White Paper on Secure and Compliant Web 3.0 Infrastructure

We would like to recognize the following contributors to the document (listed in alphabetical order):

Revision number	Description	Contributor	Date
Version 0.1	Initial release	Prof. James Lei, HKUST Ivan.xmr, HardenedVault KSTP.eth, HardenedVault	Sep 19 2023

		Shawn Chang, HardenedVault Weihua Du, HardenedLinux Laifa Fang, ASTRI Yang Liu, Metopia Xiaoyi Wang, Hangzhou High-Tech Zone (Binjiang) Blockchain and Data Security Research Institute Thomas Zhu, Head of Digital Assets Think Tank of FinTech Centre of HK PolyU Faculty of Business Terry Lam, HISUN	

1. Introduction

This whitepaper aims to provide guidelines and best practices for building a secure, compliant, and scalable infrastructure for the Web 3.0 ecosystem. It will provide a comprehensive and meticulous overview of several critical aspects of Web 3.0. It includes detailed explanations of key technologies associated with Web 3.0, explores the design of the Web 3.0 protocol stack specifically in the context of Hong Kong, discusses the considerations and measures taken regarding security and regulation, and delves into the integration of emerging information technologies within the Web 3.0 ecosystem.

1.1 Characteristics and Values of Web 3.0

The transition from Web 1.0 to Web 2.0, and now to Web 3.0, signifies the progressive evolution of Internet ideals. Web 1.0 revolved around the concept of providing information services to consumers, while Web 2.0 shifted its focus towards facilitating connections between laborers and consumers. Web 3.0, on the other hand, embraces a revolutionary vision centered on trustlessness, decentralization, and the digitization of assets. It represents the next generation of the Internet, with blockchain technology as its fundamental building block, and digital production and consumption as its primary economic drivers. Noteworthy characteristics of Web 3.0 include the utilization of distributed ledger technology to reconstruct the underlying logic of Web 2.0 applications, harnessing the potential of blockchain for trusted collaboration, distributed execution, data protection, and asset transfer. This integration of information flow, business processes, and value streams aims to replace existing Internet services with more standardized and streamlined on-chain smart contracts, liberating us from the reliance on centralized institutions.

Web 3.0 encompasses two core values: asset digitization and decentralization. From the perspective of asset digitization, Web 3.0 emphasizes the efficient circulation of value, asserting that digital rights within the digital space can flow seamlessly. It envisions a future where the internet becomes a vibrant ecosystem where individuals can create, share, and obtain value in various forms. Digital assets, such as cryptocurrencies, non-fungible tokens (NFTs), and decentralized finance (DeFi) instruments, play a central role in this vision, enabling frictionless transactions, ownership verification, and new opportunities for economic participation.

From the decentralization standpoint, Web 3.0 advocates for a paradigm shift in the structure of internet services. It emphasizes collaborative development and aims to dismantle the traditional intermediaries by fostering an open, participatory environment. Web 3.0 envisions a world where users have greater control over their data, identities, and online interactions. It promotes the use of decentralized technologies, such as blockchain and peer-to-peer networks, to enable trustless interactions, transparent governance, and censorship-resistant platforms.

Web3 also highlights the importance of interoperability and open standards. It envisions a web where different applications can seamlessly interact and share data, enabling innovative

combinations and integrations. This interoperability fosters a rich ecosystem of interconnected services, empowering users with a more personalized and seamless experience across various platforms and applications.

1.2 Key Technologies of Web 3.0

There are some key technologies that collectively establish the foundation and capabilities of Web 3.0, driving the implementation of decentralization, user autonomy, and privacy protection features. They empower users with increased autonomy and participation while advancing the development of the digital economy and society.

1. Decentralized Infrastructure Architecture
    - Blockchain Technology: Blockchain stands as a foundational technology of Web 3.0, a distributed and decentralized ledger system that ensures data consistency and security through consensus algorithms. It eliminates single points of failure and centralized control.
    - Peer-to-Peer Network: Web 3.0 infrastructure adopts a peer-to-peer network structure, enabling direct communication and interaction among participants without the need for centralized servers or intermediaries.
    - Distributed storage: divide data into smaller chunks and distribute these chunks across different nodes in the network. Each node holds a portion of the data and also has the capability to read and store data. This approach brings several advantages: high availability, fault tolerance, scalability and data privacy and security.

2. Token Economy and Digital Assets:
    - Token Economy: Central to Web 3.0, the token economy incentivizes user engagement and contribution by issuing digital assets (tokens) representing value. These tokens can serve as currencies, equity, commodities, and more, facilitating value exchange and governance.
    - Digital Assets: Digital assets are digitized forms of real world assets (RWA) or virtual assets represented on the blockchain. They encompass cryptocurrencies, digital artwork, in-game items, and other assets. Blockchain technology ensures accurate recording and verification of asset ownership and transaction history.

3. Decentralized Finance (DeFi):
    - Smart Contracts: Smart contracts are self-executing agreements on the blockchain, incorporating predefined rules and conditions. DeFi leverages smart contracts to build decentralized financial applications such as lending platforms, decentralized exchanges (DEXs), and liquidity protocols. This allows participants to engage in financial transactions without relying on trusted intermediaries.

- Decentralized Exchanges: Decentralized exchanges (DEXs) utilize smart contracts and blockchain technology to enable peer-to-peer trading between users, eliminating the need for traditional intermediaries. This enhances transaction security and empowers users with greater control over their funds.

4. Privacy Protection Technologies:
    - Encryption Algorithms: Encryption algorithms safeguard the privacy of user data and transactions. They ensure that data is encrypted during transmission and storage, and decryption is only possible with the corresponding keys.
    - Zero-Knowledge Proofs: Zero-knowledge proofs enable one party (the prover) to prove the authenticity of a statement to another party (the verifier) without revealing specific information. This technology allows for anonymity and privacy protection while ensuring the validity of transactions.
    - Selective Disclosure: Selective disclosure techniques empower users to protect their privacy while selectively sharing specific data or information with entities requiring access. This strikes a balance between privacy and the need for sharing.

5. Service Governance:
    - Decentralized Governance: Web 3.0 emphasizes community participation and consensus-driven decision-making, employing a decentralized governance model. Network protocols and rules are established through community voting, proposals, and consensus mechanisms, rather than being dictated by centralized authorities.
    - Governance Tokens: Governance tokens grant holders the ability to participate in network governance decisions. Token holders can vote, propose changes, or engage in other decision-making processes based on their token holdings, influencing the network's development and operations.

6. Metaverse Applications:
    - Virtual Reality (VR) and Augmented Reality (AR): VR and AR technologies enable users to engage in immersive interactions and experiences within virtual worlds. Users can explore, interact with, and create virtual environments and objects through these technologies.
    - Blockchain and Smart Contracts: The combination of blockchain and smart contract technologies provides a secure, transparent, and programmable foundation for metaverse applications. Blockchain ensures true ownership and transaction history of digital assets within the virtual world. Smart contracts enable the automated execution of objects and interactions in the virtual environment based on predefined rules and conditions.

1.3 Web 3.0 and Digital Economy

The digital economy refers to the broad range of economic activities conducted through digital technologies and platforms. The core concept of Web 3.0 is to build a new internet infrastructure based on decentralization, encryption, and smart contracts using blockchain and other distributed technologies. This infrastructure provides a more secure, transparent, and trustworthy environment for the digital economy.

The characteristics of Web 3.0, such as decentralized identity verification, execution of smart contracts, transparency, and traceability of blockchain, provide a better framework and tools for various economic activities within the digital economy. It disrupts existing centralized economic models and creates more opportunities and rights protection for users, creators, investors, and service providers.

Through the technologies of Web 3.0, areas such as digital currencies, decentralized finance, smart contracts, and digital asset trading have experienced rapid development, providing the infrastructure and innovative mechanisms for the thriving digital economy. Therefore, it can be said that Web 3.0 is one of the cornerstones that support and drive the development of the digital economy.

1. Financial Inclusion and Global Participation: The infrastructure and technologies of Web 3.0 can transcend geographical and institutional barriers, providing more opportunities for global participation in the digital economy. Through decentralized finance (DeFi) applications, individuals with internet access can engage in financial activities such as lending, investing, and fundraising. This financial inclusion helps reduce financial barriers and offers more opportunities for economic participants worldwide.
2. Decentralized Digital Identity: Web 3.0 advocates for decentralized identity verification and digital identity management systems, which provide a more secure and privacy-protecting means of authentication in the digital economy. By utilizing encryption technology and distributed identity systems, individuals can have better control over their identity information without relying on centralized identity verification authorities. This decentralized digital identity system helps mitigate the risks of identity theft and fraud, fostering the development of the digital economy.
3. Decentralized Content Creation and Knowledge Sharing: Web 3.0 offers creators and intellectual property holders more opportunities and rights protection. Using blockchain and smart contract technologies, creators can directly publish and sell digital content without depending on traditional intermediaries. Encryption ensures the authenticity and copyright ownership of the content, while smart contracts ensure fair compensation for creators. This decentralized model of content creation and knowledge sharing disrupts traditional copyright protection and content distribution methods, bringing forth new business models and opportunities in the digital economy.

4. Transparency and Traceability through Blockchain: Web 3.0 utilizes blockchain technology to enhance transparency and traceability, fostering a more equitable and trustworthy digital economy. Transactions and data recorded on the blockchain can be audited and verified, ensuring the credibility and compliance of transactions. This transparency helps mitigate fraudulent activities and improper operations, bolstering trust in the digital economy and providing better means of regulation for governing bodies.
5. Community-Driven Economic Ecosystem: Web 3.0 emphasizes community participation and collective governance, encouraging users to actively engage in the development and decision-making processes of the digital economic ecosystem. Community members can influence the direction of the digital economy through voting, suggesting ideas, and contributing code. This community-driven economic ecosystem better caters to user needs, promotes innovation and collaboration, and enhances the adaptive capacity of the digital economy.

Web 3.0 as a digital ecosystem encompasses the interconnected networks, platforms, and communities that facilitate and support these economic activities. The digital ecosystem includes various stakeholders such as users, developers, service providers, and regulators, and it focuses not only on economic transactions but also on the interactions, relationships, and dependencies among these stakeholders. The concept of a digital ecosystem recognizes the holistic and interconnected nature of the digital economy, highlighting the importance of collaboration, governance, and symbiotic relationships among its participants.

2. Overall Web 3.0 Architecture

The Web 3.0 Hong Kong Protocol Stack provides standardized interfaces and specifications based on distributed blockchain storage and computing technology architecture. It can be used to implement functionalities such as data element rights management and value accounting. It includes key technologies such as distributed storage infrastructure, Web3HK public chain, MaaS (Management as a Service), MinD (Mind as a Service), and integrates multiple technologies into a unified standard. Through systematic integration, the Web 3.0 Hong Kong Protocol Stack offers comprehensive Web 3.0 technologies and applications within Hong Kong, the Greater Bay Area, and even globally, providing robust support for building digital ecosystems.

The Web 3.0 Hong Kong Protocol Stack takes into consideration factors such as security, usability, and economic efficiency. Its goal is to provide infrastructure for the digital transformation and technological innovation of various industries through innovative distributed blockchain storage and computing technology architecture. This will empower the digital transformation and technological innovation across industries, driving the development and innovation of the future Internet.

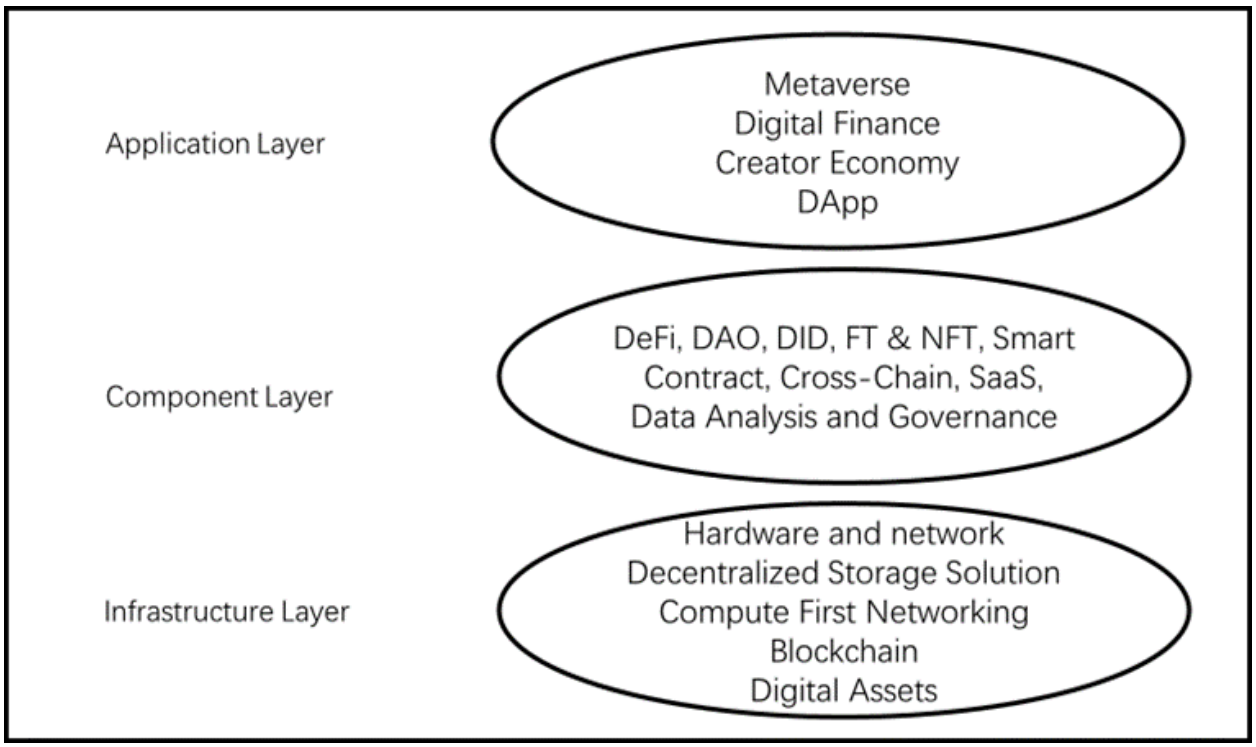


Figure 1. Web 3.0 Hong Kong Protocol Framework

Web 3.0 represents a new paradigm for the internet, characterized by decentralization, user empowerment, and enhanced privacy. As shown in figure 1, its architecture consists of three key layers: the Infrastructure Layer, the Component Layer, and the Application Layer.

At the foundation is the Infrastructure Layer, which comprises the underlying technologies that enable Web 3.0 to function. This layer includes distributed ledger technologies and related hardwares, particularly blockchain, which provide decentralized and immutable record-keeping. Blockchain facilitates secure and transparent transactions, smart contracts, and the interoperability of various blockchain networks through cross-chain capabilities.

