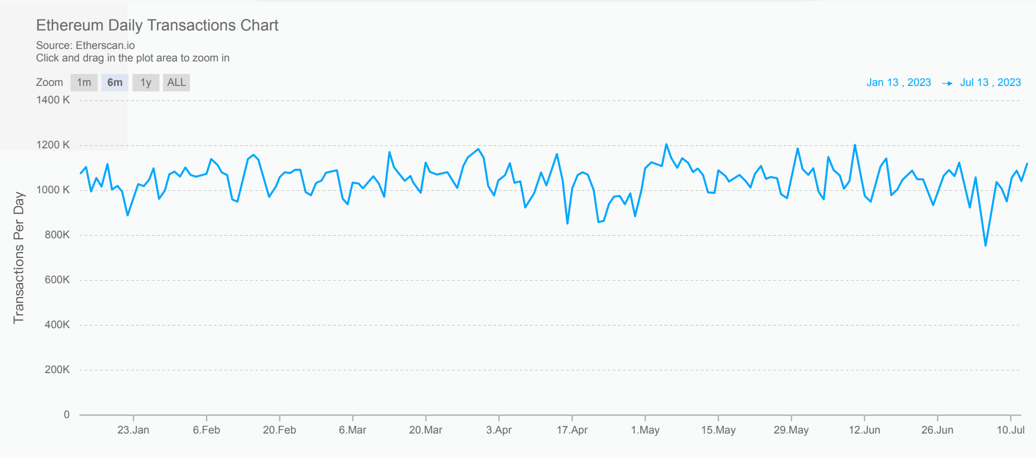


Figure 3: Daily Transaction Count on Ethereum (sourced from Etherscan)

Long Time To Finality

Low throughput keeps the network constantly congested, resulting in prolonged congestion where most transactions cannot be promptly executed and confirmed, leading to a subpar user experience. Below is a recent trend chart depicting transaction congestion on the Ethereum network over the past few days.

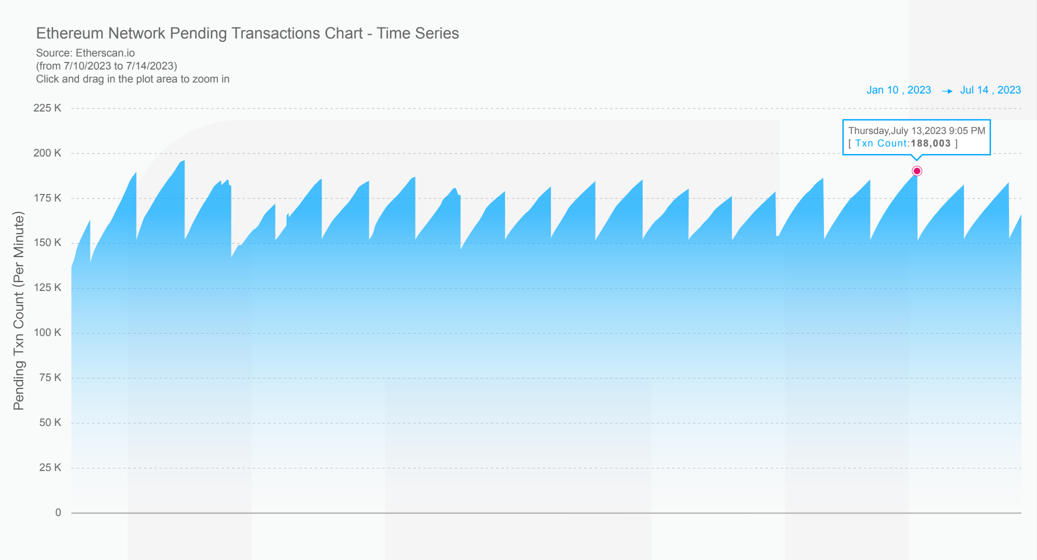


Figure 4: Pending Transactions on Ethereum (sourced from Etherscan)

1.3 Development Trends

The development of blockchain technology has entered a new stage. The past decade has been characterized by the construction of foundational infrastructure, which validated the security, robustness, reliability, and feasibility of the three layers of distributed networks, distributed ledgers, and distributed finance. These three layers form the financial infrastructure of the emerging digital economy, based on Distributed Ledger Technology (DLT) and other Web3 technologies.Looking ahead, the next decade is poised to transition into an era of application development built upon this financial infrastructure. This phase will be marked by the creation of application layer protocols tailored to specific scenarios, needs, and regions. The evolution of blockchain technology is shifting from the foundational infrastructure construction phase to the development of application layer protocols that will provide solutions to various concrete use cases.

According to the Dappradar Q2 2023 report, the total number of daily unique active wallets (dUAW) during the entire second quarter increased by a significant 7.97% compared to the first quarter. The Total Value Locked (TVL) in the DeFi sector continues to remain high, with the Uniswap protocol evolving to version V4. GMX, coupled with Chainlink's oracle support for dynamic pricing, has attracted a considerable user base. The NFT market remains hot, with Blur maintaining its dominant position. While there was a temporary decline in trading volume for OpenSea and CryptoPunks, Immutable XMarketplace and JPG Store have defied the trend by experiencing impressive increases in trading volume. The user base and applications of blockchain games are steadily growing, claiming a 36% market share.

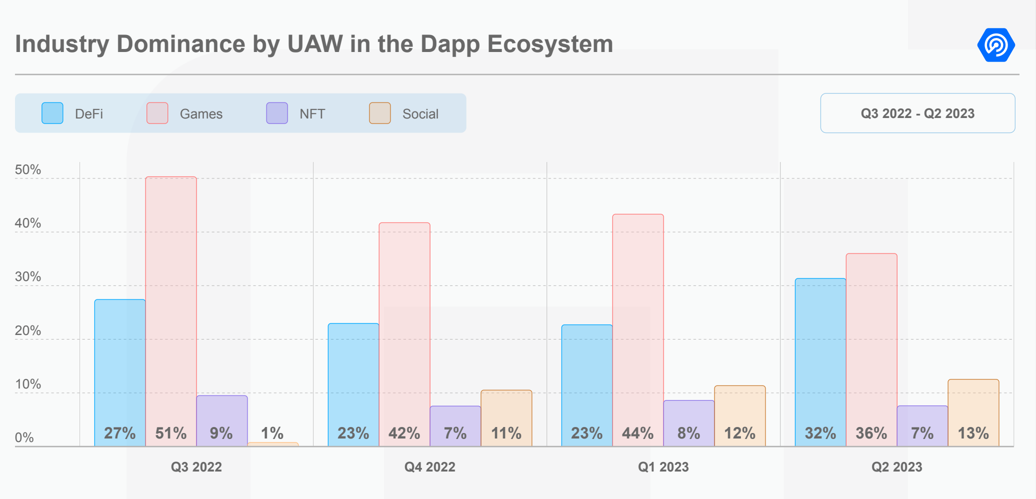


Figure 5: Statistics of Independent Active Wallets in the Dapp Ecosystem (sourced from Dappradar)

Layer1 blockchain solutions fall short in accommodating a wide range of applications and achieving limitless scalability. Layer2 solutions, like Rollup and Validium, follow a core principle of separating the core functions of the public blockchain from security and decentralized mechanisms, which are anchored in Layer1. The tasks of computation and execution are delegated to Layer2, effectively addressing the performance and cost concerns present in Layer1. Layer2 solutions serve as a way to enhance scalability, but they still reside within the foundational infrastructure realm. However, they don't fully cater to the diverse needs of specific use cases when it comes to directly supporting different applications. There are instances where certain application requirements, due to unique demands or regional constraints, can't be met solely by either Layer1 or Layer2 solutions.

During the application protocol development phase, it's unlikely that Layer1 and Layer2 alone can directly support these applications. The optimal solution lies in application chains built on top of Layer1. Similar to the role that App stores played in distributing applications during the WEB2 era, application chains in the WEB3 era, based on distributed ledger technology, will certainly be the model for deploying applications.

2 / Opportunities and Challenges of Application Chains

From the perspective of blockchain technology's development and iteration, the layering and role division of chains have become increasingly distinct. Layer1 is clearly suitable for the role of witnessing and settling, while Layer2 is positioned for computation and execution. The emergence of application chains is rooted in this concept, providing fully independent chains tailored to specific applications to carry individual services, support specific use cases, and meet distinct needs.

2.1 Definition of Application Chains

Application chains differ from Layer1 or Layer2 and are distinct from industry-specific chains. An application chain is a blockchain customized for specific applications. This implies that applications can utilize all resources on the chain. However, akin to Layer2, for security considerations, an application chain does not operate entirely independently. It relies on an existing Layer1, inheriting its security.

The application chain model can be seen as transforming the supply-driven approach to a demand-driven one at the execution level. It refines the relationship between "chain" and "application" to a deeper level. Application chains offer developers flexibility, enabling them to fine-tune various aspects of the chain to meet their application's requirements. Developers can select different Token Economies, Governance, Consensus mechanisms, etc., for the application chain. Running atop existing Layer1, application chains further clarify the hierarchical structure and role division of existing blockchains, granting developers more freedom.