Built upon the Infrastructure Layer is the Component Layer, which encompasses the fundamental building blocks of Web 3.0. Smart contracts automate agreements and transactions, eliminating the need for intermediaries. Decentralized Finance (DeFi) leverages blockchain and cryptocurrency to create alternative financial systems that are transparent, accessible, and inclusive. Decentralized Autonomous Organizations (DAOs) enable decentralized decision-making and governance, providing a framework for community-driven organizations. Self-sovereign identity (DID) empowers individuals with control over their digital identities and data. Digital asset representation includes fungible tokens (FTs) and non-fungible tokens (NFTs), enabling ownership and transfer of unique digital assets. Supporting technologies like SaaS (Software as a Service) provide cloud-based solutions for Web 3.0 functionalities. Data analysis and governance ensure proper management, security, and insights from data within the Web 3.0 ecosystem.

The Application Layer, the topmost layer, showcases the practical implementations and use cases of Web 3.0. It encompasses various applications that leverage the underlying technologies and components of Web 3.0. The Metaverse offers immersive virtual experiences and environments where users can interact and engage with digital content. Digital Finance applications revolutionize traditional financial systems by providing decentralized financial services, removing intermediaries, and enabling greater control over personal finances. The Creator Economy empowers content creators, artists, and entrepreneurs to monetize their digital creations directly, leveraging NFTs and decentralized platforms. Decentralized Applications (DApps) are built on blockchain networks, offering secure, transparent, and user-centric alternatives to traditional centralized applications across industries such as finance, gaming, supply chain, and social media.

In summary, Web 3.0 architecture is a transformative framework that moves beyond the limitations of Web 2.0, fostering decentralization, user empowerment, and new possibilities for finance, governance, identity, asset representation, and applications. The Infrastructure Layer provides the underlying technology, the Component Layer offers the foundational building blocks, and the Application Layer showcases the practical implementations, collectively shaping the future of the internet.

More details are illustrated in the following sections.

2.1 Infrastructure Layer

The Infrastructure Layer of Web 3.0 in Hong Kong comprises various components that collectively support the decentralized and distributed nature of the next generation of the internet. This layer encompasses hardware and network infrastructure, decentralized storage solutions, compute-first networking, blockchain technology, and digital assets.

The hardware and network infrastructure forms the backbone of Web 3.0 in Hong Kong. It includes high-performance servers, data centers, networking equipment, and connectivity solutions. These components are designed to provide reliable and scalable infrastructure to support the decentralized applications (dApps) and services built on Web 3.0. Robust network connectivity ensures fast and seamless data transfer between nodes, enabling efficient communication and collaboration within the decentralized ecosystem.

Decentralized storage solutions play a crucial role in Web 3.0 infrastructure. These solutions leverage distributed storage networks to store and retrieve data in a decentralized manner. Unlike traditional centralized storage systems, decentralized storage solutions offer improved data integrity, censorship resistance, and fault tolerance. Users can store and access data securely across a network of nodes, eliminating single points of failure and enhancing data privacy.

Compute-first networking is a key aspect of Web 3.0 infrastructure in Hong Kong. It focuses on distributing computational resources across nodes in the network, enabling decentralized processing and execution of tasks. By leveraging technologies like edge computing and peer-to-peer networking, compute-first networking minimizes reliance on centralized servers and enhances the scalability and responsiveness of Web 3.0 applications. It enables efficient resource allocation and utilization, ensuring that computational tasks are performed closer to the data source, reducing latency and improving overall performance.

Blockchain technology forms a foundational element of Web 3.0 infrastructure in Hong Kong. Blockchain networks, such as Ethereum or other scalable and interoperable blockchains, provide the underlying framework for decentralized applications and digital asset management. They enable secure and transparent transactions, immutability of data, and decentralized consensus mechanisms. Blockchain technology ensures the integrity and trustworthiness of Web 3.0 infrastructure, facilitating secure data sharing, smart contract execution, and the creation, transfer, and management of digital assets. Based on the techniques proposed, the Web3 Hong Kong public chain will be illustrated.

Digital assets are an integral part of Web 3.0 infrastructure in Hong Kong. These assets can include cryptocurrencies, non-fungible tokens (NFTs), digital collectibles, or other tokenized representations of real-world or virtual assets. Web 3.0 enables seamless creation, ownership, and exchange of digital assets through blockchain technology. These assets can be traded, stored, and managed with greater transparency and security, leveraging decentralized finance (DeFi) protocols, decentralized exchanges (DEXs), and other emerging platforms. We focus on Wallet and Stablecoins in the illustrations later.

Overall, the infrastructure layer of Web 3.0 in Hong Kong encompasses hardware and network infrastructure, decentralized storage solutions, compute-first networking, blockchain technology, and digital assets. This infrastructure forms the foundation for the decentralized and distributed nature of Web 3.0, enabling secure, scalable, and transparent applications and services that empower users and promote a more inclusive and open digital ecosystem.

2.1.1 Hardware and Network

Hardware and network include Hybrid Cloud Servers, POS, IoT, and STB Box.

2.1.1.1 Hybrid Cloud Servers

Hybrid Cloud Servers includes cloud servers, IDC servers and community servers.

A Concepts

Hybrid Cloud refers to the mixed use of data and applications between private cloud and public cloud. It provides a convenient way for organizations to choose to use public or private cloud services according to their needs, while ensuring the security and reliability of data and applications.

B Markets

1. In China, the government has been promoting the development of domestic cloud services, and many domestic companies, such as Alibaba Cloud and Tencent Cloud, have made significant progress in building cloud infrastructure and providing hybrid cloud solutions. These companies have built large-scale data centers and established partnerships with many enterprises to provide customers with secure and reliable cloud services.

2. In other countries, the situation is similar to that of China, where many leading cloud service providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, offer hybrid cloud solutions. These providers have also invested heavily in establishing data centers worldwide and have formed partnerships with numerous enterprises to assist customers in migrating their workloads to the cloud.

3. Overall, the trend of hybrid cloud is becoming increasingly prevalent, with more and more enterprises seeking to leverage the advantages of both public and private cloud models. This has led to intensified competition among cloud service providers, who continuously innovate to offer customers more advanced and reliable hybrid cloud solutions.

C Targets

The main purpose of writing the Hybrid Cloud protocol is to unify the underlying hardware support and access methods.

D Protocols

Cloud Severs

The hybrid cloud model combines the benefits of both public and private clouds, providing organizations with scalability, flexibility, and control over their data and applications. In the context of Web 3.0 standard development, the hybrid cloud plays a vital role in enabling decentralized applications (dApps) and services. This protocol stack outlines the various layers and components required to build a robust and secure cloud server infrastructure within the hybrid cloud environment.

Protocol Stack Layers:

1. User Layer:

- Web Servers: Software components that handle Web 3.0 requests and responses, serving web pages and RESTful APIs to clients.

2. Service Layer:

- Load Balancing: Distributes incoming traffic across multiple cloud servers to improve performance, scalability, and fault tolerance.

- Container Orchestration: Manages the deployment, scaling, and lifecycle of containerized applications, ensuring efficient resource utilization.

- Service Discovery: Enables cloud servers to discover and communicate with each other efficiently within the hybrid cloud infrastructure.

- API Gateway: Provides a single entry point for accessing multiple services and handles tasks such as authentication, rate limiting, and request routing.

3. Machine Layer:

- Virtual Machines (VMs): Isolated and virtualized environments that run operating systems and applications on physical servers.

- Containerization: Enables the packaging and isolation of applications and their dependencies for efficient deployment and management.

- Resource Orchestration: Automates the provisioning and management of cloud resources, including VMs, storage, and networking.

- Network Virtualization: Abstracts and virtualizes networking infrastructure to provide secure and isolated network environments.

- Security and Compliance: Enforces security measures, authentication, access controls, and compliance policies to protect data and applications.

4. Cloud Storage Layer:

- Object Storage: Scalable and durable storage for unstructured data, accessible via APIs, suitable for storing large amounts of data.

- Block Storage: Provides persistent and high-performance storage for virtual machines and applications, with features like snapshots and replication.

- File Storage: Shared and distributed file systems for applications that require file-based access and sharing.

5. Connectivity Layer:

- Hybrid Cloud Connectivity: Establishes secure and reliable network connections between on-premises infrastructure and public cloud resources.

- Virtual Private Networks (VPNs): Encrypted tunnels for secure communication between cloud servers and remote clients or networks.

- Content Delivery Network (CDN): Caches and delivers content globally, reducing latency and improving performance for distributed users.

IDC Servers

IDC (Internet Data Center) servers play a critical role in providing centralized infrastructure and services within the hybrid cloud environment. In the context of Web 3.0 standard development, IDC servers serve as key components for hosting centralized applications, managing data, and facilitating connectivity. This protocol stack outlines the layers and components necessary to build a robust and efficient IDC server infrastructure.

Protocol Stack Layers:

1. User Layer:

- Web Servers: Software components that handle Web 3.0 requests and responses, serving web pages and APIs to clients.

2. Service Layer:

- Load Balancing: Distributes incoming traffic across multiple IDC servers to enhance performance, scalability, and fault tolerance.

- Service Discovery: Enables IDC servers to discover and communicate with each other efficiently within the hybrid cloud environment.

- API Gateway: Provides a unified entry point for accessing multiple services and handles tasks such as authentication, rate limiting, and request routing.

3. Machine Layer:

- Physical Servers: Hardware-based servers that serve as the foundation for hosting applications and managing data within the IDC.

- Virtualization: Abstracts and partitions physical resources to create virtual machines (VMs) for efficient resource utilization.

- Resource Orchestration: Automates the provisioning and management of IDC resources, including servers, storage, and networking.

- Network Infrastructure: Establishes a reliable and high-performance network for connecting IDC servers and facilitating data transfer.

- Security and Compliance: Implements robust security measures, including firewalls, access controls, and compliance policies, to protect data and applications.

4. Storage Layer:

- Block Storage: Provides persistent and high-performance storage for IDC servers, supporting features such as snapshots and replication.

- Network-Attached Storage (NAS): Shared and distributed file systems for applications that require file-based access and sharing.

- Backup and Disaster Recovery: Implements mechanisms for data backup, replication, and disaster recovery to ensure data resilience and availability.

5. Connectivity Layer:

- Internet Connectivity: Establishes connectivity between the IDC servers and the internet, enabling access to external resources and users.

- Virtual Private Network (VPN): Securely connects IDC servers to remote networks or clients via encrypted tunnels.

- Content Delivery Network (CDN): Caches and delivers content globally, reducing latency and improving performance for distributed users.

Community Servers

Community servers play a crucial role in facilitating collaboration, communication, and interaction within online communities in the Web 3.0 era. These servers provide a platform for users to engage, share information, and participate in decentralized social networks and community-driven applications. This protocol stack outlines the layers and components required to build a robust and inclusive community server infrastructure within the hybrid cloud environment.

Protocol Stack Layers:

1. User Layer:

- Web Servers: Software components that handle Web 3.0 requests and responses, serving web pages and APIs to specific community needs, such as forums, chat platforms, or collaborative tools.

2. Service Layer:

- Identity and Access Management: Manages user identities, authentication, and access control mechanisms to ensure secure and trusted community interactions.

- Real-time Communication: Provides real-time messaging and chat capabilities, enabling instant communication and collaboration among community members.

- Content Management: Facilitates the creation, organization, and retrieval of community-generated content, including posts, articles, media files, and discussions.

- Moderation and Governance: Implements mechanisms for community moderation, content curation, and the enforcement of community guidelines and policies.

3. Machine Layer:

- Server Clustering: Utilizes multiple servers to distribute community-related workloads, improve scalability, and ensure high availability.

- Scalable Databases: Stores community data, user profiles, and metadata in scalable and distributed databases for efficient retrieval and management.

- Resource Allocation and Management: Orchestrates resources such as computing power, storage, and network bandwidth to meet the demands of the community server infrastructure.

- Security and Privacy: Implements robust security measures, encryption protocols, and privacy controls to protect user data and ensure compliance with data protection regulations.

4. Storage Layer:

- Object Storage: Provides scalable and distributed storage for community-generated content, ensuring efficient access and retrieval.

- Distributed File Systems: Enables shared and decentralized file storage, facilitating collaboration and content sharing within the community.

- Content Versioning and Backup: Implements mechanisms for content versioning, revision control, and regular backups to ensure data integrity and disaster recovery.

5. Connectivity Layer:

- Community APIs: Exposes APIs and integration points for community developers to build third-party applications, extend functionality, and integrate with external services.

- WebRTC (Web Real-Time Communication): Enables peer-to-peer communication and media streaming within the community, facilitating video calls, voice chats, and live streaming.

- Web Sockets: Provides real-time, bidirectional communication channels between community servers and client applications, supporting instant updates and notifications.

2.1.1.2 POS

A Concepts

POS (Point of Sale) is a cash register system that consolidates various information such as sales receipts, customer data, and product purchase data within a store into a single system. It is a system that encompasses functions such as inventory management, product sales, customer management, and customer purchase data management. With POS, businesses can quickly access product information, provide customer purchase records, streamline their sales processes, and enhance overall operational efficiency.

B Markets

The POS market is witnessing significant growth. According to statistics, the global POS market reached $25 billion in 2018 and is projected to reach $40.6 billion by 2026, with a growth rate exceeding 12.10%. Several factors will influence the POS market, including technological advancements, market segmentation, and government policies. It is anticipated that POS technology will continue to improve in the future, offering higher cost-effectiveness, which will attract a larger consumer base.

C Targets

The main purpose of protocol development is to identify the various protocols supported by the POS system.

D Protocols

EMV

EMV (Europay, MasterCard, Visa) is a globally standardized POS payment protocol that enables POS systems to securely process credit card payments.

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards for POS systems designed to ensure the security and protection of data within POS systems.

ISO 8583

International standard for financial transaction messaging, developed by the International Organization for Standardization (ISO), primarily used for bank card transaction processing.

Quick Response (QR) Code

A two-dimensional barcode technology used for quickly retrieving information, commonly used for payments in POS environments.

Electronic Cash Register (ECR)

An electronic cash handling system commonly used in POS environments for processing cash transactions.

Magnetic Stripe Technology (MST)

A technology commonly used to store bank card information and used in POS transactions.

Radio Frequency Identification (RFID)

A technology used for wireless transmission of product information for fast transaction processing.

Apple Pay

Apple Pay is a POS payment system introduced by Apple Inc., allowing consumers to make POS payments using Apple devices.

Android Pay

Android Pay is a POS payment system launched by Google, enabling consumers to make POS payments using Android devices.

2.1.1.3 IoT

A Concepts

The Internet of Things (IoT) is a network technology that connects physical and virtual objects to the Internet, enabling them to communicate, share data, and information. It also facilitates the collection and transmission of data, enabling automated control and the automatic completion of specified tasks.

B Markets

The IoT market is experiencing rapid growth, with the global IoT market projected to reach $1,050 billion by 2025. Among them, smart homes, smart IoT, smart logistics, and smart manufacturing are the most popular application areas in the IoT industry.

C Targets

The primary purpose of protocol development is to establish the protocols specific to the IoT domain including smart IoT, supply chain management and asset tracking.

D Protocols

Smart IoT

Connecting various devices to enable automated control and data transmission.

The Internet of Things (IoT) enables the interconnection of physical devices, sensors, and actuators, creating a network of smart objects that can collect and exchange data. In order to enable automatic control and efficient data transmission within smart IoT systems, a robust protocol stack is required. This protocol stack outlines the layers and components necessary to achieve seamless control and data transmission in smart IoT environments.

Protocol Stack Layers:

1. Device Layer:

- IoT Devices: Physical devices equipped with sensors, actuators, and communication capabilities that collect data and interact with the environment.

- Sensor and Actuator Control: Enables the control and management of sensors and actuators, including configuration, calibration, and real-time control.

2. Network Layer:

- IoT Communication Protocols: Lightweight and efficient protocols designed for IoT devices, such as MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol).

- Wireless Connectivity: Utilizes wireless technologies, including Wi-Fi, Bluetooth, Zigbee, or LoRaWAN, to establish connectivity between IoT devices and gateways.

3. Gateway Layer:

- IoT Gateway: Acts as a bridge between IoT devices and the cloud or central control system, aggregating data, performing protocol translation, and managing device connectivity.

- Protocol Translation: Converts data between different IoT protocols, ensuring interoperability between devices and various communication standards.

4. Control Layer:

- Data Processing and Analytics: Performs real-time or batch processing of IoT data to extract valuable insights, detect anomalies, and trigger automatic control actions.

- Rule Engine and Decision Making: Implements rule-based engines and decision-making algorithms to automate control actions based on predefined rules or machine learning models.

- Remote Device Management: Enables remote management, configuration, and firmware updates of IoT devices, ensuring their optimal performance and security.

Supply Chain Management

Tracking and monitoring the supply chain to achieve real-time tracking and supervision.

Supply chain management involves the coordination and integration of activities across the entire supply chain, from procurement to production, distribution, and customer service. To ensure effective collaboration, transparency, and efficiency within supply chains, a robust protocol stack is essential. This protocol stack outlines the layers and components required to facilitate seamless data exchange, process automation, and visibility in supply chain management.

Protocol Stack Layers:

1. Data Layer:

- Data Standards: Establishes common data formats and standards, such as GS1 (Global Standards One), to ensure consistency and interoperability across supply chain participants.

- Data Capture and Integration: Involves capturing data from various sources, including RFID tags, barcodes, sensors, and enterprise systems, and integrating them into a centralized data repository.

- Data Validation and Verification: Performs data validation and verification checks to ensure accuracy, completeness, and consistency of supply chain data.

2. Communication Layer:

- Application Programming Interfaces (APIs): Defines interfaces and protocols for seamless communication between different supply chain participants, enabling data exchange and process integration.

- Electronic Data Interchange (EDI): Facilitates the standard exchange of business documents, such as purchase orders, invoices, and shipping notices, between trading partners.

- Web Services: Enables real-time communication and integration between systems through web-based protocols, such as SOAP (Simple Object Access Protocol) or REST (Representational State Transfer).

3. Process Automation Layer:

- Workflow Management: Automates and streamlines supply chain processes, including order fulfillment, inventory management, demand planning, and transportation scheduling.

- Business Process Management (BPM): Defines, models, and orchestrates end-to-end supply chain processes, ensuring efficient collaboration and cross-functional coordination.

- Rules Engine: Implements rule-based engines to automate decision-making, exception handling, and business rule enforcement within the supply chain.

4. Visibility and Tracking Layer:

- Track and Trace: Enables real-time tracking and visibility of goods and assets throughout the supply chain using technologies like RFID, GPS, or blockchain.

- Event Management: Monitors and captures supply chain events, such as order status updates, shipment delays, or inventory levels, to provide stakeholders with timely and accurate information.

- Analytics and Reporting: Applies data analytics techniques to derive meaningful insights from supply chain data, enabling performance measurement, predictive analysis, and optimization.

5. Compliance Layer:

- Secure Data Exchange: Implements encryption, digital signatures, and secure communication protocols to protect sensitive supply chain data from unauthorized access or tampering.

- Authentication and Authorization: Establishes mechanisms for verifying the identity of supply chain participants and controlling access to critical systems and data.

- Regulatory Compliance: Ensures adherence to industry-specific regulations and standards, such as FDA regulations for pharmaceutical supply chains or customs regulations for international trade.

Asset Tracking

Tracking the location and status of assets, as well as interactions between devices.

Asset tracking involves monitoring and managing the location, condition, and movement of assets within an organization. Whether it's equipment, inventory, or vehicles, a robust protocol stack is essential to enable effective asset tracking. This protocol stack outlines the layers and components required to facilitate seamless tracking, real-time visibility, and efficient management of assets.

Protocol Stack Layers:

1. Hardware Layer:

- Asset Tags: Utilizes various tracking technologies, such as RFID tags, barcode labels, GPS trackers, or sensors, to attach to assets and capture relevant data.

- Scanners and Readers: Includes handheld scanners, stationary readers, or mobile devices equipped with scanning capabilities to capture asset identification and location information.

- Communication Devices: Enables asset communication, either through cellular networks, Wi-Fi, or low-power wireless technologies like Bluetooth or Zigbee.

2. Network Layer:

- Wireless Connectivity: Utilizes wireless technologies to establish connectivity between asset tracking devices, such as RFID readers or GPS trackers, and the infrastructure.

- Local Area Network (LAN) or Wide Area Network (WAN): Provides network connectivity for asset tracking devices to transmit data to centralized management systems.

- Internet Connectivity: Enables remote access and real-time data transmission for asset tracking systems through the internet.

3. Middleware Layer:

- Data Integration: Collects and consolidates asset data from various tracking devices and sensors, normalizing and transforming it into a standardized format for further processing.

- Data Filtering and Processing: Filters and processes asset data to extract relevant information, such as location updates, condition monitoring, or event triggers.

- Event Management: Detects and handles predefined events or anomalies, such as asset theft, maintenance alerts, or asset utilization thresholds.

4. User Layer:

- Asset Management System: Provides a centralized platform to monitor and manage assets, including asset registration, tracking, allocation, maintenance scheduling, and reporting.

- Real-time Tracking and Visualization: Offers real-time tracking capabilities and visual representation of asset locations on maps or floor plans.

- Notifications and Alerts: Sends notifications and alerts to relevant stakeholders based on predefined rules, such as asset movement outside designated areas or maintenance due dates.

- Analytics and Reporting: Provides data analytics and reporting functionalities to derive valuable insights from asset tracking data, such as utilization patterns, maintenance trends, or asset performance metrics.

5. Integration Layer:

- Access Control: Ensures secure access to asset tracking systems and data, implementing authentication, authorization, and encryption mechanisms.

- Integration with Existing Systems: Integrates with other enterprise systems, such as inventory management, supply chain, or enterprise resource planning (ERP) systems, to synchronize asset data and streamline processes.

- Data Privacy and Compliance: Adheres to data privacy regulations and compliance requirements when handling sensitive asset information, ensuring data protection and confidentiality.

2.1.1.4 STB Boxes

A Concepts

STB boxes (Set-Top Boxes) are hardware devices used to support blockchain applications, such as cryptocurrency transactions, decentralized applications (dApps), and accessing distributed ledgers. In addition, they provide users with a secure and reliable means to access distributed applications in web3, making it easier to participate in the blockchain ecosystem.

B Markets

Indeed, the market for STB boxes is experiencing rapid growth. Currently, there are over 150 brands offering such services in the market, and the sales volume continues to increase annually. Moreover, with the rapid development of blockchain technology, the market prospects for STB boxes are highly promising.

C Targets

The primary purpose of protocol development is to establish the protocols specific to STB boxes.

D Protocols

Set-Top Box (STB) boxes play a crucial role in delivering multimedia content, such as television broadcasts, video-on-demand, and interactive services, to consumers' televisions. To ensure seamless content delivery, interactive features, and compatibility with various service providers, a robust protocol stack is required. This protocol stack outlines the layers and components necessary to enable efficient communication and functionality within STB boxes.

Protocol Stack Layers:

1. Physical Layer:

- Hardware Interfaces: Includes various physical interfaces, such as HDMI, component video, Ethernet, USB, or RF, to connect the STB box to the television, network, and other peripherals.

- Signal Encoding: Utilizes encoding schemes, such as MPEG-2, MPEG-4, or H.265 (HEVC), to compress and transmit audio and video signals efficiently.

- Remote Control: Facilitates communication between the user and the STB box, enabling navigation, channel selection, and control of interactive features.

2. Transport Layer:

- Internet Protocol (IP) Connectivity: Enables IP-based communication between the STB box and service providers' networks, allowing for the delivery of streaming media, interactive applications, and software updates.

- Digital Video Broadcasting (DVB): Defines the standards for delivering digital television and interactive services over broadcast networks, including DVB-S/S2 (satellite), DVB-T/T2 (terrestrial), or DVB-C (cable).

- Conditional Access System (CAS): Ensures secure access to encrypted content, implementing encryption algorithms, smart card integration, and key management.

3. Middleware Layer:

- User Interface (UI) Framework: Provides a graphical user interface (GUI) for users to navigate through channels, access menus, and interact with interactive services.

- Electronic Program Guide (EPG): Presents a user-friendly interface for browsing and selecting television programs, displaying program schedules, descriptions, and reminders.

- Interactive Services: Enables the delivery of interactive applications, such as video-on-demand, catch-up TV, gaming, or social media integration.

- Content Protection: Implements Digital Rights Management (DRM) solutions to protect copyrighted content, preventing unauthorized copying or distribution.

4. User Layer:

- Media Player: Supports audio and video playback, including various file formats, codecs, and streaming protocols.

- Streaming Protocols: Implements streaming protocols such as HTTP Live Streaming (HLS), Dynamic Adaptive Streaming over HTTP (DASH), or Real-Time Streaming Protocol (RTSP) to deliver streaming media content.

- Application Development Framework: Provides tools, APIs, and libraries for developers to create and deploy custom applications on the STB box, enhancing functionality and user experience.

- Interactive Advertising: Supports targeted advertising and personalized promotions, integrating advertising platforms and enabling interactive ad experiences.

5. Network Layer:

- IP Networking: Implements IP-based networking protocols, such as TCP/IP or UDP/IP, to enable communication with the service provider's backend systems, content servers, and other networked devices.

- Quality of Service (QoS): Ensures reliable and high-quality content delivery by implementing QoS mechanisms, prioritizing real-time video and audio streams.

- Network Management: Facilitates remote management and monitoring of STB boxes, including software updates, diagnostics, and performance optimization.

2.1.2 Decentralized Storage Solution

A Concepts

Decentralized storage systems leverage distributed networks of nodes to store and retrieve data, offering enhanced security, privacy, and resilience compared to centralized storage solutions. To enable efficient data storage, retrieval, and coordination within decentralized storage, a robust protocol stack is essential. This protocol stack outlines the layers and components necessary to facilitate seamless communication and functionality within decentralized storage systems.

The focus of our proposal in the protocol are Maas and MinD. Other distributed method such as IPFS may be also considered.

MaaS (Mesh as a Service): It refers to connecting points in a network to form a mesh-like network structure, serving as a service. This network architecture allows for greater flexibility in adapting to user needs and easier scalability.

MinD (Mesh insiDe): It is a protocol that enables communication between different networks. It uses edge servers to store and transmit data, addressing across networks to ensure continuous data transmission.

This protocol is based on the decentralized domain name resolution system in the blockchain Web3 industry, similar to ENS. Unlike ICANN, this protocol achieves data storage and computation by arranging server devices in valuable regions. These devices can resolve domain names, provide content, and charge Gas fees that are returned to users or partner merchants. Users can access the system using addresses like "mass://mind33762/peter/HKUST/NT/HK". It automatically resolves to a local server, which performs addressing and corresponds to a server IP, thereby locating the content stored at Peter's address in the Technology University. This resolves the issue of fixed IP and resembles P2P. The address content is similar to a postal code used to indicate country, city, region, and other information.

B Markets

The decentralized domain name market already has protocols like ENS, but the MaaS and MinD protocols provide a new solution. Our solution is based on edge node storage, where these nodes can be utilized as servers, each capable of offering stable storage and computing capacity. This approach is more flexible, catering to a wider range of needs, and exhibits significant performance advantages.

By leveraging edge nodes as storage and computing resources, our solution ensures data availability and reduces reliance on centralized infrastructure. This distributed architecture enhances resilience, scalability, and responsiveness. Additionally, the ability to utilize edge nodes as servers allows for efficient content delivery and faster response times, leading to improved user experiences.

The MaaS and MinD protocols introduce a novel approach to decentralized domain name resolution, leveraging edge node storage and computation. This innovative solution offers enhanced flexibility and notable performance advantages, setting it apart from existing protocols in the decentralized domain name market.

C Targets

The primary purpose of protocol development is to establish the protocols specific to decentralized storage solutions with MaaS and MinD.

D Protocols

The protocol stack for decentralized storage provides a comprehensive framework for efficient and secure data storage, retrieval, and coordination within distributed networks. By leveraging this protocol stack, decentralized storage systems can offer enhanced privacy, security, and resilience compared to centralized storage solutions. This contributes to data ownership, censorship resistance, and the empowerment of users in the digital age.

Protocol Stack Layers:

1. Network Layer:

- Peer Discovery: Enables nodes within the decentralized storage network to discover and establish connections with each other, facilitating node coordination and communication.

- Routing and Addressing: Defines protocols and mechanisms for routing data across the decentralized network, ensuring efficient data transfer between nodes. For example, The MaaS protocol resolves requests by parsing domain names in a format similar to postal codes. This directs the user's request to local storage and computing servers, corresponding to the server's IP address. The server provides resolution services and charges a gas fee, which is later returned to the user or partner merchants as an incentive. The address resolution is achieved through a peer-to-peer (p2p) process involving servers located in all Metopia residential communities. The addressing protocol resolves the issue of fixed IP addresses by utilizing distributed storage and computing hardware devices in a manner similar to P2P.

- Domain Name Format: The MaaS domain name format follows a structure resembling "mass://mind33762/peter/HKUST/NT/HK", where the content functions like a postal code and can identify country, city, and region information.

- Network Security: Implements cryptographic protocols, such as encryption and digital signatures, to ensure data privacy, integrity, and secure communication between nodes.

2. Storage Layer:

- Data Chunking and Distribution: Breaks data into smaller chunks and distributes them across multiple nodes within the decentralized storage network, improving scalability and fault tolerance.

- Replication and Redundancy: Implements mechanisms for data replication across multiple nodes, ensuring data availability and resilience against node failures or network disruptions.

- Data Integrity and Verification: Utilizes cryptographic algorithms, such as hashes or Merkle trees, to verify the integrity of stored data and detect any tampering or corruption.

3. Consensus Layer:

- Consensus Algorithms: Implements consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), to ensure agreement and coordination among nodes regarding data storage, retrieval, and access control.

- Incentive Mechanisms: Introduces economic incentives, such as token rewards or micropayments, to motivate nodes to contribute storage space, bandwidth, and computational resources to the decentralized storage network.