2.2 Characteristics of Application Chains

Application chains lean towards satisfying performance and security while downplaying decentralization in the "impossible triangle." Application chains possess the following features:

Specialization

The value of application chains is greatly manifested in their specialization. If you aim to construct an application requiring privacy protection, you can independently develop and deploy an application chain that supports various cryptography algorithms at the underlying level. Similarly, if you wish to support high-frequency concurrent transactions, you can develop an application chain dedicated to high-frequency transactions. Specialized chains can entirely disregard unrelated applications.

Customizability

A significant issue with existing public chains is their lack of customization in development. After all, public chains serve as infrastructure for the masses, aiming to satisfy the general needs of most users. However, customized development allows application developers to focus on specific business scenarios. They can easily customize functions such as consensus algorithms, virtual machines (VMs), data availability services, and more, leading to a substantial increase in the speed of business development.

Control

Application chains are semi-centralized or moderately centralized platforms. This means that they are tied to a specific application, and the owner of the application should have control over the chain. In the event of a hacker attack or a significant failure leading to user losses, the owner of the application chain should have an effective set of measures in place. For instance, freezing assets, rolling back blocks, and other strategies can ensure the security of the application chain.

Efficiency

Application chains should support higher performance. Since all resources are dedicated to a single application, both the network scale and the total number of accounts are not expected to be large. Therefore, application chains can support higher throughput. These chains can also optimize business processes tailored to specific applications, achieving better performance.

2.3 Opportunities of Application Chains

The solution of application chains infuses new vitality into the entire ecosystem. As the industry continues to explore customized blockchain solutions, an increasing number of applications have recognized the necessity of developing application chains. The opportunities of application chains are reflected in several aspects:

Diverse Ecosystems

During application development, compatibility issues often arise. For instance, applications developed on Cosmos might struggle to be deployed on an EVM ecosystem, and migrating applications from EVM to a MoveVM chain can also be challenging. As an independent execution layer, application chains can effectively address such problems. Application development only needs to adapt to the underlying layer of a single application chain, without concern for compatibility with Layer1.

High-Performance Execution Layer

When certain Layer1 chains cannot meet an application's throughput or cost requirements, building an application chain becomes an ideal choice. Throughput won't be affected by third-party application activities since the application is equipped with a dedicated blockchain that doesn't contend for resources, ensuring a consistent and smooth experience. Blockchain-based gaming applications provide a prime example; most interactive games require high throughput to support user interactions. Deploying a high-performance application chain specifically designed for gaming can easily address performance issues.

Specific Technologies

Some specialized applications require specific technologies. For instance, applications focused on privacy protection might necessitate zero-knowledge proofs (zkp) technology, while applications involving artificial intelligence require AI-related techniques. Due to their compute-intensive nature, these technologies might not be natively supported by Layer1. Hence, employing a dedicated application chain to support them is more appropriate.

Economic Considerations

For applications that require frequent interaction with the underlying blockchain for payment, high transaction fees undoubtedly limit their ability to attract more users. By using an application chain as the execution layer for an application, transaction fees naturally reduce to a minimum. This is due to the fact that all resources on the chain are dedicated solely to one application, eliminating resource competition.

2.4 Challenges of Application Chains

Upon the introduction of application chains, discussions within the community have grown more intense. Despite the aforementioned advantages of application chains, there remain numerous challenges in constructing them for application developers:

Security

Application chains inherit the security of the main chain. Mechanisms like Staking and Slashing can impose high costs on malicious actors, but these mechanisms are not foolproof. The cost of attacks can fluctuate with the actual token price, introducing a certain level of vulnerability to the security of the application chain itself.

Development Costs

For an application developer, deploying a smart contract on Layer1 is far easier than developing an application chain. Running an application chain comes with a series of additional infrastructural requirements and off-chain services. Infrastructure needs include public RPC nodes to support wallet and user interactions with the chain, data analysis infrastructure including block explorers and archive nodes to facilitate user access to on-chain information. Additionally, there are network monitoring, cross-chain solutions, off-chain Oracle services, and more.

Lack of Standard Protocols and Frameworks

Currently, there is no unified protocol for developing and deploying application chains. Public chains each formulate their own framework protocols tailored to their characteristics. This significantly limits the development of application chains. Rather than having application chain developers adapt to different public chains, it would be more beneficial to establish a set of protocol standards. This way, developers could easily accomplish the development and deployment of application chains through simple feature customization and interface implementation.

Lack of Composability

Application chains are individually separate, which can increase the complexity of developing applications with dependencies. While dependencies in deploying smart contracts can be easily managed through cross-contract atomic operations, on application chains, developers need to consider seeking assistance from cross-chain systems.

Challenges of Cross-Chain Interaction

Interactions between application chains and the main chain must occur through cross-chain systems. Cross-chain asset transfers can undoubtedly increase the risk to user assets, and the timeliness of cross-chain messages relies on the processing performance and stability of cross-chain bridges. These factors can somewhat affect the user experience.

3 / PlatON Application Chain

PlatON, as a high-performance Layer1 infrastructure, is well-positioned to foster the development of Layer3 application chain ecosystems, despite the fact that numerous Ethereum Layer2 scaling solutions are already proposing such developments. Unlike Ethereum, which faces scalability challenges, PlatON doesn't encounter scalability issues due to its robust foundational architecture. This makes PlatON an excellent choice for building and advancing Layer3 application chain ecosystems. PlatON's technological advantages encompass the following aspects:

High Throughput and Scalability

PlatON's architecture is designed to handle high transaction throughput and scalability, making it capable of supporting numerous applications and users concurrently without sacrificing performance. Indeed, PlatON network boasts an impressive transaction throughput of over 10,000 transactions per second (10K+ TPS), coupled with a rapid transaction confirmation time measured in seconds, also known as Time to Finality (TTF). This exceptional performance advantage positions PlatON as a leader in scalability within the blockchain landscape.

Customizability and Flexibility

PlatON provides a customizable framework that allows developers to tailor application chains to specific use cases. This flexibility empowers developers to optimize the performance and features of their application chains to meet diverse demands. PlatON is fully compatible with the Ethereum Virtual Machine (EVM), which means that all applications developed using Solidity smart contracts can be directly deployed on PlatON. The RPC interfaces are also fully compatible with Ethereum. Developers can easily port any application to PlatON with minimal adjustments or even without making any modifications at all.

Security and Reliability

PlatON adopts a Proof of Stake (PoS) based consensus mechanism that has been verified by Runtime Verification, ensuring high levels of security and reliability. The PoS mechanism reduces the risk of network attacks and enhances the security of the ecosystem.

Comprehensive Infrastructure

PlatON provides developers with a rich set of tools and resources to support the development and deployment of application chains. This empowers developers to efficiently build application chains. For developers, a robust ecosystem undoubtedly alleviates a significant portion of development workload. PlatON's well-established ecosystem offers support for developers in various aspects, including wallets, browsers, SDKs, cross-chain tools, off-chain Oracle services, integrated RPC services, and more.

Outstanding Economic Efficiency

With its high-performance infrastructure, congestion is minimal, and miners strive to include as many transactions as possible in each block. As a result, transaction fees on the PlatON chain are very low. According to transaction data from PlatScan, the average transaction cost on PlatON in the first half of 2023 was less than 0.001 LAT. This provides a significant incentive for more application developers to build applications on PlatON.

In the PlatON application chain framework solution, we are dedicated to building an application chain extension standard with PlatON as the RootChain, based on the new layered blockchain and modular architecture approach. This aims to provide flexible, reliable, and all-in-one blockchain solutions for various industries and different application scenarios.

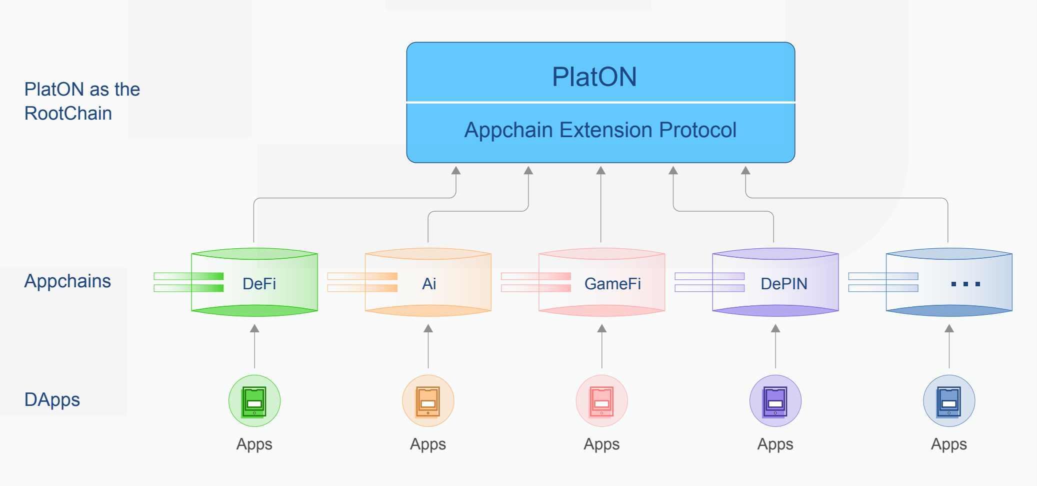


Figure 6 PlatON AppChain Framework

Since the application chain itself cannot independently host applications, it becomes essential to establish standardized and efficient inter-chain communication protocols between the application chain and its RootChain. On one hand, rigorous inter-chain protocols can ensure the security and stability of the application chain. On the other hand, through the standardization of inter-chain communication, standardized underlying interfaces can be provided for various application chains, adapting to different scenarios and reducing unnecessary and repetitive development efforts.