4. Rule Layer:

- Data Access and Retrieval Protocols: Defines protocols, such as InterPlanetary File System (IPFS), Filecoin, or Storj, for accessing and retrieving data stored in the decentralized storage network.

- API and Interface Standards: Establishes standardized application programming interfaces (APIs) and interfaces to facilitate seamless integration of decentralized storage into applications and services.

- Smart Contracts: Enables the creation and execution of smart contracts, which define rules and conditions for data storage, retrieval, and access within the decentralized storage network.

- Communication Fee Charging: When users interact with the system, such as conducting transactions, querying information, or performing system domain name resolution, the system charges a certain amount of MMD as a gas fee. The gas fee calculation takes into account factors such as the complexity of the operation and the size of data transmission, and it is collected in MMD. Users must confirm and pay the corresponding amount of MMD to complete the operation. Users can use the provided wallet to make MMD payments or pre-deposit MMD into other wallets for paying the gas fee. The system periodically updates gas fee prices based on market conditions. Approximate pricing: The price of MMD fluctuates depending on the market. Generally, the gas fee required for each operation is relatively small, typically ranging from a few MMD to a few tens of MMD. The corresponding price is approximately between 0.1 HKD to 1 HKD. The specific prices are dynamically adjusted based on market conditions to ensure fair and reasonable charges.

- Location-Based DID/DDNS: DID, which stands for Decentralized Identifier, is a distributed identity protocol primarily used for decentralized identity verification in Web3 environments. DDNS, which stands for Dynamic Domain Name System, is a protocol for managing dynamic IP addresses and their corresponding domain names.

5. User Layer:

- Data Encryption and Access Control: Implements encryption algorithms and access control mechanisms to protect the privacy and security of stored data, ensuring that only authorized users can access and modify data.

- Data Management and Search: Offers functionalities for organizing, searching, and managing data within the decentralized storage network, enabling efficient data retrieval and discovery.

2.1.3 Compute First Networking

A Concepts

The next-generation Computing First Network (CFN) connects discrete computing power. Compute nodes produce computing power as networks connect it. In addition, an intelligent CFN brain centrally perceives, orchestrates, and schedules computing power on the network.

Here are some of the properties of CFN compared to other networks:

Decentralization: CFN is a decentralized network, meaning that there is no central authority that controls the network. This makes CFN more resistant to censorship and data manipulation.

Security: CFN is a secure network, thanks to its use of strong encryption and authentication protocols. This makes CFN a good choice for storing and sharing sensitive data.

Scalability: CFN is a scalable network, meaning that it can handle a large number of users and transactions. This makes CFN a good choice for applications that need to process a lot of data.

Efficiency: CFN is an efficient network, meaning that it can process transactions quickly and with low fees. This makes CFN a good choice for applications that need to process a lot of transactions.

Interoperability: CFN is an interoperable network, meaning that it can connect to other networks and systems. This makes CFN a good choice for applications that need to interact with other systems.

B Markets

The market for CFN is growing rapidly, as more and more businesses and individuals are looking for ways to reduce their computing costs. CFN provides a cost-effective way to access computing resources, and it is also a more secure way to share data than traditional methods.

As of 2023, there are over 10,000 active nodes on the CFN network. The majority of these nodes are located in the United States, Europe, and Asia. The network is growing rapidly, with new nodes being added every day.

The market for CFN is also growing rapidly. In 2022, the market for CFN was estimated to be worth $1 billion. This number is expected to grow to $5 billion by 2025.

The growth of the CFN market is being driven by a number of factors, including the increasing cost of traditional computing resources, the need for more secure ways to share data, and the growing popularity of cloud computing.

C Targets

The main purpose of protocol development is to identify the technique aspects considered for CFN system.

D Protocols

Physical Layer

The physical layer is responsible for the physical transmission of data over a network. This includes the physical media (e.g., copper wire, fiber optic cable, wireless spectrum), as well as the protocols that govern how data is transmitted and received.

For CFN, the physical layer could be based on a variety of technologies, such as Ethernet, Wi-Fi, or Bluetooth.

Data Link Layer

The data link layer is responsible for ensuring that data is transmitted and received correctly between two nodes on a network. This includes error detection and correction, as well as flow control.

For CFN, the data link layer could be based on a variety of protocols, such as Ethernet, PPP, or HDLC.

Network Layer

The network layer is responsible for routing data between nodes on a network. This includes determining the best path for data to take, as well as managing congestion.

For CFN, the network layer could be based on a variety of protocols, such as IP, IPX, or BGP.

Transport Layer

The transport layer is responsible for ensuring that data is delivered reliably between two nodes on a network. This includes error detection and correction, as well as flow control.

For CFN, the transport layer could be based on a variety of protocols, such as TCP, UDP, or SCTP.

User Layer

The User layer is responsible for providing specific services to users, such as web browsing, email, or file sharing.

For CFN, the application layer could be based on a variety of protocols, such as HTTP, SMTP, or FTP.

Security Layer

The security layer is responsible for ensuring the security of data transmitted over a network. This includes encryption, authentication, and authorization.

For CFN, the security layer could be based on a variety of protocols, such as SSL/TLS, IPSec, or Kerberos.

2.1.4 Blockchain

This section focuses on general description of blockchain. The details of Web3HK Public Chain design for Web 3.0 Hong Kong system will be seen in Section 3.

A Concepts

Blockchain is a decentralized digital ledger that records and verifies transactions across multiple computers or nodes. It operates on the principle of transparency, security, and immutability. Unlike traditional centralized systems, where a single authority controls the ledger, blockchain distributes the ledger among various participants, creating a shared network. Each transaction is bundled into a block and added to a chain of blocks in a chronological order, forming a permanent and unchangeable record. The key features of blockchain include cryptographic validation, consensus mechanisms, and decentralized governance. This technology provides trust and eliminates the need for intermediaries by ensuring that all participants have access to the same information, making it highly resistant to fraud and tampering. Blockchain has applications beyond cryptocurrencies, such as supply chain management, healthcare, finance, and more, where transparency, security, and accountability are crucial.

B Markets

Currently, the market for blockchain technology exhibited significant growth and adoption across various industries. According to a report by Market Research Future, the global blockchain market was valued at $3.0 billion in 2020 and was projected to reach $39.7 billion by 2025, with a compound annual growth rate (CAGR) of 67.3% during the forecast period. The financial sector remained a key driver of blockchain adoption, with banking institutions and financial service providers exploring use cases for improving efficiency, security, and transparency. In terms of geographical distribution, North America held the largest market share, followed by Europe and Asia-Pacific. The market witnessed increased investment and funding in blockchain startups and projects, with venture capital funding reaching $4.1 billion in 2020. Despite challenges such as regulatory uncertainty and scalability concerns, the market for blockchain technology continued to expand, driven by the potential for transformative applications and the growing recognition of blockchain's benefits in various industries.

C Targets

This section aims to provide protocols design details regarding a public blockchain.

D Protocols

The general protocol design for a public chain involves several key components and considerations.

Consensus Mechanism

The consensus mechanism determines how agreement is reached among network participants on the validity and order of transactions. Popular consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). The choice of consensus mechanism impacts factors such as security, scalability, and energy efficiency.

Block Structure

Blocks are containers that group transactions together and form the blockchain. The block structure defines the format, size, and contents of each block. It includes fields for a block header, transaction data, timestamps, and references to the previous block.

Transaction Validation

Public chains employ rules and algorithms to validate the authenticity and integrity of transactions. This includes verifying digital signatures, checking for double spending, enforcing smart contract conditions, and ensuring compliance with network rules.

P2P Network

Public chains rely on a peer-to-peer (P2P) network for communication and data propagation. The protocol includes mechanisms for node discovery, message broadcasting, peer connectivity, and data synchronization across the network.

Governance and Upgrades

Public chains often include mechanisms for decentralized governance, allowing stakeholders to participate in decision-making processes, such as protocol upgrades, parameter changes, and network improvements. This may involve voting systems, on-chain governance, or off-chain governance models.

Security and Cryptography

Public chains employ cryptographic techniques to secure transactions, protect user identities, and prevent unauthorized access. This includes cryptographic hashing, digital signatures, public-private key encryption, and secure key management.

Scalability and Performance

Addressing scalability challenges is crucial for public chains as they aim to handle a large number of transactions and support a growing user base. Different techniques, such as

sharding, sidechains, state channels, and layer 2 solutions, can be incorporated into the protocol design to improve scalability and performance.

2.1.5 Digital Assets

Digital assets are digital entities that can be traded, held, and transferred across different blockchain networks. These elements can include cryptocurrencies, securities, real estate properties, intellectual property, commodities, and other tangible or intangible assets. The ownership and transaction records of these assets are recorded on the blockchain, enabling transparent and decentralized management and public trading. Digital assets possess high liquidity, security, and programmability, making them highly versatile in areas such as the digital economy, finance, and social governance. They represent an important application scenario for blockchain technology.

This section include Wallet and Stable Coins.

Wallet

A Concepts

Wallets are typically tools used to store digital assets and manage digital asset transactions. These wallets commonly utilize cryptographic techniques with public-private key pairs to protect users' digital assets and record transactions on blockchain networks. Users can utilize the private keys of their wallets to sign transactions and verify the ownership of assets.

B Markets

The global blockchain wallet market is currently in a rapid growth phase, with an estimated market size of around $15 billion USD, projected to reach $41 billion USD by 2023. The presence of dominant players is also evident, with the top 5 cryptocurrency wallets on Android devices (Trust, Metamask, Crypto.com, imToken, and BitPay) having a combined installation base of over 20 million, far exceeding the wallets ranked lower in popularity.

C Targets

The main purpose of writing a wallet protocol is to establish the specifications and standards for the format of wallets.

D Protocols

Wallet Standard: The structure and functionality of wallets.

A wallet standard defines the specifications for the design and functionality of digital wallets. It includes elements such as user interfaces, security features, key management systems, and storage protocols. The standard ensures that wallets provide a consistent and user-friendly experience across different platforms and applications. It may specify features like balance

tracking, transaction history, address management, backup and recovery options, and integration with other services, such as decentralized exchanges or token swaps.

1. Address Standard: The structure and functionality of addresses.

An address standard outlines the format and rules for generating and using addresses within a public chain. It defines the structure of addresses, which typically consist of a combination of alphanumeric characters. The standard may specify the algorithm or cryptographic functions used to generate addresses from public keys. It ensures that addresses are unique, easily recognizable, and compatible with the chosen blockchain protocol. Address standards also cover address validation, error detection, and methods for securely sharing addresses for transactions or fund transfers.

2. Account Management Standard: Methods for managing account rights, such as deposits, withdrawals, transfers, investments, etc.

An account management standard provides guidelines for managing various account operations within a public chain. It defines the procedures and protocols for depositing funds into an account, initiating withdrawals, transferring balances between accounts, and managing investments or holdings. The standard may include security measures for authentication, access control, and account recovery. It ensures consistent and secure account management practices across different applications or services built on the public chain.

3. Asset Form Standard: Definition of asset forms within a wallet, such as cryptocurrencies and encrypted assets.

An asset form standard specifies the types of assets that can be stored and managed within a wallet on a public chain. It covers various forms of digital assets, including cryptocurrencies, tokens, non-fungible tokens (NFTs), and encrypted assets. The standard defines the protocols and formats for representing and storing these assets within the wallet, including token standards (e.g., ERC-20, ERC-721), metadata standards, and interoperability guidelines. It ensures compatibility and seamless integration of different asset forms across wallets and platforms.

4. Transaction and Confirmation Standard: Methods for conducting transactions and confirming them.

A transaction and confirmation standard outlines the procedures and protocols for initiating, processing, and confirming transactions on a public chain. It defines the structure of transactions, including the sender's address, recipient's address, transaction amount, and any additional data or metadata. The standard includes guidelines for transaction validation, consensus mechanisms, and confirmation processes. It ensures that transactions are executed accurately, securely, and with appropriate confirmation times, maintaining the integrity and consistency of the public chain's transaction history.

5. Multi-Signature Standard: Methods for implementing multi-signature functionality.

A multi-signature standard describes the protocols and mechanisms for implementing multi-signature functionality within a public chain. It defines how multiple parties can jointly control and authorize transactions by requiring multiple signatures. The standard specifies the structure of multi-signature addresses, the number of required signatures, and the process for validating and executing multi-signature transactions. It ensures enhanced security, decentralization, and trust for transactions involving multiple participants on the public chain.

6. Payment Protocol: A protocol used to guide payments.

A payment protocol is a set of rules and procedures that govern the process of making payments within a public chain. It defines the communication protocols, data formats, and transaction flow between the sender and receiver during a payment transaction. The protocol may include elements like payment request generation, invoice formatting, address verification, transaction fee estimation, and error handling. It ensures standardized and efficient payment interactions, simplifying the payment process for users and enabling interoperability among different wallets and applications.

7. Protocol Payment URL Standard: Definition of the URL format for payments.

A protocol payment URL standard specifies the format and structure of URLs used for initiating payment requests within a public chain. It defines the parameters, syntax, and data elements included in the URL to facilitate seamless payment initiation and processing. The standard may include information such as the recipient's address, payment amount, asset type, and optional metadata. By following the standard, wallets and applications can generate and interpret payment URLs consistently, allowing users to easily initiate payments by clicking on or scanning a payment URL.

8. Smart Contract Standard: The format and functionality of smart contracts.

A smart contract standard outlines the format, structure, and functionality of smart contracts within a public chain. It defines the programming language, data structures, and protocols for creating, executing, and interacting with smart contracts. The standard may specify elements such as contract creation, function definitions, event handling, data storage, and contract upgrading. It ensures that smart contracts are interoperable, reusable, and compatible across different platforms and applications, facilitating automated and trustless execution of contractual agreements on the public chain.

Stable Coins

A Concepts

MMD is a blockchain-based points system similar to various commercial loyalty programs, where points can be exchanged for goods or services and used in specific stores or markets. MMD can be used as a means of payment for goods or services and can also be utilized to pay

transaction fees. The transactions and transfers of MMD can be tracked and confirmed on the blockchain, ensuring transparency and security.

Stablecoins, on the other hand, are a type of cryptocurrency that offers relatively stable prices compared to other digital currencies. They are typically backed by fiat currencies or other assets as collateral or endorsement. The purpose of stablecoins is to overcome the price volatility associated with other cryptocurrencies, making them more suitable as payment instruments or stores of value.

B Markets

The blockchain asset market continues to thrive due to the security and trustworthiness provided by blockchain technology. This has sparked increasing interest among investors, who are now more actively involved in the blockchain asset market than ever before. Currently, digital assets are highly favored by investors, and trading volumes continue to rise. As blockchain technology continues to evolve, the digital asset market will present even more investment opportunities.

The market capitalization and trading volume of stablecoins have experienced rapid growth in recent years, attracting the attention of numerous investors and businesses. This growth has also facilitated the widespread adoption of digital assets. Stablecoins can be used in various areas such as cryptocurrency trading, international remittances, payments, insurance, lending, and deposits, making them an integral part of digital economic development.

C Targets

The purpose of this writing is to specify the detailed information regarding the Assets (MMD/Stablecoins) protocol stack of the Web 3.0 Hong Kong protocol stack.

D Protocols

MMD

1. Non-Fungible Token (NFT) Protocol: Used for distributing unique and non-replaceable digital assets.

The Non-Fungible Token (NFT) protocol is a set of rules and standards governing the creation, ownership, and transfer of unique digital assets on a public chain. It defines the structure and functionality of NFTs, which are distinct and indivisible tokens that represent ownership or proof of authenticity for digital assets like artwork, collectibles, or virtual real estate. The protocol specifies how NFTs are minted, stored, and transferred, ensuring that each NFT is unique and non-replaceable. It may include standards for metadata, royalties, provenance, and interoperability, enabling seamless distribution and trading of NFTs across different platforms and marketplaces.

2. Anti-Mistake Asset Transfer Protocol: Designed to prevent accidental sending of assets.

The Anti-Mistake Asset Transfer Protocol is a protocol designed to mitigate the risk of accidental asset transfers within a public chain. It introduces additional security measures and confirmation mechanisms to prevent users from mistakenly sending assets to the wrong addresses or unintended recipients. The protocol may include features such as address verification, transaction confirmation prompts, and transaction reversal mechanisms. By implementing this protocol, users are provided with safeguards against unintended asset transfers, reducing the likelihood of irreversible mistakes and enhancing the overall security of asset management within the public chain.

3. Protocol for Supporting Flexible Asset Transfers and Permission Control: Enables flexible transfer of assets and provides control over permissions.

The Protocol for Supporting Flexible Asset Transfers and Permission Control is a set of guidelines and mechanisms that enable users to transfer assets with flexibility while maintaining control over permissions. This protocol allows users to define and manage granular permissions for asset transfers, specifying conditions and restrictions that must be met for a transfer to occur. It provides a framework for setting up rules such as time-based restrictions, approval workflows, multi-factor authentication, or specific recipient criteria. By adhering to this protocol, users have the ability to customize and enforce asset transfer rules according to their specific needs, enhancing security, and control over asset transactions within the public chain.

Stablecoins

1. Protocol for Supporting Stablecoin Digital Asset Transactions: Enables transactions involving stablecoin digital assets.

The Protocol for Supporting Stablecoin Digital Asset Transactions establishes a standardized framework for conducting transactions involving stablecoin digital assets within a public chain. It defines the protocols, data formats, and transaction flow specific to stablecoins, which are cryptocurrencies designed to maintain a stable value relative to a reference asset like a fiat currency. This protocol ensures seamless interoperability and compatibility among different stablecoin implementations, enabling users to securely and efficiently transact with stablecoins on the public chain.

2. Unified Interface for Asset Mobility and Management Protocol: Provides a standardized interface for the movement and management of assets.

The Unified Interface for Asset Mobility and Management Protocol introduces a standardized interface that facilitates the movement and management of assets, including stablecoins, within a public chain ecosystem. This protocol defines a common set of methods, data structures, and communication protocols for asset transfers, balance inquiries, account management, and other asset-related operations. By adhering to this protocol, wallets, exchanges, and other applications can provide a unified and consistent user experience for asset mobility and management, simplifying asset transfers and enhancing overall usability.

3. Protocol for Supporting Voting, Incentives, and Smart Contract Management: Facilitates voting, incentivization, and management of smart contracts.

The Protocol for Supporting Voting, Incentives, and Smart Contract Management establishes guidelines and mechanisms for supporting voting, incentivization, and management functionalities related to stablecoins and associated smart contracts within a public chain. This protocol outlines the procedures, data structures, and decision-making processes for voting on governance proposals, distributing incentives or rewards, and managing smart contract upgrades or modifications. By implementing this protocol, stablecoin ecosystems can foster community participation, transparent governance, and efficient management of stablecoin-related operations.

4. Protocol for Flexible Asset Transfer and Permission Control: Allows for flexible transfer of assets and provides mechanisms for permission control.

The Protocol for Flexible Asset Transfer and Permission Control enables flexible and customizable asset transfers while incorporating mechanisms for permission control within stablecoin ecosystems. This protocol allows users to define and enforce specific rules and conditions for asset transfers, such as transaction limits, approval workflows, time-based restrictions, or multi-factor authentication requirements. It ensures that asset transfers occur within predefined parameters, enhancing security and control over stablecoin transactions while accommodating various use cases and compliance requirements.

5. Protocol for Supporting Multiple Digital Currencies: Supports various protocols for different digital currencies.

The Protocol for Supporting Multiple Digital Currencies is designed to facilitate the integration and interoperability of different digital currencies, including stablecoins, within a public chain ecosystem. This protocol allows for the coexistence of multiple digital currency standards, such as ERC-20, BEP-20, or other custom protocols. It establishes guidelines for asset representation, token standards, cross-chain compatibility, and data interoperability. By adhering to this protocol, stablecoin ecosystems can support a diverse range of digital currencies, providing users with flexibility and choice while maintaining seamless interoperability across different blockchain networks and platforms.

2.2 Component Layer

The Component Layer for Web 3.0 encompasses various technologies and concepts that are driving the evolution of the internet towards a more decentralized, user-centric, and efficient ecosystem. Within this layer, several key components are propelling this transformation.

At the core of Web 3.0 are fundamental blockchain technologies that underpin its functionality. Smart contracts serve as self-executing contracts, automating transactions and enforcing agreements without intermediaries. Cross-chain technology enables interoperability between different blockchain networks, facilitating seamless communication and asset transfers.

Decentralized Finance (DeFi) is a prominent component of Web 3.0, leveraging blockchain and cryptocurrency to recreate traditional financial systems in a decentralized manner. DeFi

applications provide users with greater financial inclusion, transparency, and control over their assets, enabling activities such as lending, borrowing, trading, and earning interest without relying on intermediaries like banks.

Decentralized Autonomous Organizations (DAOs) are another crucial component, operating on blockchain networks and embodying decentralized decision-making and governance. DAOs enable participants to have voting rights and influence over the organization's direction and operations, creating transparent, efficient, and community-driven models for collaboration and governance.

In the realm of identity management, Decentralized Identifiers (DIDs) empower individuals and entities with self-sovereign digital identities. DIDs offer control over personal data and enable secure and selective sharing with different parties, reducing reliance on centralized identity providers and enhancing privacy and security.

The representation of digital assets is facilitated by Fungible Tokens (FTs) and Non-Fungible Tokens (NFTs). FTs are interchangeable digital assets, akin to cryptocurrencies, while NFTs represent unique and indivisible assets like digital art, collectibles, or in-game items. NFTs have gained significant attention for their ability to establish ownership and provenance of digital assets on the blockchain, opening new possibilities for digital ownership and monetization.

Supporting these components are technologies such as Software as a Service (SaaS), which delivers applications over the internet, offering cloud-based solutions for various Web 3.0 functionalities.

Together, these components form the foundation of Web 3.0, fostering decentralization, user empowerment, and new possibilities for financial systems, governance models, identity management, asset representation, and data analysis.

2.2.1 DeFi

A Concepts

CeFi, short for Centralized Finance, refers to the traditional financial system where central institutions or banks control and manage the system. These institutions are responsible for currency issuance, record-keeping, and overseeing the circulation of money.

DeFi, short for Decentralized Finance, is a type of financial system created using blockchain technology and smart contracts. It leverages decentralized technology to eliminate reliance on central institutions, making finance more transparent, secure, and reliable. DeFi applications include decentralized lending, savings, borrowing, insurance, and more.

Overall, DeFi and CeFi represent two different financial systems that utilize different technologies and architectures to cater to different financial needs. DeFi is gaining popularity

due to its ability to provide more transparency, security, and reliability while meeting the evolving demands of financial services.

B Markets

The CeFi (Centralized Finance) market has been widely adopted in the financial industry and represents the mainstream model of the traditional financial system. CeFi market conditions have remained stable as it operates on top of the traditional financial system and is run by large financial institutions. It offers various conveniences such as bank accounts, credit services, investments, and has gained broad support.

The DeFi (Decentralized Finance) market is an emerging market that utilizes blockchain technology to provide a decentralized financial system. The DeFi market has experienced rapid growth, attracting increasing investors and developers. DeFi offers higher transparency, lower costs, and faster transaction speeds, free from the limitations of the traditional financial system.

However, the DeFi market also faces challenges such as security issues, legal concerns, and a lack of awareness and understanding of DeFi. Therefore, the development of the DeFi market still requires addressing these issues. Nevertheless, the DeFi market remains a dynamic market and is expected to continue growing in the future.

C Targets

This section is to illustrate the CeFi and DeFi protocol scopes of Web 3.0 Hong Kong system.

D Protocols

CeFi

1. Credit Cards: The credit card system is maintained by various financial institutions and allows users to make purchases of goods and services on credit.

2. Bank Transfers: Bank transfers are a common payment method that enables easy sending and receiving of funds through online banking or mobile applications.

3. PayPal: PayPal is an online service for digital payments that utilizes secure technology to protect user data and transaction records.

4. ACH Payments: ACH (Automated Clearing House) payments are an automated payment system that allows for automatic debiting of accounts on specified dates.

DeFi

1. Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They are deployed on a blockchain network and automatically execute when predetermined conditions are met. Smart contracts play a fundamental role in decentralized finance (DeFi) by enabling the automation and enforceability

of financial transactions and services. They eliminate the need for intermediaries, reduce counterparty risk, and ensure transparent and reliable execution of agreements. Smart contracts facilitate various DeFi applications such as lending, borrowing, decentralized exchanges, yield farming, and more.

Aave is a decentralized lending protocol that utilizes smart contracts to enable lending and borrowing operations. Users can deposit their digital assets into liquidity pools, and these assets are used as collateral for borrowing other assets. Smart contracts handle the collateral management, interest calculations, and repayment processes. The protocol dynamically adjusts interest rates based on supply and demand factors within the platform. Aave's smart contracts ensure the safety of deposited assets and automate the lending process, providing users with low-cost and decentralized lending services.

2. Decentralized Exchanges: Decentralized exchanges (DEXs) are platforms that allow users to trade cryptocurrencies and other digital assets directly with each other without relying on intermediaries or centralized institutions. DEXs operate on blockchain networks and utilize smart contracts to facilitate peer-to-peer trading. By eliminating the need for a central authority to hold custody of funds, DEXs enhance security, privacy, and user control over their assets. They offer a transparent and permissionless environment for trading, where users retain ownership of their assets throughout the entire transaction process.

Uniswap is a popular decentralized exchange protocol that utilizes an AMM model. It relies on smart contracts to enable token swaps between users. Uniswap creates liquidity pools by users depositing assets into smart contracts. These pools facilitate token swaps based on an algorithmic pricing mechanism. Smart contracts handle the order matching, asset custody, and settlement processes, ensuring secure and transparent trading without requiring users to trust a centralized authority.

3. Decentralized Lending: Decentralized lending is a lending service that operates on a blockchain network, removing the need for traditional financial intermediaries. In decentralized lending protocols, borrowers can obtain loans by pledging collateral in the form of digital assets. Lenders, on the other hand, provide funds and earn interest on their holdings. Smart contracts govern the lending process, automating collateral management, interest calculations, and loan repayments. Decentralized lending protocols provide users with lower costs, increased accessibility, and the ability to participate in lending activities without relying on banks or credit institutions.

Compound is a decentralized lending protocol that allows users to lend and borrow digital assets. Users deposit their assets into liquidity pools and receive interest on their deposits. Borrowers can use deposited assets as collateral to borrow other assets. Smart contracts enforce collateral requirements, calculate interest rates algorithmically, and automate the lending process. The protocol dynamically adjusts interest rates based on supply and demand dynamics within the platform.

4. Decentralized Asset Swapping: Decentralized asset swapping refers to the process of exchanging one digital asset for another directly on a blockchain network without the involvement of intermediaries. Decentralized asset swapping platforms, also known as decentralized exchanges (DEXs), utilize smart contracts to facilitate secure and transparent asset swaps. Users can trade their digital assets on these platforms without the need for traditional order books or centralized control. Decentralized asset swapping provides users with greater control over their assets, reduces reliance on centralized exchanges, and ensures efficient and secure swapping of various tokens and cryptocurrencies.

SushiSwap is a decentralized asset swapping protocol that operates based on an AMM model. It allows users to swap tokens directly through liquidity pools. Users provide liquidity by depositing assets into smart contracts and receive liquidity provider (LP) tokens in return. These LP tokens represent the user's share of the liquidity pool. Smart contracts handle the swapping process, ensuring secure and transparent asset exchanges without relying on centralized control. SushiSwap also includes additional features like yield farming and decentralized governance.

2.2.2 DAO

A Concepts

A DAO (Decentralized Autonomous Organization) is an organizational structure built on blockchain technology. It aims to achieve decentralized decision-making, management, and governance by utilizing smart contracts and algorithms instead of traditional centralized governing authorities. A DAO is formed by a group of stakeholders who collectively participate and vote, enabling them to govern and manage the organization, as well as share in its internal revenues and rights.

B Markets

Currently, DAOs are experiencing gradual growth and development as a new form of organization. Some cryptocurrency exchanges and crypto investment funds are utilizing DAOs as governance and management mechanisms. Additionally, there is a rising number of DAO projects emerging in various fields such as crowdfunding, art trading, social networks, and more.

C Targets

The primary purpose of this section is to illustrate the protocols related to DAO. Overall, these protocols together form the technical foundations of DAOs, providing the necessary tools and functionalities for governance, decision-making, financial management, contribution tracking, and identity verification within the decentralized organizational structure.

D Protocols

1. DAO Framework Protocols: DAO Framework Protocols provide the underlying infrastructure and tools to create, manage, and govern Decentralized Autonomous Organizations (DAOs). Examples like Aragon and DAOstack offer frameworks that enable the creation of DAOs with customizable governance structures, voting mechanisms, and smart contract templates. These protocols provide the necessary building blocks for DAO functionality, such as token management, proposal submission, voting mechanisms, and dispute resolution.

2. Voting Protocols: Voting protocols play a crucial role in DAOs by enabling participants to make collective decisions and shape the direction of the organization. Examples like AdChain and GovernX provide specific voting mechanisms and governance frameworks tailored for DAOs. These protocols typically utilize blockchain-based voting systems, where participants can submit and vote on proposals using their governance tokens. Voting protocols ensure transparency, accountability, and decentralized decision-making within the DAO.

3. Financial Protocols: Financial protocols within DAOs facilitate the management and allocation of funds. Examples like Moloch and MetaCartel are designed to handle financial operations within a DAO, including fundraising, budgeting, and asset management. These protocols often utilize smart contracts to govern the flow of funds, allowing participants to contribute assets, propose funding requests, and vote on resource allocation. Financial protocols ensure transparency, auditability, and effective financial management within the DAO.

4. Contribution and Incentive Protocols: Contribution and incentive protocols incentivize active participation and reward contributors within a DAO. Examples like Colony and SourceCred provide mechanisms for tracking and rewarding contributions. These protocols often utilize reputation systems, where participants earn reputation tokens based on their contributions, and these tokens can be used for governance and decision-making within the DAO. Contribution and incentive protocols encourage collaboration, recognize valuable contributions, and promote engagement within the DAO ecosystem.