3.1 PoS-based PlatON application chain extension protocol

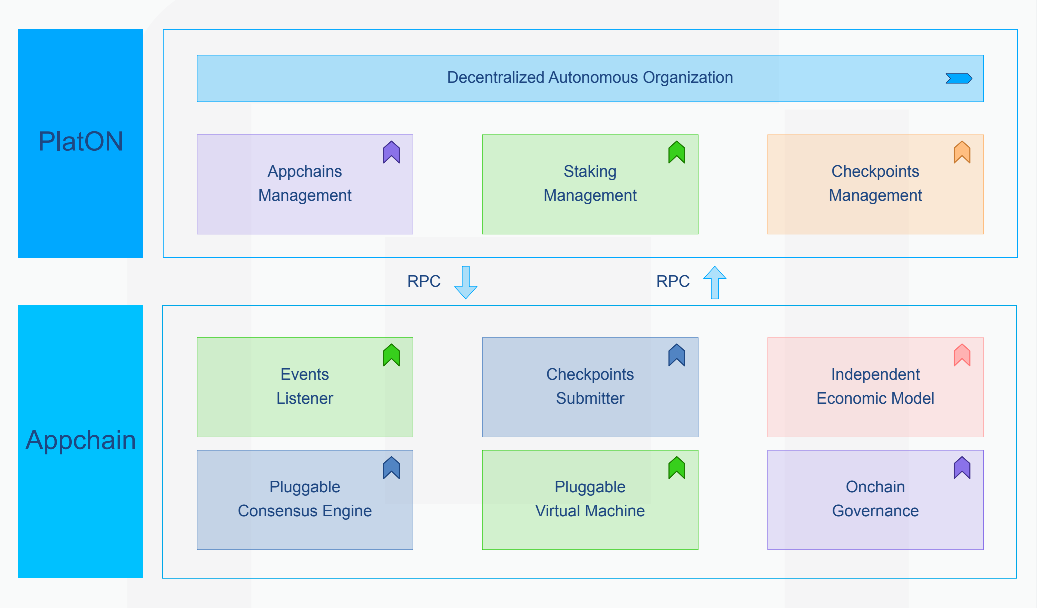


Figure 7 PlatON application chain extension protocol

PlatON's application chain extension protocol clearly distinguishes the roles of the main chain (RootChain) and the application chains (Appchains). In this framework, PlatON serves as the RootChain that the application chains depend on, playing the role of the witnessing layer. The application chains, on the other hand, serve solely as the execution layer.

3.1.1 Witness Layer

The design principles of the application chain itself weaken the "decentralization" feature, but this does not mean that applications built on the application chain are private or "centralized." Through clever design, we can effectively enhance the RootChain's "decentralized" attributes and make it the "witness layer" of the entire application chain extension protocol.

As the core of a blockchain network, the RootChain possesses high security and decentralization characteristics. The attributes that the application chain lacks can be well complimented on the RootChain. To achieve a harmonious integration between the two, the PlatON application chain extension protocol specifies the responsibilities of the RootChain in the entire framework from the following three dimensions.

Trust Mechanism

The application chain employs efficient consensus algorithms that necessitate a limited count of validating nodes for swift consensus. To bolster trust within this context, PlatON employs the following strategies within its primary network:

- Validating nodes affiliated with the application chain are required to engage in Staking on the PlatON network. This involves using tokens such as LAT, native token of appli cation chain or well-established stablecoins. Once Staking is initiated, the tokens become locked. During each instance of consensus participation, nodes are carefully selected from a subset of all validating nodes that have undergone the Staking process. This selection process is verifiable, ensuring transparency and integrity. Staking serves two main purposes: it raises the entry bar for entities aspiring to become validators for the application chain, weeding out low-quality validators. Additionally, the open recruitment of validators and their random selection for consensus participation ensures the decentralization of validating nodes. Depending on the context, validators can also collectively engage in consensus throughout the process.

- At regular intervals, the application chain is required to submit its state (transaction tree root, receipt tree root, etc.) along with valid proofs (Merkle Proofs) as a Checkpoint to PlatON. PlatON then performs legitimacy verification of the submitted Checkpoint within the EVM. Once the verification is successful, the latest state of the application chain is recorded on Layer1.

Since both the staking by application chain validators and the submission of Checkpoints occur on the PlatON platform, this not only establishes admission criteria for application chain validators but also enables the periodic feedback of execution results from the application chain to PlatON. Additionally, the verification of these phase-wise execution results on the main chain enhances the credibility of application chain data.

Security

The Staking mechanism can elevate the barrier for malicious activities. Additionally, PlatON integrates Layer1's Slashing to further enhance the security of the application chain. In the event that a validation node engages in inaction (such as not producing blocks or not signing) or malicious actions like double-spending blocks or double-signing votes, if such behavior is detected by other nodes in the network, any validator can submit evidence to the Staking contract on PlatON for verification. Upon successful verification, appropriate penalties will be imposed on the offending validator according to the protocol.

Incentives

PlatON's application chain extension protocol is based on Proof of Stake (PoS). To introduce a positive competition mechanism, according to protocol rules, any node contributing to the network's normal operation will receive system rewards based on factors such as the duration of staking or delegation, participation in consensus rounds, and submission of Checkpoints. The funding for these rewards can come from the issuance of application chain tokens, dedicated incentive pools, or separate foundations established by the application chain projects.

- Staking Rewards: Nodes staking tokens receive periodic rewards based on their staked amount (weight) and staking duration.

- Delegation Rewards: Ordinary accounts delegating tokens to validators receive rewards based on the validator's configured ratio and weight.

- Submitting Slashing Proof Rewards: To encourage active reporting of inaction and malicious behavior, the Staking contract on PlatON's application chain provides a fixed reward to validators reporting instances of inaction, according to system parameters (modifiable through on-chain governance). For malicious behavior, the protocol enforces the confiscation of all staked tokens from the offending node and rewards the reporting validator with 50% of the confiscated amount.

- Submitting Checkpoints Rewards: Checkpoints, crucial for the healthy and stable operation of the application chain, carry significant importance. To encourage validators to submit Checkpoints promptly, validators who submit Checkpoints are rewarded with a fixed amount.

Furthermore, the PlatON application chain protocol maintains a decentralized autonomous organization (DAO) that ensures the healthy development of the application chain ecosystem. On one hand, the DAO actively participates in the construction, supervision, and governance of the application chain's development. On the other hand, this decentralized governance approach helps mitigate the risk of centralized control over the application chain.

3.1.2 Execution Layer

As the execution layer, the application chain is responsible not only for supporting the necessary transaction computations and executions required for application development but also for real-time monitoring of events on the main chain and related to the current application chain. It also involves submitting Checkpoints to the main chain:

Event Listeners

The application chain's event listeners are responsible for real-time monitoring of events occurring on the main chain, such as staking, delegation, penalties, reward distribution, validator exits, updates to application chain system parameters, version upgrades, and more. Once an event related to the application chain is detected, the protocol allows the block proposer to initiate an internal transaction to synchronize the event information and update the application chain accordingly.

Checkpoint Submitter

The Checkpoint submitter periodically compiles information from the application chain, including blocks, transactions, and receipts, into a fixed data structure according to rules such as Merkle trees. It then generates a digest and proof, forming a Checkpoint message. This Checkpoint message is submitted to the main chain by the rotating set of validator nodes.

Independent Economic Model

The application chain has the flexibility to independently execute transactions unique to itself and establish its own economic model. PlatON's application chain incorporates a configurable economic model that enables settings like capped total circulation or fixed annual issuance ratios. Block proposers can also introduce fixed miner rewards, or opt for unified incentivization and settlement on Layer1, providing significant freedom of choice to application developers.

On-Chain Governance

On-chain governance, achieved through contracts like DAO deployed on the main chain, employs governance proposals to facilitate version upgrades and system parameter adjustments for the application chain. This mechanism empowers the application chain with a governance system executed on the main chain.

3.1.3 Application Chain Governance

Once an application chain is developed according to the PlatON Application Chain Extension Protocol, it needs to be registered within the AppchainRegistry contract on the PlatON main chain. Upon successful registration, it can be seamlessly deployed onto the PlatON application chain framework and integrated into all infrastructure components. Centralized management of application chains serves several purposes:

Support for Required Infrastructure:
Developing an application chain entails not only the execution layer but also relies on various infrastructure components like browsers, wallets, cross-chain systems, and payment gateways. Centralized management facilitates the registration of the application chain's ID within the associated infrastructure. This streamlines the generation and deployment of components compatible with the application chain.