5. Identity Verification and Permission Control Protocols: Identity verification and permission control protocols are essential for ensuring the integrity and security of DAO operations. Examples like uPort and Civic provide identity verification solutions that enable participants to establish and verify their digital identities within the DAO. These protocols utilize cryptographic techniques to secure user identities and ensure that only authorized individuals can access certain functions or perform specific actions within the DAO. Identity verification and permission control protocols enhance security, prevent fraud, and enable proper access control within the DAO ecosystem.

2.2.3 DID

A Concepts

DID (Decentralized Identifier): DID is a decentralized identity system used to identify and authenticate users within decentralized systems. It utilizes blockchain technology, such as Ethereum, to store user identity information and ensures data security through encryption.

DDNS (Decentralized Domain Name Service): DDNS is a decentralized domain name resolution service that maps human-readable domain names to corresponding IP addresses. It employs blockchain technology, like Ethereum, to store domain name mappings and utilizes a distributed network of nodes for decentralized data storage. This technology ensures reliability, security, and availability in domain name resolution.

B Markets

DDNS technology is used to map dynamic IP addresses to domain names for accessing devices within home networks. This technology is commonly used in personal, home, and small business environments, and there is a significant market demand for it.

DID is an emerging technology in the field of distributed identity, aiming to provide a means to ensure reliable and controllable identities for individuals and organizations. DID technology is still in its early stages, but with increasing focus on digital identity and privacy protection, it holds promising market prospects.

Overall, both technologies have favorable market conditions, but DDNS has a more mature market, while DID is in a stage of continuous development.

C Targets

The primary purpose of this section is to illustrate the protocols related to DID and DDNS. Web 3.0 Hong Kong encompasses the utilization and advancement of these technologies and concepts to enable a more decentralized, user-centric, and secure web experience.

D Protocols

DID

1. W3C DID (World Wide Web Consortium Decentralized Identifier): W3C DID is a specification developed by the World Wide Web Consortium (W3C) that defines a method for creating and managing decentralized identifiers. Decentralized identifiers are unique identifiers that are not controlled by any central authority. They enable individuals and entities to have self-sovereign control over their digital identities and associated data. W3C DID provides a standardized format and protocols for creating, resolving, and interacting with decentralized identifiers, allowing for interoperability and compatibility across different systems and platforms.

2. Self-sovereign Identity (SSI): Self-sovereign identity refers to the concept of individuals and entities having full control and ownership over their digital identities and personal data. It allows users to manage and share their identity information in a secure and privacy-preserving manner, without relying on centralized authorities or intermediaries. SSI solutions leverage decentralized technologies such as blockchain and decentralized identifiers (DIDs) to enable individuals to create, manage, and control their identities, selectively share identity information, and verify their identities without sacrificing privacy or being subject to data breaches.

3. Sovrin DID (Sovrin Decentralized Identifier): Sovrin DID is a type of decentralized identifier based on the Sovrin Network, which is a public permissioned blockchain network designed specifically for self-sovereign identity. Sovrin DIDs enable individuals and entities to create unique identifiers that are globally resolvable, cryptographically secure, and under their own control. The Sovrin Network provides the infrastructure and protocols for managing and resolving Sovrin DIDs, ensuring privacy, security, and interoperability for self-sovereign identity solutions.

4. HTC DID (Hyperledger Trust Chain Decentralized Identifier): HTC DID is a type of decentralized identifier based on Hyperledger technologies, specifically the Hyperledger Indy framework. Hyperledger Indy is an open-source project focused on providing a decentralized identity infrastructure. HTC DIDs are designed to enable secure and privacy-preserving digital identity management. The Hyperledger Trust Chain (HTC) is used to establish and verify the integrity of DIDs, ensuring trust and authenticity within the system. HTC DIDs leverage blockchain technology to provide decentralized identity solutions.

5. IPFS DID (InterPlanetary File System Decentralized Identifier): IPFS DID is a type of decentralized identifier that utilizes the InterPlanetary File System (IPFS) for decentralized data storage and retrieval. IPFS is a distributed file system that provides a content-addressable and peer-to-peer method for storing and sharing data. IPFS DIDs allow individuals and entities to create identifiers that reference data stored on the IPFS network. This approach ensures data integrity, immutability, and censorship resistance, making IPFS DIDs suitable for applications where decentralized and resilient identity solutions are required.

DDNS

1. ENS (Ethereum Name Service): ENS is a decentralized domain name system built on the Ethereum blockchain. It allows users to register and manage human-readable domain names for their Ethereum addresses, smart contracts, and decentralized websites. ENS replaces long and complex Ethereum addresses with easy-to-remember domain names, making interactions with the Ethereum ecosystem more user-friendly. ENS leverages smart contracts to map domain names to Ethereum addresses, enabling seamless resolution and interaction with blockchain-based services.

2. Handshake: Handshake is a decentralized naming protocol that aims to create a more secure and censorship-resistant internet. It operates as a peer-to-peer network, utilizing blockchain technology to enable the registration and ownership of top-level domain names. Handshake introduces a decentralized auction mechanism for domain name registration, ensuring fair and transparent allocation of domain names. By decentralizing the domain name system, Handshake aims to reduce reliance on centralized authorities and enhance security and ownership of domain names.

3. Unstoppable Domains: Unstoppable Domains is a domain name system built on blockchain technology, primarily utilizing the Ethereum and Zilliqa blockchains. It allows users to register domain names that are stored on the blockchain, ensuring censorship resistance and ownership

rights. Unstoppable Domains leverages blockchain smart contracts to handle domain registration, resolution, and ownership transfers. These domain names can be used for websites, email addresses, and cryptocurrency addresses, providing a decentralized and user-centric approach to internet naming.

4. DNS (Domain Name System): The Domain Name System (DNS) is a decentralized hierarchical naming system that translates domain names into IP addresses. It is a fundamental component of the internet infrastructure, enabling users to access websites and services using human-readable domain names. DNS operates through a distributed network of servers, which store and propagate DNS records. When a user enters a domain name, DNS servers resolve it to the corresponding IP address, allowing the user's device to establish a connection with the desired destination.

5. HTTP (Hypertext Transfer Protocol): HTTP is the protocol used for transmitting hypertext, such as HTML, over the internet. It is the foundation of the World Wide Web and facilitates communication between web browsers and web servers. HTTP defines a set of rules and standards for requesting and delivering web content. When a user requests a webpage, the browser sends an HTTP request to the server, and the server responds with the requested content. HTTP enables the retrieval and display of webpages, the submission of form data, and the interaction between clients and servers on the web.

6. FTP (File Transfer Protocol): FTP is a network protocol used for transferring files between a client and a server on a computer network. It provides a simple and standardized way to upload and download files over the internet. FTP operates on a client-server architecture, where the client establishes a connection with the server and performs file transfer operations using FTP commands. It supports various file transfer modes, including ASCII and binary, and provides features such as directory listing, file permissions, and file management.

7. SMTP (Simple Mail Transfer Protocol): SMTP is a protocol used for sending and receiving email messages over the internet. It is responsible for the transmission of email between email clients and mail servers. SMTP operates on a client-server model, where the client initiates a connection with the server to send an email. The server handles the delivery of the email to the recipient's mail server. SMTP defines the rules and procedures for email transfer, including addressing, message formatting, and error handling, ensuring the reliable delivery of email messages.

2.2.4 FT&NFT

A Concepts

FT (Fungible Token):

Fungible tokens, often abbreviated as FTs, are digital assets that are mutually interchangeable and indistinguishable from one another. Each unit of a fungible token is considered equivalent to every other unit of the same token. This means that fungible tokens are interchangeable on a

one-to-one basis, just like physical currencies. They have identical properties and values, enabling seamless exchange and interchangeability without any impact on their functionality or value.

Key characteristics of FTs can be listed as follows.

1. Interchangeability: Each unit of an FT is equivalent to every other unit of the same token, with no unique distinguishing features.

2. Indivisibility: FTs can be divided into smaller units, enabling fractional ownership and transactions.

3. Uniformity: All units of an FT are identical in terms of properties, value, and functionality.

4. Interoperability: Fungible tokens can be easily exchanged or traded with one another without any loss of value.

Examples of FTs can be classified as follows.

1. Cryptocurrencies: Popular cryptocurrencies like Bitcoin (BTC) and Ethereum (ETH) are fungible tokens.

2. Stablecoins: Stablecoins, such as Tether (USDT) and USD Coin (USDC), are fungible tokens pegged to a specific value, typically a fiat currency.

NFT (Non-Fungible Token):

Non-fungible tokens, or NFTs, are digital assets that are unique and indivisible. Each NFT has distinct properties, attributes, and characteristics that differentiate it from other tokens. Unlike fungible tokens, NFTs cannot be exchanged on a one-to-one basis as they possess unique and non-replaceable qualities, making them valuable for their individuality and scarcity.

Key characteristics of NFTs are listed as follows.

1. Uniqueness: NFTs are one-of-a-kind digital assets, with each token having distinct properties and attributes.

2. Indivisibility: NFTs cannot be divided into smaller units. Each token represents a whole and cannot be fragmented.

3. Ownership and Authenticity: NFTs are often used to prove ownership and authenticity of digital assets, such as artwork, collectibles, virtual real estate, and more.

4. Scarcity: NFTs can be intentionally limited in supply, creating scarcity and value for collectors and enthusiasts.

Examples of NFTs can be classified as follows.

1. Digital Art: NFTs have gained significant popularity in the digital art world, allowing artists to tokenize and sell their unique digital creations.

2. Collectibles: NFTs enable the creation and ownership of digital collectibles, such as virtual trading cards, virtual pets, and virtual real estate.

3. Virtual Assets: NFTs can represent ownership of virtual assets within video games and virtual worlds, such as virtual land, in-game items, and characters.

NFT++ is an upgraded technology that focuses on Non-Fungible Tokens (NFTs) with the aim of realizing the intrinsic value of NFTs and enabling data transformation calculations. The main difference between NFT++ and NFT lies in NFT++ emphasizing the inherent value of data and enabling data transformation calculations. By leveraging Smart Contracts and next-generation privacy-preserving computations, NFT++ achieves enhanced security and trustworthiness.

B Markets

Indeed, the market for NFT++ is experiencing rapid growth. With the continuous development of cryptocurrency and blockchain technology, NFT++ is gaining popularity among a growing number of users. The market prospects for NFT++ are optimistic, and it is expected that the market size will significantly increase in the future.

C Targets

The purpose of this section is to specify the related protocols to the NFT.

D Protocols

1. ERC-721 and ERC-1155:

ERC-721 and ERC-1155 are Ethereum token standards used to create non-fungible tokens (NFTs) and unique digital assets that can be traded on the Ethereum blockchain.

ERC-721:

- ERC-721 is the standard for creating non-fungible tokens on Ethereum.

- Each ERC-721 token is unique and represents a distinct asset or digital item.

- ERC-721 tokens are indivisible and cannot be divided into smaller units.

- They are often used for representing digital collectibles, unique artwork, and virtual assets in games.

- Each ERC-721 token has a unique identifier (token ID) that distinguishes it from other tokens.

- ERC-721 includes functions for transferring ownership of tokens and querying token metadata.

ERC-1155:

- ERC-1155 is a multi-token standard that allows the creation of both fungible and non-fungible tokens on Ethereum.

- It enables the creation of multiple token types within a single contract.

- ERC-1155 tokens can be either fungible (identical and interchangeable) or non-fungible (unique and distinct).

- It provides a more efficient way to manage and interact with multiple types of digital assets.

- ERC-1155 supports batch transfers, allowing for the efficient transfer of multiple tokens in a single transaction.

- It is widely used for the creation of gaming assets, where both unique and fungible tokens are needed.

2. ERC-1400:

ERC-1400 is an Ethereum token standard used for creating digital assets based on asset ownership. It focuses on security, privacy, and regulatory compliance for tokenized assets.

- ERC-1400 introduces the concept of partitioning tokens based on different ownership categories, such as different investor types or regulatory requirements.

- It includes features like controlled token transfers, which enforce certain conditions or permissions for transferring tokens.

- ERC-1400 supports token issuance, redemption, and modification of token properties.

- It provides mechanisms for verifying investor eligibility and enforcing compliance with regulations.

- ERC-1400 includes events and functions for tracking and managing token transfers, approvals, and rejections.

3. ERC-1410 and ERC-1411:

ERC-1410 and ERC-1411 are Ethereum token standards used to create digital assets that can have multiple types, and they allow for managing, splitting, and merging tokens in batches.

- ERC-1410 enables the creation of tokens with multiple customizable partitions, allowing for different types of ownership or rights.

- It provides functions for transferring tokens between partitions, checking partition balances, and querying token metadata.

- ERC-1410 supports batch transfers, enabling the efficient transfer of tokens across multiple partitions in a single transaction.

- ERC-1411 extends ERC-1410 by introducing token split and merge functionalities.

- Token splitting allows for dividing a token into smaller units, while token merging enables combining multiple tokens into a single unit.

- These features offer increased flexibility and granularity in managing token ownership and rights.

4. ERC-20, ERC-223, and ERC-777:

ERC-20, ERC-223, and ERC-777 are Ethereum token standards used to create token-based assets that support smart contracts and custom transaction handling.

- ERC-20 is the most widely adopted token standard on Ethereum, providing a basic set of functions for creating fungible tokens.

- ERC-20 tokens are interchangeable and can be divided into smaller units (divisibility).

- They support common operations such as balance checking, transferring tokens, and approving token spending.

- ERC-20 tokens are widely used for initial coin offerings (ICOs), token sales, and general-purpose tokenization.

- ERC-223 is an improvement over ERC-20 that provides additional safety measures for token transfers.

- ERC-223 introduces a tokenFallback function to prevent accidental loss of tokens during transfers to contracts that do not support token handling.

- ERC-777 is an advanced token standard that enhances the functionality and flexibility of ERC-20 tokens.

- ERC-777 introduces hooks and callbacks, allowing for more control and customization of token transfers.

- It provides enhanced security features, including token recovery in case of accidental token transfers to incorrect addresses.

These token standards play a crucial role in creating and managing various types of digital assets, providing interoperability, compatibility, and standardized functionalities within the Ethereum ecosystem.

2.2.5 Smart Contract

A Concepts

A Smart Contract is a special type of computer program based on blockchain technology. It is designed to manage and execute business logic such as contracts, transactions, and protocols. Smart contracts can be viewed as automated contracts that can automatically execute and manage transactions between parties without the need for any intermediaries or regulatory bodies. The execution outcomes of smart contracts are recorded on the blockchain, ensuring their immutability and tamper-resistance.

B Markets

Smart contracts are indeed one of the significant applications of blockchain technology and have been widely adopted in various fields such as finance, digital assets, supply chain management, digital identity authentication, and the Internet of Things (IoT). In the decentralized finance (DeFi) sector, smart contracts are extensively used for the automated management and execution of various financial products. As of early 2022, the total value locked in the DeFi sector has surpassed $250 billion. The market prospects for smart contracts are vast, and it is projected to reach $31.5 billion by 2028.