Ensuring Application Chain's Controllability:
One of the benefits of application chains is the increased freedom and control offered to developers. Both the application's developers and the on-chain autonomous organization share control over the application chain. This control encompasses:

- Node Admission: When an application developer stakes and registers a new application chain on the main chain, they can decide whether the application chain's nodes should be subject to admission control. This control can involve authentication (KYC), providing specific qualifications, or employing whitelisting mechanisms.

- On-Chain Governance: The PlatON Application Chain Protocol features a comprehensive governance framework. Application chains can opt for self-governance (where current application chain validators participate) or governance through a DAO mechanism to propose upgrades and manage adjustable system parameters. To prevent malicious occupation of resources and useless attacks, registered application chains must complete staking and become DAO members.

3.2 Scalable Application Chain Framework

Customizable development has consistently been regarded as the primary advantage of application chains. The term "customization" doesn't merely refer to the underlying infrastructure but can encompass the interdependent foundational elements as well. PlatON's application chain offers developers an extensive set of components to ensure comprehensive support tailored to their needs.

3.2.1 Pluggable Consensus Mechanism

Recognizing that diverse applications might have varying consensus algorithm requirements, the PlatON application chain incorporates a pluggable consensus engine design. This design includes an engine interface layer and includes built-in BFT consensus algorithms and PoA consensus. Developers can also implement custom consensus mechanisms through a unified interface.

Built-in Consensus Based on Giskard

BFT consensus typically requires extensive communication and complex message passing among nodes, which can lead to performance issues and high latency. While there are optimizations that can improve performance, BFT consensus may still demand more computational and communication resources compared to other consensus algorithms.

The BFT consensus of PlatON's application chain adopts a solution based on the Giskard consensus (for specific details, please refer to the PlatON technical documentation), and has been optimized specifically to address the performance issues associated with BFT consensus. Through a series of technological innovations, the PlatON application chain effectively enhances consensus efficiency and throughput while ensuring system security and correctness.

Specifically, the PlatON application chain modifies the process of the Giskard consensus to adopt a Leader mode. This optimization transforms the broadcast of consensus messages into point-to-point message transmission, reducing the number of consensus messages from exponential to constant levels. This optimization significantly lowers the consumption of network resources and enhances consensus efficiency.

In the new block proposal process, the Leader proposes a block and sends it to other validators. Validators verify and execute the block, then send block votes to the Leader. The Leader collects block votes and sends a Quorum Certificate (QC) to other validators, ultimately finalizing the block and continuing the block proposal. Although PlatON's application chain sacrifices some decentralization characteristics by adopting the Leader mode in its BFT consensus, it simultaneously guarantees system security and correctness.

PoA Consensus Protocol Combined with Staking

Proof of Authority (PoA) is a permissioned consensus mechanism that leverages identity staking to facilitate fast transactions and adds blocks through a network of authorized and reputable validators. However, the challenge with PoA consensus lies in its centralized nature.

In the context of PlatON's application chain, an approach is taken to address the centralization issue of the PoA consensus mechanism by integrating it with a Staking mechanism. Validators can become validators by staking a certain amount of LAT (or the native token of the application chain) or stablecoins. In each block generation round, validators are selected for block production through a Verifiable Random Function (VRF), introducing an element of randomness.

Through this approach, the PlatON application chain ensures both the benefits of PoA consensus, such as fast transactions and validation by authorized participants, and the achievement of decentralization goals. By combining the Staking mechanism with the PoA consensus, the application chain strikes a balance between speed, security, and decentralization.

3.2.2 Pluggable Virtual Machines

The PlatON application chain inherently supports the EVM (Ethereum Virtual Machine) and WASM (WebAssembly) virtual machines. The underlying code is entirely open-source, based on the LGPL open-source license. Through abstracting the underlying interfaces, developers can perform secondary development based on standard interfaces, allowing the creation of any virtual machine compliant with standards, including MoveVM.

3.2.3 Customizable Economic Model

The economic incentive mechanism of the PlatON application chain can be easily configured through system parameters. Mechanisms such as token issuance, miner incentive strategies, and slashing measures can all be customized through these system parameters, and these parameters are subject to on-chain governance.

3.2.4 Customizable On-Chain Governance

Whether it's Bitcoin or Ethereum, the underlying protocols of blockchain have been continuously evolving and improving since their inception. Influenced by the idea of decentralization, decisions regarding the self-improvement of public chain protocols do not rest solely with the code developers or ordinary users; they belong to the entire community.

3.2.4.1 On-Chain Governance and Applications

On-chain governance involves encoding and storing governance rules, combining on-chain voting and automated vote counting to determine the effectiveness of new protocols. On-chain governance digitizes community decisions, significantly reducing coordination costs for stakeholders. Traditional on-chain governance is commonly used for the following purposes:

System Parameter Governance

Core parameter values affecting blockchain system security and stability often require adjustments based on the network's actual operational status. For instance, values such as the maximum number of validators, token annual issuance rate, and the proportion of staked funds to be slashed in case of malicious or inactive behavior of validator nodes. The adjustment of these parameters' values is influenced by factors like technical iterations, total circulating token supply, and price, and they need to be adjusted to values deemed secure and reasonable by the community at different times.

Major Version Upgrades

For underlying protocol rules that cannot be easily modified by adjusting parameter values, the community can initiate proposals for version upgrades. Similarly, after community discussion and deliberation, if the proposal is voted upon and approved by the community, developers proceed with version development and deployment. Validators upgrade to the new version, initiate on-chain proposals and voting. Once the proposal is approved, the old version becomes incompatible with the new protocol and can no longer synchronize with the main network information.

3.2.4.2 Challenges of On-Chain Governance

While traditional on-chain governance is straightforward and efficient, it also has several shortcomings:

Lack of Participation

On one hand, frequent governance activities can lead to voter fatigue, where voters might not fulfill their voting responsibilities diligently. On the other hand, voters often show indifference to proposals unrelated to their interests, resulting in a lack of enthusiastic participation.

Governance Attacks

Token voting systems are essentially controlled by financial stakeholders, giving those with the highest financial interests significant decision-making power. This susceptibility allows the governance system to be vulnerable to bribery attacks. Small token holders can't influence protocol improvements.

Inadequate Incentives

Proposal voting requires making transactions and paying transaction fees, yet there aren't enough incentives for voting behavior.

Tendency Towards Benefitting Interests Rather Than Rational Decision-Making

Voters, as stakeholders, usually prioritize whether new protocols are beneficial to them. Over time, this could lead to proposal trends that are more focused on self-interest rather than the protocol's long-term success.

Lack of Flexibility

The equal participation requirement for both major improvements and minor proposals limits the flexibility of governance.

3.2.4.3 Customizable On-Chain Governance

To address the aforementioned issues, PlatON has meticulously designed a set of application-specific governance contracts called DAO (Decentralized Autonomous Organization) for its application chains. These DAO contracts modularize voter management, weight management, and governance methods, catering to various governance requirements of the application chains.

Voter Management

Application chains should never allow validators to gain control over governance, as rational validators will continually strive to maximize their own interests within the application chain's economy. This directly conflicts with the interests of other participants and goes against the concept of cryptographic networks as Minimally Extractive Coordinators. Defining stakeholders and their various objectives at the outset of a project is crucial for the success of a governance system. This approach enables addressing how conflicting objectives are handled to best achieve the overall goals of the platform. Every participant in the blockchain ecosystem has an interest in the overall success of the ecosystem, as it operates on a mutually beneficial basis. The objectives of a governance system and the motivation behind a "decentralized" governance mechanism aim to ensure that decisions made for the ecosystem align with the desires of all participants.

Any account holding LAT (or native token of application chain) tokens can become a DAO member by staking those tokens. DAO members are essentially voters with distinct powers and responsibilities. They assist in managing off-chain governance processes (such as PIP proposals), maintain alignment with the community through transparent and data-driven opinions, and have the right to supervise and use their votes responsibly. Additionally, they can propose on-chain votes without typical proposal thresholds.

The purpose of voter management is to delegate specialized tasks to specialized individuals. DAO members are dedicated to governing all application chains. Due to varying levels of familiarity and concern for different application chains, members must actively participate in community discussions and development to garner support from stakeholders. DAO members acquire tokens through delegation from various stakeholders (owners, users, validators) of the application chain. Once their stake reaches a system threshold, they can participate in the on-chain governance of the designated application chain.

Weight Management

An important and often overlooked issue in governance design revolves around the weighting of stakeholders in the ecosystem. For blockchain-based platforms, many resources that are crucial to the network's success are contributed voluntarily by participants, such as the hardware resources of mining nodes. These critical resources play an essential role in the operation of the entire network, so it's important to give sufficient consideration to their allocation when considering governance privileges.

Weight management involves establishing rules for the proportions of different types of tokens (such as freely circulating tokens and tokens locked by validators) in terms of their respective weights. These rules can be customized and managed by the application chain developers or operators.

Governance Method Management

When designing the governance process, it's crucial to understand what decisions need to be made within the governance framework. The multitude of decisions that the ecosystem faces may benefit from different governance processes. For example, some decisions might require proprietary information and expert involvement, while others might need to incorporate the preferences of community members to ensure sufficient support for the decision.

Listing out in advance the categories of operational processes that might need upgrading over time, as well as all potential decisions that might need to be made, can help ensure the establishment of a cohesive and robust governance system. Governance modes manage the ability to customize categories of governance decisions for the project. These categories can include the stages and rounds in which decisions are to be voted upon, rules defining voting rights, required quorum, available voting tokens, how votes are counted, pass rates, and more.

In conclusion, PlatON addresses issues such as governance fatigue and governance attacks through a modular governance framework using the DAO approach. This provides developers with a more flexible and viable on-chain governance solution.

4 / Supporting Infrastructure

The inherent complexity of developing application chains has deterred some developers from pursuing this path. In order to further mitigate the challenges associated with application chain development, PlatON not only introduces the Application Chain Extension Protocol and Application Chain Framework, but also provides a wealth of complementary applications and tools. These tools facilitate one-click deployment of application chains, fundamentally addressing the difficulties in application chain development. Developers can now focus primarily on providing robust foundational support for their developed applications, without the need to concern themselves with the development and deploy ment of peripheral infrastructure.

4.1 PlatON-Bridge

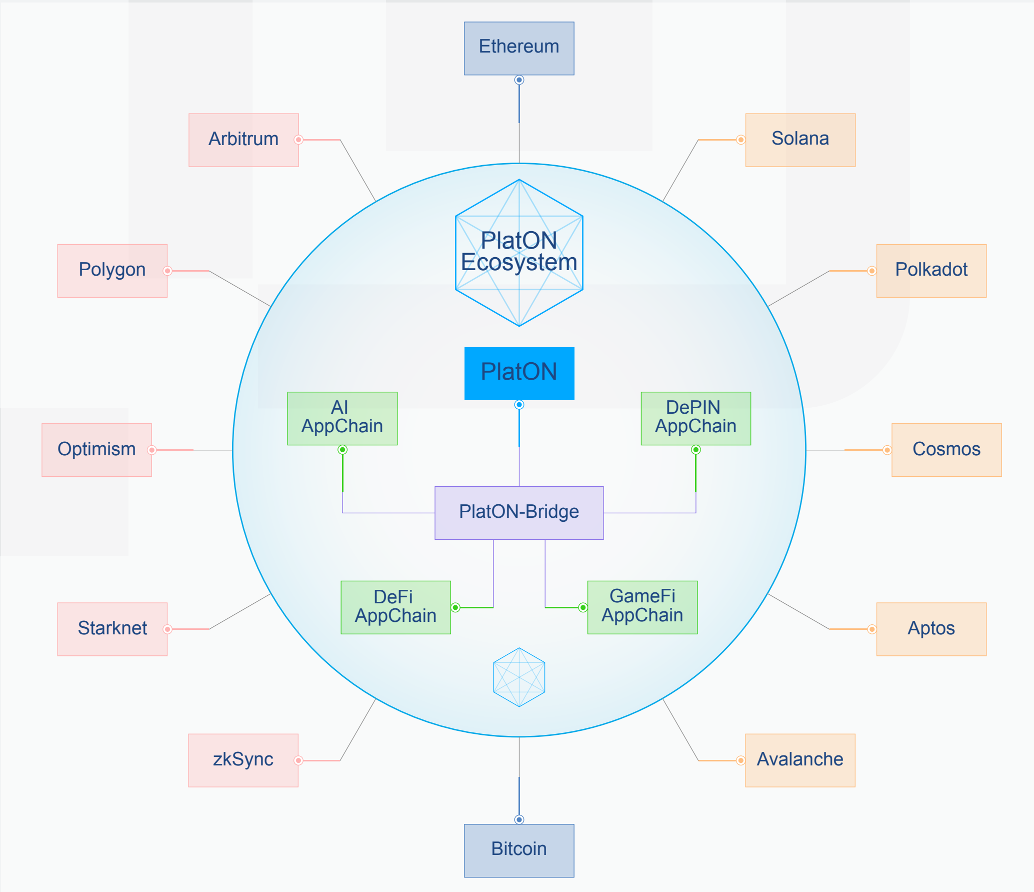


Figure 8 PlatON Crosschain Bridge

PlatON-AppChain offers developers an efficient platform to run applications that meet requirements for throughput, security, and cost-effectiveness. However, each individual AppChain leads to network fragmentation, where each chain operates in isolation. Therefore, the need for cross-chain functionality arises to form a super network. PlatON-Bridge, built upon message flow, overcomes limitations imposed by contract virtual machines (such as EVM, WASM, Move, etc.). As depicted in the diagram, through PlatON-Bridge, the cross-chain bridge not only interconnects AppChain networks but also establishes a connection between AppChain and the PlatON ecosystem, as well as other Layer1 public chain ecosystems. The flow of messages and assets within the AppChain and PlatON ecosystem creates a value-rich network.

PlatON-Bridge, as a part of the AppChain network, employs an external verification approach for cross-chain transactions. This implies that PlatON-Bridge acts as a chain within the AppChain network itself. This approach offers the advantage of reducing the complexity for other AppChains. They do not need to listen to messages from the network's chains, thus lowering communication complexities for the AppChains. With sufficient decentralization assurance, PlatON-Bridge as an AppChain uses BFT consensus to confirm cross-chain messages, preventing malicious tampering.For network security, the number of validators will be adjusted based on the scale of the PlatON-AppChain. Initially, with a limited number of AppChains and a smaller total network value, the validator count might be 25+. As the network evolves and its total value increases, the validator count could transition from 25 to 35, and even up to 45, ensuring the decentralized nature of the cross-chain network.PlatON-Bridge will serve as the foundation for the flow of networks within the AppChain ecosystem.

PlatON-Bridge adopts the Arbitrary Message Bridge (AMB) solution, which allows for the transmission of various message types from the source chain to the target chain based on project requirements. PlatON-Bridge provides a contract suite to developers, encompassing modules for sending and receiving cross-chain messages. Developers can focus on their business logic by deploying their business contracts, thus achieving cross-chain application development. All PlatON-AppChains deployed on the mainnet will possess the cross-chain capabilities of PlatON-Bridge.

PlatON-Bridge extends support to the EVM ecosystem, not only interconnecting different AppChains but also providing support to other EVM-based public chains such as Ethereum, BSC, Polygon, etc. Through the deployment of contract suites, PlatON-Bridge establishes connections between diverse network ecosystems and the PlatON ecosystem, fostering ecosystem growth. Leveraging PlatON-Bridge, developers can construct various projects like

DeFi, Oracle, Social, Gaming, and more. Additionally, beyond EVM, PlatON-Bridge plans to support contract ecosystems like WASM and Move, culminating in a fully networked message flow.

Asset flow is a crucial direction for the PlatON-AppChain ecosystem. Building upon the AMB cross-chain bridge, PlatON-Bridge has constructed an asset cross-chain bridge. Utilizing the AMB cross-chain messaging mechanism and a comprehensive cross-chain contract development suite, this bridge facilitates asset movement not only within the PlatON-AppChain ecosystem but also between AppChain and the PlatON ecosystem, as well as between AppChain and other Layer1 ecosystems. Through PlatON-Bridge's asset cross-chain bridge, user asset liquidity is enhanced, driving further innovation in applications.

4.1.1 Cross-Chain Architecture

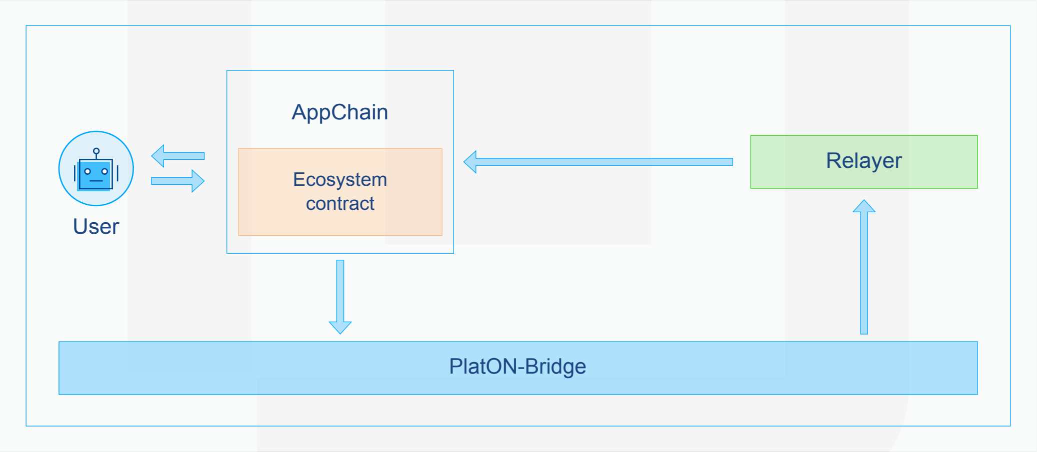


Figure 9 PlatON Cross–Chain Architecture

PlatON-Bridge is composed of Ecosystem Contracts, Bridge, and Relayers.

Ecological Contracts

Ecological contracts in the PlatON-Bridge ecosystem are governed by the PlatON-Bridge platform itself, constituting an internal system with the primary purpose of providing a functional suite for other AppChain developers.