C Targets

The purpose of this section is to specify the related protocols to smart contract.

D Protocols

1. Programming Language Protocols:

Smart contract programming languages are used to write the code that defines the behavior and logic of the contracts. Here are some commonly used programming languages for smart contracts:

- Solidity: Solidity is the most widely used programming language for Ethereum smart contracts. It is a statically-typed language specifically designed for writing smart contracts on the Ethereum platform.

- Vyper: Vyper is another programming language for Ethereum smart contracts. It is a Python-inspired language that aims to improve security and simplicity compared to Solidity.

- Rust: Rust is a systems programming language that has gained popularity for smart contract development, particularly on the Substrate framework. It focuses on memory safety and performance.

- Java: Java is a general-purpose programming language that has been adapted for smart contract development on platforms like Corda and Hyperledger Fabric.

- C++: C++ is a widely used programming language that can be used for smart contract development on various blockchain platforms, including EOSIO.

Different blockchain platforms may support different programming languages for writing smart contracts, depending on their specific design and virtual machine architecture.

2. Standard Protocols:

Standard protocols for smart contracts provide a set of rules and interfaces that define how contracts should be structured and interact with each other. Here are a few examples.

- ERC-20: ERC-20 is a token standard on the Ethereum platform that defines a common set of rules for fungible tokens. It specifies the functions and events that a token contract should implement to enable seamless integration with other contracts and wallets.

- ERC-721: ERC-721 is a token standard for non-fungible tokens (NFTs) on Ethereum. It allows the creation and management of unique tokens, such as collectibles, digital art, and in-game assets.

- ERC-1155: ERC-1155 is a multi-token standard on Ethereum that allows the creation of contracts capable of managing both fungible and non-fungible tokens. It provides efficiency benefits by allowing multiple token types to be managed within a single contract.

These standard protocols enable interoperability between different contracts and provide a foundation for building decentralized applications (dApps) and token ecosystems.

3. Development Tool Protocols:

Development tool protocols are software tools and environments that assist developers in building, testing, and deploying smart contracts. Here are a few examples:

- Truffle: Truffle is a popular development framework for Ethereum that provides a suite of tools for managing the development lifecycle of smart contracts. It includes features like contract compilation, deployment, testing, and asset management.

- Remix IDE: Remix IDE is an integrated development environment specifically designed for smart contract development. It offers a browser-based interface with features like code editing, debugging, and deployment to various blockchain networks.

- Ganache: Ganache is a local blockchain emulator that provides a testing environment for smart contracts. It allows developers to simulate blockchain behavior locally, enabling rapid iteration and testing of contract functionality.

These development tool protocols help streamline the development process, improve efficiency, and provide an environment for developers to write, test, and debug their smart contracts.

4. Security Standard Protocols:

Security standard protocols aim to address the potential vulnerabilities and risks associated with smart contracts. Here are a couple of examples:

- Solidity Smart Contract Security Standard (SOS): SOS is a set of guidelines and best practices for writing secure smart contracts in Solidity. It covers topics such as secure coding patterns, avoiding common vulnerabilities, and mitigating attack vectors.

- OpenZeppelin's Smart Contract Security Standard: OpenZeppelin is a widely-used library for secure smart contract development on Ethereum. They have defined their own standard for secure contract development, which includes guidelines for secure coding practices, access control, and upgradeability.

These security standard protocols provide developers with guidelines, best practices, and tools to ensure the security and reliability of their smart contracts.

5. Smart Contract Design Protocols:

Smart contract design protocols offer frameworks and methodologies to assist developers in designing and implementing smart contracts effectively. Here are a couple of examples:

- Domain-specific Language (DSL) protocols: DSL protocols provide specialized languages or frameworks tailored to specific business domains. For example, the Marlowe DSL is designed for financial contracts on the Cardano blockchain, providing abstractions and tools for contract modeling and analysis.

- Formal Verification protocols: Formal verification is a technique that uses mathematical proofs to ensure the correctness and security of smart contracts. Protocols like the Ethereum Foundation's Formal Verification Initiative provide tools, libraries, and methodologies to formally verify smart contracts, reducing the risk of bugs and vulnerabilities.

These smart contract design protocols help developers create robust contracts that meet the requirements of specific industries or domains while minimizing the potential for errors and vulnerabilities.

2.2.6 Cross Chain

A Concepts

The concept of cross-chain technology in the context of Web 3.0 refers to the ability to facilitate interoperability and seamless communication between multiple blockchain networks. It enables the transfer of assets, data, and functionality across disparate blockchains, thereby creating a connected and integrated ecosystem. Cross-chain technology plays a pivotal role in unlocking the full potential of Web 3.0 by addressing the issue of blockchain fragmentation and enabling collaboration between different blockchain networks.

B Markets

The market status of cross-chain interoperability showed significant growth and interest within the blockchain industry. According to a report by Deloitte, the total value locked (TVL) in cross-chain projects exceeded $8 billion in early 2021, indicating the growing adoption and utilization of interoperability solutions. Additionally, several notable cross-chain protocols and projects gained traction during this period. For instance, Polkadot, a prominent interoperability-focused blockchain platform, reached a market capitalization of over $30 billion, showcasing the market's enthusiasm for cross-chain solutions. Partnerships and collaborations were actively pursued, with the number of blockchain networks integrating with interoperability frameworks and cross-chain bridges steadily increasing. The market witnessed a rising emphasis on data interoperability, with a focus on developing standards and protocols for secure and efficient cross-chain data exchange.

C Targets

This section illustrates the protocol stack desugb for cross-chain technology in the context of Web 3.0.

D Protocols

The protocol stack for cross-chain technology in the context of Web 3.0 encompasses various layers that enable interoperability and communication between different blockchain networks. Here is a high-level design of the protocol stack for cross-chain in Web 3.0:

1. Consensus Layer:

At the lowest layer of the protocol stack, the consensus layer ensures the secure and decentralized agreement on the state of each participating blockchain network. This layer includes the consensus protocols used by individual blockchains, such as Proof of Work (PoW), Proof of Stake (PoS), or other consensus mechanisms specific to each blockchain network.

2. Network Layer:

The network layer is responsible for establishing connectivity and communication between different blockchain networks. It defines the protocols and infrastructure for transmitting data and messages across networks. This layer includes protocols like TCP/IP, UDP, and transport layer security (TLS) to ensure secure and reliable communication between nodes.

3. Cross-Chain Messaging Layer:

The cross-chain messaging layer facilitates the exchange of messages and information between different blockchain networks. It enables the transfer of assets, data, and functionality across chains. This layer includes protocols like Inter-Blockchain Communication (IBC), Cross-Chain Communication Protocol (CCCP), or other messaging protocols specifically designed for cross-chain communication.

4. Cross-Chain Consensus Layer:

The cross-chain consensus layer ensures consensus among different blockchain networks when interacting and transferring assets or data. It establishes the rules and mechanisms for validating and confirming cross-chain transactions. This layer may include protocols like Threshold Signature Scheme (TSS), Multi-Party Computation (MPC), or other consensus mechanisms tailored for cross-chain operations.

5. Interoperability Layer:

The interoperability layer provides the necessary protocols and standards for seamless interaction and data exchange between different blockchains. It includes protocols like Atomic Swaps, Token Bridges, Cross-Chain Smart Contracts, or other interoperability frameworks. This layer allows for the transfer of assets and data across chains while preserving security, integrity, and consistency.

6. Data Layer:

The data layer handles the storage and retrieval of cross-chain data and metadata. It may include protocols for indexing, querying, and accessing data across different blockchains. This layer ensures efficient and secure access to cross-chain information and facilitates the development of decentralized applications that rely on cross-chain data.

7. User Layer:

The application layer represents the highest level of the protocol stack and encompasses the decentralized applications (DApps) built on top of the cross-chain infrastructure. DApps leverage the underlying layers to provide users with seamless access to cross-chain functionality, assets, and services. This layer includes various application-specific protocols and standards specific to each DApp or use case.

It's important to note that the design and composition of the protocol stack may vary based on specific cross-chain implementations and requirements. The protocol stack outlined here provides a generalized framework for understanding the different layers involved in enabling cross-chain interoperability in Web 3.0.

2.2.7 SaaS

A Concepts

SaaS (Software as a Service) in Web 3.0 refers to the delivery model where software applications are provided as on-demand services over the decentralized web. It involves the deployment of applications on decentralized infrastructure, such as blockchain platforms, and enables users to access and use these applications through web browsers or decentralized interfaces. SaaS in Web 3.0 leverages the benefits of decentralization, such as increased security, user control over data, and the ability to interact with smart contracts and decentralized

protocols. It allows for the development and deployment of innovative, decentralized applications that offer scalability, interoperability, and enhanced user experiences.

B Markets

The market status of Software-as-a-Service (SaaS) in Web 3.0 was experiencing significant growth and interest. The emergence of Web 3.0, which focuses on decentralized and blockchain-powered applications, opened up new opportunities for SaaS providers. According to a report by Statista, the global SaaS market was projected to reach a value of $157 billion in 2020, reflecting the increasing demand for cloud-based software solutions. In the context of Web 3.0, SaaS providers were exploring the integration of blockchain technology to offer enhanced security, transparency, and decentralization to their services. Projects were being developed to leverage blockchain's distributed ledger capabilities, smart contracts, and decentralized storage to offer SaaS solutions aligned with the principles of Web 3.0. While specific statistics on the market size of SaaS in Web 3.0 may not be readily available, the market was witnessing a growing interest and exploration of blockchain-powered SaaS solutions during this period.

C Targets

The purpose of this section is to illustrate the aspects of protocol design for SaaS.

D Protocols

When designing a protocol for Software-as-a-Service (SaaS) with a model-driven approach, the protocol design is guided by the use of models that capture the structure, behavior, and interactions of the SaaS application and its components. Here's an illustration of the protocol design for SaaS with a model-driven approach:

1. Domain Modeling:

The protocol design begins with domain modeling, which involves creating models that represent the domain concepts, entities, and relationships relevant to the SaaS application. Domain-specific modeling languages, such as UML (Unified Modeling Language) or domain-specific languages (DSLs), can be used to create these models. The domain models provide a high-level understanding of the SaaS application's functionalities and help define the scope of the protocol design.

2. Service Contract Modeling:

Based on the domain models, the protocol design proceeds with service contract modeling. Service contracts define the interactions between the client and the SaaS application, including the operations, input/output parameters, and expected behavior. The model-driven approach allows the creation of service contract models using tools like UML or Web Services Description Language (WSDL). These models capture the interfaces and communication protocols that clients can use to interact with the SaaS application.

3. Protocol Specification:

Using the service contract models, the protocol design moves on to specify the underlying protocols that enable communication between the client and the SaaS application. Model-driven protocol specification languages, such as Message Sequence Charts (MSC) or Sequence Diagrams, can be used to define the sequence of messages exchanged, the order of operations, and the expected responses. These models provide a visual representation of the protocol flow, making it easier to understand and validate the protocol design.

4. Transformation to Formal Specifications:

The service contract models and protocol specifications created in the previous steps can be transformed into formal specifications using model-driven engineering techniques. Formal specification languages such as Abstract State Machines (ASM), Petri nets, or formal modeling languages like Alloy can be used to express precise and unambiguous specifications of the protocol behavior. These formal specifications help verify the correctness and consistency of the protocol design and can be used for automated analysis and validation.

5. Code Generation:

Once the protocol design and formal specifications are established, the model-driven approach facilitates code generation. Code generators can automatically generate the necessary code artifacts, such as API endpoints, message handlers, and data structures, based on the formal specifications. This reduces manual coding efforts and ensures that the implemented protocol adheres to the defined design.

6. Testing and Validation:

The model-driven approach allows for automated testing and validation of the implemented protocol. Test cases can be generated from the models and specifications, ensuring comprehensive coverage of the protocol's behavior and edge cases. Model-based testing tools can execute these test cases and compare the actual protocol behavior with the expected results, enabling efficient verification and validation of the implemented protocol.

7. Iterative Refinement:

The model-driven approach enables iterative refinement of the protocol design. As the SaaS application evolves or new requirements emerge, the models and specifications can be updated, and the code can be regenerated to reflect the changes. This iterative process ensures that the protocol design remains aligned with the evolving needs of the SaaS application and its users.

By leveraging a model-driven approach, the protocol design for SaaS benefits from visual modeling, formal specification, automated code generation, and rigorous testing. This approach enhances the clarity, consistency, and correctness of the protocol design, leading to more reliable and efficient SaaS applications.

2.2.8 Data Analysis and Governance

A Concepts

Data Analysis in Web 3.0 refers to the process of extracting insights and value from decentralized data sources within the context of a decentralized web ecosystem. It involves applying statistical analysis, machine learning, and other techniques to decentralized data to identify patterns, trends, and anomalies.

Data Governance in Web 3.0 refers to the policies, processes, and frameworks that ensure the proper management, control, and protection of decentralized data. It encompasses user control over personal data, smart contract-based governance mechanisms, compliance with regulations, and the establishment of standards and interoperability for data exchange and integration.

B Markets

The data analysis and governance market is a rapidly growing industry driven by the increasing need for organizations to effectively manage and derive insights from their data while ensuring data quality, security, and compliance.

Market Size: The data analysis and governance market has been expanding significantly in recent years. According to market research reports, the global market size was estimated to be in the range of billions of dollars in 2020. The market is expected to continue growing at a healthy rate over the coming years.

Increasing Investments: Organizations across various sectors are increasingly investing in data analysis and governance solutions. These investments include spending on data analytics tools, data management platforms, data governance software, and related services.

Cloud-based Solutions: Cloud computing has had a significant impact on the market. Many organizations are adopting cloud-based data analysis and governance solutions due to their scalability, flexibility, and cost-effectiveness. Cloud-based offerings also allow businesses to leverage advanced analytics capabilities without substantial infrastructure investments.

Data Governance and Compliance: The growing number of data regulations, such as the GDPR and CCPA, has heightened the importance of data governance and compliance. Organizations

are investing in solutions that help them establish data governance frameworks, adhere to regulatory requirements, and protect sensitive data.

Analytics Tools and Platforms: The market offers a wide range of data analysis tools and platforms, including business intelligence (BI) software, data visualization tools, predictive analytics solutions, and machine learning platforms. These tools enable businesses to process and analyze large volumes of data, uncover patterns, and derive actionable insights.

Market Players: The data analysis and governance market is highly competitive, with a mix of established software providers and specialized vendors. Major players in the market include companies like IBM, Oracle, Microsoft, SAP, SAS Institute, and Tableau, among others. Additionally, there are numerous emerging startups offering innovative solutions in specific niches.

C Targets

The purpose of this section is to illustrate the aspects of protocol design for data analysis and governance.

D Protocols

In the context of Web 3.0, data analysis and governance rely on various protocol stacks to provide the necessary infrastructure and frameworks. These protocol stacks encompass different layers and components that work together to enable decentralized data analysis and governance. Here's an overview of the protocol stacks for data analysis and governance in Web 3.0 based on the blockchain platform.