Bridge

Functioning as a cross-chain bridge AppChain, the Bridge component adopts a PoS (Proof of Stake) + BFT (Byzantine Fault Tolerance) hybrid consensus mechanism. This hybrid approach involves the election of validators through the PoS model, followed by the BFT consensus process to confirm cross-chain messages. To ensure decentralization, the plan involves enlisting influential industry projects to participate as validators within the Bridge's consensus process.

Unlike traditional PoS Chains, where validators only verify transactions within their own chain, cross-chain bridge validators undertake a more intricate role. They are not only responsible for validating transactions within their own chain but also for monitoring cross-chain transaction information from other AppChains within the PlatON-AppChain network. Each validator is required to verify the cross-chain transaction information and transform it into Verifiable Transaction Approval (VTA) transactions specific to the cross-chain bridge. These VTA transactions are then aggregated into blocks and verified and signed by BFT validators.

Relayer

The Relayer plays a crucial role in the entire cross-chain process. If the Bridge assumes the role of "reading" from the source chain, then the Relayer plays the role of "writing" to the target chain.

Although the Relayer is a vital component of PlatON-Bridge, it doesn't pose a security threat but affects only the liveness. In other words, the Relayer is responsible for transmitting the VTA (Verifiable Transaction Approval) information from the Bridge to the target chain and cannot modify the VTA to tamper with the information on the target chain. Based on this, the Relayer acts as the delivery mechanism to the target chain.There are several forms of Relayers:

- Client Relayer: Client Relayers can be deployed within wallets and browsers. Users' client applications handle the delivery process of the Relayer. Although this simplifies the development process, it makes the user's operation process cumbersome, and users must pay on-chain transaction fees for the Relayer. This approach is not usually chosen in mature projects due to its complexity for users but might be suitable for MVPs or rapid prototype verification.

- Dedicated Relayer: Application projects can add a dedicated Relayer to handle specific types of VTA transactions. This addresses the user experience issues of the client Relayer. The dedicated Relayer can also reduce Gas fees for VTA transactions through batch processing methods like bundling. Despite being called "dedicated," it's still an untrusted role. However, the submitted VTA is publicly immutable, making the submitted VTA "trusted".

- Universal Relayer: As an integral part of PlatON-Bridge, PlatON will introduce a universal Relayer to enhance user experience and improve developer efficiency, simplifying the process for users and making it more efficient for developers.

4.1.2 Cross-Chain Security and Governance

PlatON-Bridge operates under the PoS consensus mechanism, elected by validators, with BFT (Byzantine Fault Tolerance) consensus. The validators are endorsed by well-known projects. To ensure the reliability of information from the source chain, each validator will deploy independent full nodes for each AppChain. Validators will generate state proofs for each on-chain cross-chain transaction, which can be independently verified by any party.

PlatON-Bridge's governance will be conducted through on-chain governance. A PoS-based governance contract will be deployed on PlatON, responsible for validator elections and contract upgrades. Current governance directions include modifying the validator set, expanding the validator set, and upgrading ecosystem contracts. All on-chain governance contracts will be open-source and will undergo auditing by reputable industry audit firms.

To ensure the security of Relayer transactions, MPC (Multi-Party Computation) key management services will be provided for distributed key generation and signing services. Distributed keys ensure that the loss of individual key shards does not compromise the security of the Relayer system. Additionally, traditional identity verification methods such as Two-Factor Authentication (2FA) can be used to enhance security. Shards can be refreshed periodically or manually to maintain security. Distributed signatures will ensure that Relayer signatures cannot be controlled by any single entity for initiating unauthorized transactions, ensuring the security of signatures.

4.2 Browser

PlatON's application chain browser provides automatic support for collecting and displaying block and transaction information on the application chain. For an application chain to use the browser, it only needs to register with a unique ID for the application chain. Additionally, the application chain needs to configure its account address format, token units, total token supply, and other relevant information to easily deploy the browser.

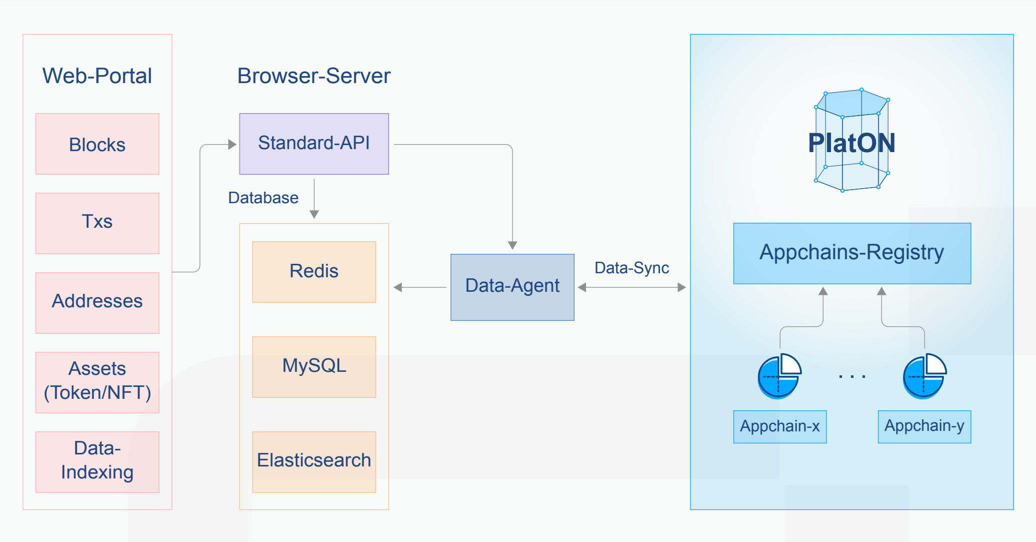


Figure 10 PlatON AppChain Browser Architecture

Web-Portal

The Web Portal provides modular functional components, including standardized modules for blocks, transactions, addresses, assets (tokens/NFTs), and more. It also supports custom data displays for various application chains.

Browser-Server

The Browser-Server is the unified server program for the application chain browser, offering standardized data query APIs.

Database

The storage layer utilizes three different types of databases to handle different types of user data query needs:

- Redis: Used for storing frequently accessed hot data, such as commonly used ERC20 contract addresses, frequently repeated addresses, etc.
- MySQL: MySQL is employed to store complex relational data structures, such as staking-delegation relationships, governance proposals, and voting progress.
- Elasticsearch: Elasticsearch supports bulk data queries and traversal, such as block, transaction, and other data.

Data-Agent

The Data-Agent is a data proxy service that listens to and synchronizes on-chain data from different application chains. It not only synchronizes standard on-chain data like transactions and blocks into the database but also responds in real-time to query requests from the Browser-Server by directly reading on-chain data from the application chain via RPC.

In addition to the regular block explorer, PlatON's application chains also have dedicated NFT-customized browsers, providing significant convenience for NFT application development.

4.3 Wallets

Wallets play a crucial role as one of the foundational tools in the WEB3 ecosystem. They have evolved from simple functions like transfers and account key management to encompassing a wide range of capabilities in the WEB3 space, including DeFi, NFTs, GameFi, and more. As traditional applications find their way into the WEB3 world through areas like DeFi, NFTs, and GameFi, wallets have become key players in guiding users from WEB2 to WEB3.

In order to provide robust support for application developers to attract users, the PlatON ecosystem offers both ready-to-use wallets and wallet services for managing keys and assets. Additionally, PlatON supports wallet plugins and SDKs that developers can customize:

Ready-to-Use Wallets

- ATON: PlatON's ATON wallet backend service automatically listens to PlatON application chain management contracts. When a new application chain is successfully registered, the ATON backend service activates the wallet service for the new application chain based on the chain's ID, address format, token name, and other information. Application chain developers don't need to perform any development or customization to use all wallet functionalities available on ATON.

- WEB Wallet: With an increasing number of users accustomed to using wallets in web interfaces, PlatON's application chain browser integrates a WEB wallet plugin. This plugin integrates third-party wallets like MetaMask, WalletConnect, and Particle, giving users the option to easily access the application chain using their preferred wallet. Third-party wallets also support social account login and social recovery features, significantly enhancing the user experience of using a WEB wallet.

- Third-Party Wallets: PlatON has integrated with various third-party wallets such as imToken, Mathwallet, Tokenpocket, Coin98, Bitkeep, Cobo, Bitpie, Particle, OpenBlock, Unipass, and more. Other EVM-compatible chain wallets can also be easily configured for direct use on the PlatON application chain.

Wallet's Fundamental Services

- MPC Key Custody Service: For accounts requiring an extremely high level of security, using a regular ready-to-use wallet may pose certain security risks. To mitigate these risks, the industry commonly employs a strategy to distribute and manage risks across multiple parties. MPC (Multi-Party Computation) key custody wallets are a typical solution for this. PlatON's MPC key custody service supports generating and managing key shards through secure multi-party computation. The service currently supports two sets of key systems: ECDSA and BLS, with 2-2 and 2-3 algorithms. In the 2-2 algorithm, users and the MPC server negotiate algorithmically for their respective key shards. Users hold one key shard, while the MPC server manages the other shard. To perform a transfer, both parties need to cooperate in the calculation to sign the transaction. In the 2-3 algorithm, users hold two key shards, while the MPC server holds only one. Users regularly use one shard to sign transactions with the server's shard. If one shard is accidentally lost, the user can still conduct transfers using the other shard along with the server's shard, greatly enhancing account security.

- Abstract Account Public Service: PlatON supports the EIP-4337 standard and provides a unified standard Bundler service. The public Paymaster contract uses LAT (PlatON's native token or native token of application chains) as the default transaction fee for sending transactions. Of course, users can also define using other ERC-20 tokens.

- Social Account Login and Recovery: To bridge the gap between WEB2 and WEB3 for developers, PlatON's wallet plugin and SDK integrate the ability to log in and recover accounts through social accounts. Application chain developers can easily incorporate social logins (such as Facebook, Google, Apple, Github, etc.) into their dApps. Social logins not only facilitate rapid application access for users but also allow binding of a guardian email to a WEB3 account. When a contract wallet is used, and a user loses their key, they can use PlatON's provided guardian email domain key (Domain Keys Identified Mail) verification service to apply for account recovery, preventing asset loss and further enhancing account security.

4.4 Unified API Services

Application developers often face the challenge of migrating and adapting their applications to different chains. The various API interfaces of different chains can create significant burdens for developers in terms of adaptation and debugging. To provide developers with the utmost convenience, PlatON's application chain offers a unified API service.

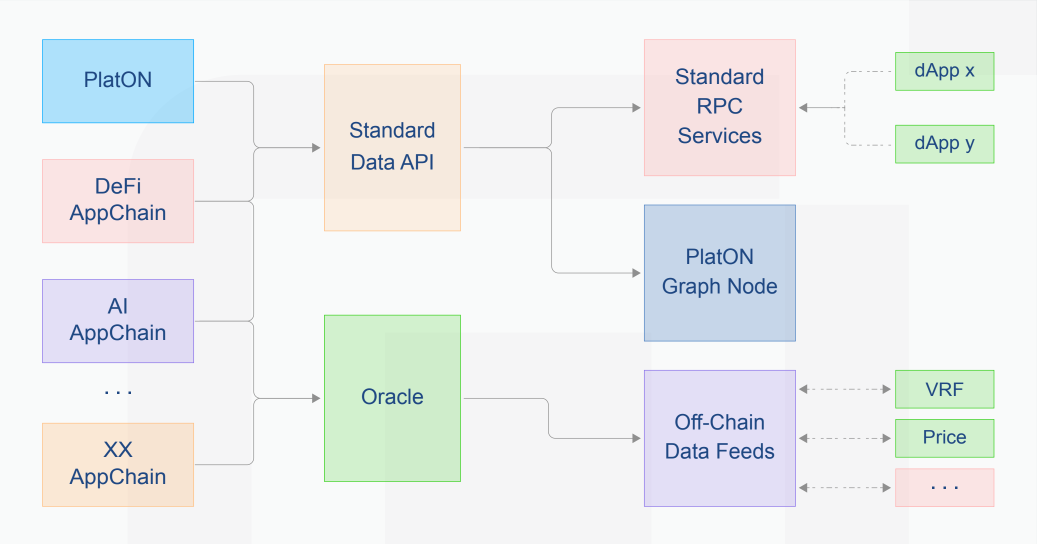


Figure 11 PlatON Application Chain Public API

Unified RPC Service

After successful registration in PlatON's Registry, each application chain will automatically use standardized API interfaces to retrieve on-chain data based on the application chain ID and its default endpoint. This data will then be transformed into Ethereum's RPC standardized interfaces. Application chains can also develop their own RPC based on their specific situations. For most users, they don't need to worry about the differences between different Appchains. They can easily use the unified RPC service simply by using the application chain's ID.

Data Indexing Service

Upon successful registration of an application chain, the application chain framework will activate the corresponding application chain ID in the PlatON Graph Node. This allows for the indexing of data related to the application chain. Developers only need to deploy the application subgraph to the PlatON Graph Node to easily access and store the data of interest to users.

Off-Chain Data Service

As more applications require off-chain data, the flexible off-chain Data Feeds mechanism allows developers to use off-chain data in development without worrying about security and implementation. PlatON's Oracle oracle service supports various common off-chain data Feeds, such as verifiable random numbers (VRF), token prices, etc. In addition to this, developers can also customize other off-chain data of interest based on standard interfaces.

4.5 Privacy Computation Service

PlatON's Datum privacy computing platform offers a range of solutions for data privacy protection and data asset monetization, enabling high-performance web3 services for data asset issuance. It employs cryptographic techniques such as secure multi-party computation, zero-knowledge proofs, homomorphic encryption, and proxy re-encryption to perform privacy computations on data. Additionally, leveraging PlatON's blockchain infrastructure, it facilitates data asset ownership verification, authorization, computation scheduling, automatic settlement, and regulatory auditing, thereby creating a decentralized trading system for data, models, and computing power.

Datum offers a diverse range of service APIs and SDKs, allowing users to selectively choose relevant services to meet their needs. These services encompass data transmission and custody, data based NFT issuance, data asset management and trading, trusted sharing, and multi-party data joint query computations. It provides a variety of privacy-enhancing technologies to ensure comprehensive privacy protection in data applications. By using Datum, users can effortlessly channel data into the application chain.

Datum provides five major service capabilities across various stages of data circulation.

Secure Data On-chain Service

Datum offers data in the form of APIs and SDKs to be stored on decentralized platforms such as IPFS and Arweave, as well as cloud storage solutions like AWS, Azure, and GCP, enabling the flow of data into the Web3 world. This lays the foundation for subsequent data asset applications by securely transferring data onto the blockchain.

Data Assetization Service

Datum offers data asset issuance services in the form of APIs and SDKs, supporting various NFT contract templates. It provides a quick way to publish, view, and configure attributes for different applications' needs.

Secure Data Trading Service

Datum provides data asset trading services through APIs and SDKs, including services for authorized access, access authentication, download, and data consistency verification. By attaching verifiable credentials to Data NFTs and leveraging proxy re-encryption algorithms, it enables functionalities such as data access authorization, secure data sharing, and ownership transfer.

Data Oracle Service

Datum offers Data Oracle services in the form of APIs and SDKs to provide web3-style entrance for existing web2 data services and data models, allowing off-chain data to be used in on-chain contract calls. It provides various service components to enable users to quickly access off-chain data for use in on-chain Dapps.

Secure Data Computation Service

Datum provides two-party and multi-party data joint query, analysis, or computation services through APIs and SDKs. It leverages privacy-enhancing technologies such as PSI, secure multi-party computation, and homomorphic encryption to offer capabilities like privacy data matching, privacy data queries, privacy datat statistical analysis, and privacy AI.

5 / Use Cases and Case Studies

An increasing number of well-known applications have either started or are preparing to use application chains to host their services. In this section, we will delve into the domains that are most suitable for building application chains.

5.1 AI Large Model Application Chain

With the emergence of models like ChatGPT, the era of rapidly evolving AI large models has arrived, and their applications are continuously being realized. However, the ecosystem for large models is still in its early stages and faces challenges such as funding difficulties, homogenous competition, lack of production resources, and closed ecosystems.

PlatON-AppChain aims to support the development of AI by creating dedicated and customized controllable AI application chains. This will facilitate the implementation of large model applications, foster the creation of large model application chains, and establish a decentralized market to enhance AI and democratize its access. Every individual should have access to and ownership of large models, and both developers and users should be able to contribute algorithms and data to LLM (Large Language Model) models and share in their future profits.

- The concept of a large model ecosystem incubator is proposed. A complete AI industry ecosystem includes underlying infrastructure, large models, prompt engineering platforms, and end applications. An AI application chain built around large models can utilize tokens to help incubate the entire AI industry ecosystem, promoting the commercial implementation of large models.

- Decentralized DAO Governance. The current successful large models are often developed by major tech companies, closed-source, and lack transparency. They are typically managed by a closed group of stakeholders who decide on the model's features and maintenance. In the context of a large model application chain, the large models are fully open and can be managed by a DAO (Decentralized Autonomous Organization) consisting of governments, businesses, and relevant opinion leaders/experts. This DAO would coordinate the development and maintenance of the models. The platform's native token would be used to build a governance framework and voting rights, along with economic incentives.

- Decentralized GPU Computing Network. The rise of AI large models has led to a significant demand for high-performance GPUs like Nvidia A100. However, these resources are concentrated in a few large companies or cloud providers. There's an urgent need for an affordable on-demand serverless computing platform for training purposes. Built on the PlatON application chain, a decentralized GPU computing network can be established. This allows individuals and organizations to rent out their unused GPU resources to meet the needs of AI researchers and developers.

- Decentralized Data Annotation Crowdsourcing Marketplace. From the perspective of AI data annotation, an application chain can establish a decentralized crowdsourcing platform where users can earn rewards by completing data annotation tasks. This approach aims to significantly reduce the cost of annotating AI datasets. Data workers (e.g., model data annotation, data quality assessment) can participate in model building through the decentralized data infrastructure and receive peer-to-peer rewards.

- Decentralized AI SaaS (Software as a Service) Offering. In contrast to traditional large model APIs that require licensing, the large model APIs within the large model application chain are open and license-free. These APIs can be hosted and deployed within the application chain, accessible and usable by anyone. Leveraging the decentralized computing network of the application chain, it provides deployment and hosting services for large models. These models are registered in the application chain's smart contracts, accessible for searching and calling by paying users. Payments for AI large model services can be settled using tokens.

5.2 GameFi Application Chain

GameFi gaming is entering a new era, requiring a more open economic ecosystem and fairer game incentives. Transparent platforms for trading game assets are also needed. The GameFi economy is offering a new standard for game developers, empowering them with more control and building an economic system around in-game commodities that will bring more people into the digital world.

An increasing number of individuals are realizing the significance of building blockchain-based games on application chains. This recognition is driven not only by the fact that high-performance application chains provide players with excellent user interaction experiences, but also because the independent economic structure, high level of control, and ultra-low transaction costs of application chains align well with the requirements of blockchain games. In addition, PlatON-AppChain can contribute to the development of GameFi in the following ways:

- Cross-Network Game Marketplace: Game developers and players desire games to run on cost-effective and fast networks while also wishing to sell items on highly liquid networks. Leveraging PlatON-Bridge, game developers can transform a game from a single platform to a multi-platform experience. Players can engage in games using their wallets on any network. Additionally, virtual in-game items can be traded across different networks, increasing their liquidity and enhancing playability.

- Game Development Kit: Building a game from scratch is not an easy task for developers. PlatON-AppChain offers a development kit with low latency and high-performance AppChain nodes. Developers can target specific game components for development and upgrade individual parts without needing to update the entire game. This enhances composability in game development and reduces costs as on-chain storage fees are lower, saving users on interaction costs. The cross-platform wallet provides a game entry point for various users, seamlessly integrating with the DeFi ecosystem without concerns about user traffic.Unified Developer Dashboard: Developers can access detailed user and game analytics data as well as payment systems through a unified developer panel. This offers valuable insights and management tools to enhance the gaming experience.

5.3 DeFi Application Chain

With the vigorous growth of DeFi projects, every DeFi protocol seeks expansion, and the trend of DeFi protocols embracing AppChains is becoming an inevitable course. Firstly, AppChains can empower DeFi with sovereignty. DeFi protocols can attain decentralization through AppChains, thereby freeing themselves from the operational differences of Layer 1 (L1) and mitigating the potential impact of L1 on DeFi operations. Secondly, AppChains can open doors to enhanced interoperability, offering a broader range of possibilities in this realm.

PlatON-AppChain utilizes PlatON-Bridge to assist in the expansion of DeFi protocols. By directly establishing fund flow between chains, it ensures efficient delivery and facilitates wider adoption of DeFi. Most notably, PlatON-AppChain offers various decentralized consensus protocols to avoid the potential regulatory labeling of DeFi projects as securities due to centralized protocols (such as centralized orderers), providing added protection to DeFi initiatives.

- RWA (Real World Assets) applications involve the transformation of tangible or intangible assets into digital tokens, followed by the mapping of their ownership and equivalent value onto the blockchain for trading. This process aims to introduce real-world assets into the realm of DeFi, thereby enhancing liquidity. Given that the scale of RWA significantly surpasses that of native crypto assets, constructing customizable application chains through PlatON-AppChain offers the potential to bring liquidity from global markets of RWA such as bonds, real estate, and gold into DeFi. Undoubtedly, this initiative has the potential to substantially amplify the scope of the DeFi market.

- DEX applications. In contrast to centralized exchanges that require KYC verification, decentralized exchanges (DEX) align better with the concept of decentralization, which is a significant factor contributing to their popularity. PlatON-AppChain can bring new value propositions to Dex from three perspectives:

- A.The decentralized nature of PlatON-AppChain can eliminate moral hazards associated with market makers.
- B.Open-source code and protocols facilitate regulatory scrutiny.
- C.Application chains support various complex trading patterns, including high-frequency trading, thereby greatly reducing transaction costs.

5.4 DePIN Application Chain

Due to the substantial capital requirements and logistical challenges of traditional tangible infrastructures such as telecommunications networks, cloud services, mobile networks, and power grids, their deployment and management have traditionally been dominated by large enterprises. These companies have nearly formed a monopoly over end-users in terms of pricing, rules, and services, resulting in a lack of competition and innovation mechanisms within the industry, until the emergence of blockchain and Web3.The integration of real-world assets into the Internet of Things (IoT) is known as MachineFi. As token incentives play an increasingly pivotal role in the rational allocation and circulation of these real-world assets (RWA), the industry combines token-incentivized physical infrastructure networks (TIPIN) with the concept of Proof of Physical Work (PoPW) technology, leading to the creation of Decentralized Physical Infrastructure Networks (DePIN). DePIN is a blockchain-based network that leverages token incentives to generate value from physical infrastructures, marking a new frontier in blockchain technology. It fulfills the desire to map RWAs into the Web3 and is regarded as one of the most authentic applications on the blockchain. DePIN can play a crucial role in promoting fair and efficient allocation of real-world resources.

Utilizing the PlatON-AppChain network to build a decentralized hardware resource market can attract more available hardware infrastructure resources to the WEB3 network through economic incentives. PoPW technology enables effective mapping of various offline assets such as storage, sensors, integrated circuits, and data onto the blockchain to provide services, establishing a decentralized distribution network for physical assets. Leveraging PlatON-Bridge allows these physical resources and data to flow across networks, providing high-quality hardware resources and data to various projects while also increasing user benefits. This approach effectively facilitates the distribution and division of resources such as computing power, storage, and data services in the network, offering a new way to build and operate real-world infrastructures. This method is fairer, more efficient, and aligned with the interests of network participants, and is expected to foster the emergence of more high-quality products.

6 / Application Chain Ecosystem Roadmap

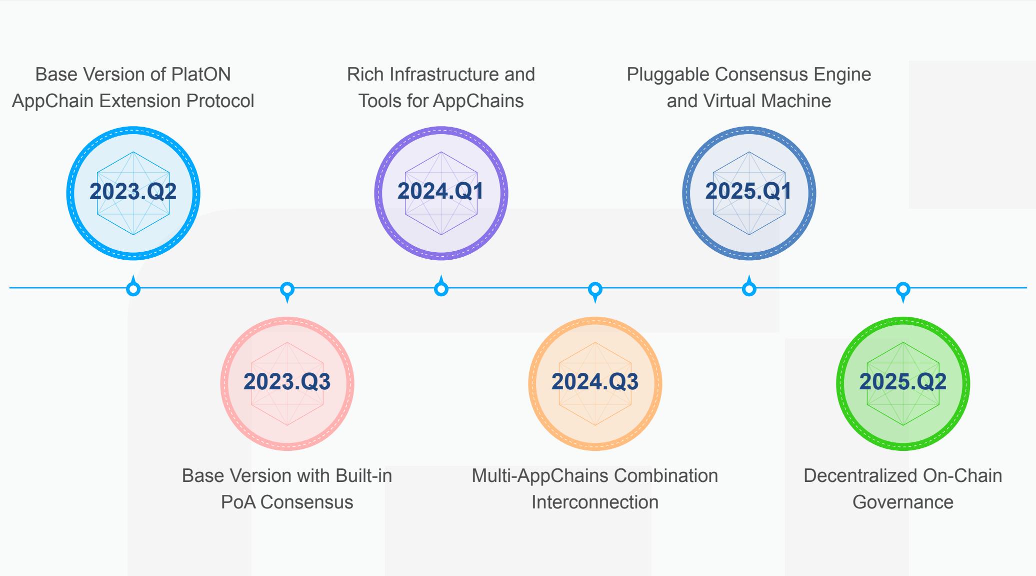


Figure 12 PlatON Application Chain Development Roadmap

2023 Q2

The foundational application chain expansion protocol has been successfully completed, encompassing application chain governance, node staking, and the implementation of the Checkpoint mechanism. The underlying components of the application chain, including the Giskard consensus mechanism, EVM virtual machine, economic model, on-chain governance, as well as complementary tools like browsers and SDKs, have all been finalized. Additionally, a test network for the application chain has been established and is operational.

2023 Q3

Inherent implementation of the Proof of Authority (PoA) consensus mechanism, suitable for a wide range of application scenarios. Further supporting infrastructure features have been provided, including a comprehensive wallet named ATON, a browser, and a development toolkit SDK. The application chain become capable of achieving interoperability with the main chain and other application chains through existing asset cross-chain bridges.

2024 Q1

Further expansion of complementary infrastructure, including unified RPC services,data indexing services, Oracle services, and foundational wallet services.

2024 Q3

Implementation of PlatON-Bridge's message cross-chain bridge, enabling all application chains on PlatON to directly manage and configure cross-chain rules for any messages between chains at the business level, achieving multi-chain interconnection and interoperability.

2025 Q1

Support for plug-and-play consensus mechanisms and virtual machines. In addition to allowing developers to create consensus protocols and virtual machines more aligned with their specific applications through standard interfaces, options will also include optimized consensus mechanisms based on Giskard and a WASM virtual machine.

2025 Q2

Introduction of customizable on-chain governance functionality, providing robust protocol-layer support for flexible self-customization of governance for application chains.