1. Interoperability Layer:

The interoperability layer focuses on enabling seamless data exchange and integration across different decentralized applications and platforms. Protocols like Polkadot, Cosmos, and InterPlanetary Linked Data (IPLD) facilitate interoperability by establishing standards, cross-chain communication, and data interoperability protocols.

2. Decentralized Identity Layer:

Decentralized identity protocols play a crucial role in data governance by providing users with control over their identities and personal data. Protocols like SelfKey, uPort, and Sovrin enable

users to manage their identities, consent, and data sharing permissions in a self-sovereign manner.

3. Consensus and Security Layer:

The consensus and security layer ensures the integrity and security of decentralized data. It includes consensus algorithms, cryptographic techniques, and smart contract platforms. Examples of protocols in this layer are Ethereum, Polkadot, Avalanche, and protocols like zero-knowledge proofs (Zcash, zk-SNARKs) that enhance privacy and confidentiality.

4. Governance and Compliance Layer:

The governance and compliance layer focuses on establishing frameworks and mechanisms for decentralized data governance. This layer includes protocols like Aragon, DAOstack, and decentralized governance frameworks that enable community-driven decision-making, voting, and consensus on data governance rules and policies. Compliance solutions, such as KYC/AML protocols, are also included in this layer.

5. Analytics and Insights Layer:

The analytics and insights layer encompasses the tools, frameworks, and protocols for performing data analysis on decentralized data sources. This layer includes decentralized analytics platforms, machine learning frameworks, and privacy-preserving analytics techniques like federated learning and differential privacy. Examples of protocols and frameworks in this layer include Ocean Protocol, SingularityNET, and projects integrating AI/ML with blockchain technology.

These protocol stacks work together to provide the necessary infrastructure, standards, and frameworks for data analysis and governance in Web 3.0. However, it's important to note that the specific protocols and projects within each layer may evolve and change over time as the Web 3.0 ecosystem continues to develop and mature.

2.3 Application Layer

The Application Layer for Web 3.0 encompasses a range of innovative applications and use cases that leverage the underlying technologies of the Web 3.0 ecosystem. Within this layer, several key components shape the user experience and drive the transformation of the internet.

At the forefront is the concept of the Metaverse, a virtual universe where users can engage with computer-generated environments and interact with others in real-time. The Metaverse offers immersive experiences, spanning virtual reality (VR), augmented reality (AR), and virtual worlds. It presents opportunities for social interactions, entertainment, gaming, e-commerce, and even virtual asset ownership.

Digital Finance applications are another crucial component of the Application Layer. These applications utilize blockchain technology to revolutionize traditional financial systems. They encompass decentralized financial services such as lending, borrowing, decentralized exchanges, liquidity provision, yield farming, and asset management. By leveraging the decentralized nature of Web 3.0, Digital Finance applications provide users with greater control over their finances and enable secure and transparent transactions without relying on intermediaries.

The Creator Economy is a thriving ecosystem within Web 3.0 that empowers content creators, artists, influencers, and entrepreneurs to monetize their digital creations directly. Web 3.0 enables creators to tokenize their work as non-fungible tokens (NFTs), allowing for unique digital asset ownership and new monetization opportunities. Additionally, decentralized content platforms, peer-to-peer marketplaces, and micropayments enable creators to engage directly with their audience, bypassing traditional gatekeepers and capturing the value they generate.

Decentralized Applications (DApps) are at the core of the Web 3.0 Application Layer. These applications are built on blockchain networks, leveraging the decentralized and transparent nature of Web 3.0. DApps operate without intermediaries, granting users control over their data and assets. They span various industries, including finance, gaming, supply chain, social media, and more. By offering enhanced security, privacy, and user empowerment, DApps revolutionize traditional centralized applications and foster a user-centric internet experience.

Together, these components within the Application Layer of Web 3.0 drive the transformation of how users interact with digital content, engage in finance, and participate in online communities. The Metaverse provides immersive virtual experiences, Digital Finance applications empower users with decentralized financial services, the Creator Economy enables content creators to monetize their work, and DApps leverage blockchain technology to create decentralized and transparent applications, reshaping multiple industries and fostering a user-centric internet experience.

2.3.1 Metaverse

A Concepts

The metaverse is an advanced technology that combines augmented reality (AR), virtual reality (VR), and mixed reality (XR). It utilizes blockchain technology to provide users with a digital world where they can create, manage, and exchange digital assets.

As the top-level application of Web3, the metaverse integrates the virtual world of Web3 with the real world, significantly enhancing user experience and immersion. It requires the development and integration of protocols across various layers to support its functionality.

B Markets

Currently, the market for metaverse applications is favorable, particularly in recent years. With the advancement of metaverse technology, the overall performance of metaverse applications has greatly improved, and their applications have expanded into various fields. Moreover, consumers are increasingly interested in metaverse application content. Notable metaverse application projects include Intel's RealSense technology, Google's Project Tango, Microsoft's HoloLens, and more. These technologies enable real-time 3D sensing, indoor positioning, 3D graphics modeling, virtual reality experiences, augmented reality, and mixed reality functionalities. With the development of 5G technology, the market prospects for metaverse applications are even more optimistic.

C Targets

This section is to outline the protocols for the Layer 3 metaverse in the Hong Kong Web 3.0 application.

D Protocols

1. Hardware Device Layer Protocol:

The Hardware Device Layer Protocol in the context of the Web 3.0 metaverse in Hong Kong defines the communication standards and protocols that facilitate seamless interaction between various hardware devices and components within the metaverse ecosystem. This protocol ensures effective communication between devices such as virtual reality headsets, augmented reality glasses, motion controllers, and other peripherals. It establishes guidelines for device compatibility, data formats, input/output mechanisms, synchronization, and integration with other layers of the metaverse architecture. The protocol enables devices to exchange data and commands, allowing users to interact with the virtual environment and control their avatars or digital representations.

2. Network Layer Protocol:

The Network Layer Protocol in the Web 3.0 metaverse of Hong Kong is responsible for managing data routing and communication between different networks within the metaverse ecosystem. This protocol ensures efficient and secure transmission of data packets across local area networks (LANs), wide area networks (WANs), and the internet. It establishes the guidelines and standards for network addressing, routing algorithms, packet prioritization, congestion control, security measures, and data integrity. The Network Layer Protocol enables seamless communication between users, devices, and virtual environments, facilitating real-time interactions, multiplayer experiences, and data exchange within the metaverse.

3. Computing Power Protocol:

The Computing Power Protocol in the Web 3.0 metaverse of Hong Kong supports the enablement and provision of computing resources required to power the metaverse. This protocol defines the mechanisms for accessing and utilizing computational capabilities, including processing power, memory, and storage within the metaverse ecosystem. It encompasses distributed computing, cloud computing, edge computing, and peer-to-peer computing models to efficiently handle the computational demands of metaverse applications and services. The Computing Power Protocol ensures scalability, resource allocation, fault tolerance, load balancing, and efficient utilization of computing resources, enabling immersive and responsive experiences within the metaverse.

4. Transport Layer Protocol:

The Transport Layer Protocol in the Web 3.0 metaverse of Hong Kong is responsible for the reliable and secure transfer of data between devices and across networks. These protocols establish communication channels and standards for transferring data packets from one device to another within the metaverse ecosystem. They handle tasks such as segmentation, reassembly, error detection, and error correction to ensure data integrity and efficient transmission. The Transport Layer Protocol enables seamless and efficient data exchange between devices, facilitating real-time interactions, content streaming, and synchronization within the metaverse.

5. Video Image Protocol:

The Video Image Protocol in the Web 3.0 metaverse of Hong Kong defines the formats and transmission methods for graphic content, including images and videos, within the metaverse ecosystem. This protocol establishes standards for encoding, compression, and rendering of visual data to optimize bandwidth usage and ensure high-quality visual experiences. It enables the seamless transmission and display of graphical content across devices and platforms, supporting immersive visuals, realistic environments, and engaging visual interactions within the metaverse.

6. Virtual Platform Protocol:

The Virtual Platform Protocol in the Web 3.0 metaverse of Hong Kong enables the development and operation of immersive digital simulations, environments, and worlds. This protocol

establishes guidelines and standards for the creation, management, and exploration of virtual spaces where users and businesses can interact, create, socialize, and engage in various experiences. It encompasses aspects such as virtual world creation tools, physics simulations, avatar customization, object interactions, social networking features, and economic systems. The Virtual Platform Protocol forms the foundation for immersive and interactive experiences within the metaverse, fostering creativity, collaboration, and economic activities.

7. User Layer Protocol:

The User Layer Protocol in the Web 3.0 metaverse of Hong Kong defines the protocols and standards for interaction between applications and users within the metaverse. This protocol governs the user interface, user input mechanisms, and data exchange between applications and users. It ensures consistency, compatibility, and interoperability among metaverse applications, allowing users to seamlessly navigate and interact with various metaverse experiences. One example of an User Layer Protocol is OpenXR, a universal VR and AR application programming interface (API) protocol, which provides a standardized interface for developers to create metaverse applications that can run across different devices and platforms.

8. Metaverse Content, Services, and Asset Protocol:

The Metaverse Content, Services, and Asset Protocol in the Web 3.0 metaverse of Hong Kong is designed to enable the creation, distribution, and management of digital assets within the metaverse ecosystem. This protocol encompasses protocols and standards for designing, creating, selling, reselling, storing, securing, and managing various digital assets, such as virtual goods, virtual currencies, and user-generated content. It addresses aspects such as asset ownership, provenance, interoperability, security, privacy, and financial transactions within the metaverse. The Metaverse Content, Services, and Asset Protocol ensures a secure and efficient marketplace for digital assets, fostering creativity, economic opportunities, and user participation within the metaverse.

2.3.2 Digital Finance

Digital finance in Web 3.0 refers to the integration of decentralized technologies, such as blockchain and cryptocurrencies, into traditional financial systems, enabling new possibilities for financial transactions, services, and infrastructure. Here we discuss open banking and eKYC.

Open Banking

A Concepts

Open Banking is a concept in financial technology (Fintech) that aims to transform the traditional service models of banks and financial institutions by granting access to customer data to third-party financial service providers. This enables customers of banks and financial institutions to more easily utilize services provided by third parties, such as financial management and investment services, while ensuring the security of customer data.

B Markets

The market status of open banking for Web 3.0 is still in its early stages but shows promising growth and potential. As Web 3.0 technologies, such as blockchain and decentralized finance (DeFi), gain momentum, there is increasing interest in integrating traditional banking services with these decentralized systems. Currently, several initiatives and projects are exploring the convergence of open banking and Web 3.0. This includes the development of decentralized identity solutions, decentralized lending and borrowing platforms, decentralized exchanges, and cross-chain interoperability protocols.

Furthermore, blockchain platforms like Ethereum are being utilized to create programmable money and smart contract-based financial services, enabling individuals to access and manage their financial assets in a decentralized manner.

While the market is still maturing, the potential benefits of open banking in the Web 3.0 era include enhanced financial inclusivity, improved transparency and security, reduced reliance on intermediaries, and the ability to create innovative financial products and services.

C Targets

The purpose of the section is to outline the specific details of the second-layer Open Banking protocol stack within the Web 3.0 Hong Kong protocol stack.

The primary objective of Open Banking is to encourage data sharing among Account Servicing Payment Service Providers (ASPSPs). It aims to unify Web3 payment standards and achieve security, convenience, and scalability in a decentralized manner. The MMD wallet serves as the core component for connecting various payment channels.

D Protocols

1. Data Sharing Protocol: Customer banking data must be shared with third-party service providers only with the customer's consent. For example, OAuth 2.0 (UK) is an open standard authorization protocol used for authentication and authorization, allowing third-party applications to access a bank customer's data without requiring the customer to provide access passwords.

2. Customer Authentication Protocol: Third-party service providers must authenticate customers through the bank to ensure that only authorized providers can access customer banking data. OpenID Connect (UK) is an example of an authentication protocol that allows third-party applications to access a bank customer's data through a unified authentication and authorization interface.

3. Data Security Protocol: All shared data must be kept confidential, and both banks and third-party service providers must take appropriate security measures to ensure data security. For example, JSON Web Token (JWT) is used for data interchange between banks and third parties, allowing encryption of data by banks and verification of its authenticity. Transport Layer Security (TLS) is a network communication protocol used to ensure secure transmission of data.

4. Technical Standards Protocol: Banks and third-party service providers must comply with applicable technical standards to ensure data security and consistency. APIs (Application Programming Interfaces) provide interfaces for accessing open banking data, allowing third-party service providers to access bank data.

5. Privacy Protection Protocol: Banks and third-party service providers must comply with applicable privacy laws and regulations to ensure the protection of customer privacy.

6. Payment Account Opening Rules: Payment Account Opening Rules are a set of rules designed to provide customers with more choices and facilitate fund transfers and financial management across different banks and payment service providers. These rules require banks and payment service providers to allow third-party applications access to customer payment accounts for managing funds across different channels.

eKYC

A Concepts

eKYC (Electronic Know Your Customer) is an electronic method of customer identification used to verify the true identity of individuals. It is commonly employed in financial transactions as an effective measure to prevent fraud, money laundering, and illicit financial activities. eKYC is conducted through mobile devices or the internet, enabling users to undergo customer identity verification without the need for in-person proof of identity.

B Markets

With the widespread adoption of the internet and mobile payments, eKYC has a promising market outlook. According to data from market research firms, the global eKYC market size reached approximately $2 billion in 2020 and is projected to grow to around $6.8 billion by 2025, with a compound annual growth rate of approximately 27%. Additionally, the market application of eKYC is continuously expanding. For example, during the COVID-19 pandemic, eKYC technology found broader applications in healthcare and other sectors. It is foreseeable that eKYC technology will have even broader application scenarios in the future.

C Targets

The purpose of this section is to outline the specific details of the second-layer eKYC protocol stack within the Web 3.0 Hong Kong protocol stack.

eKYC, as the primary method for virtual digital asset identity verification, plays a crucial role in strictly authenticating customer qualifications, ensuring security, and enforcing Web3 standards in the financial domain. Therefore, it is essential to establish corresponding protocols for eKYC.

D Protocols

1. Identity Verification Protocol:

The Identity Verification Protocol validates the user's identity by verifying the provided identification information to ensure the authenticity and validity of the user's identity. It typically involves a series of steps, including document verification, biometric authentication, and data cross-referencing. The protocol may interact with external identity verification services, government databases, or other trusted sources to validate the user's identity.

2. Data Validation Protocol:

The Data Validation Protocol is responsible for verifying the accuracy and validity of the data provided by the user. It performs various checks, such as format validation, range validation, and consistency checks to ensure that the data meets the required criteria. The protocol may also involve business rules and logic specific to the application or industry to validate the data against predefined standards.

3. Data Storage Protocol:

The Data Storage Protocol handles the secure storage of validated data in a database or storage system. It ensures that the data is stored in a reliable and resilient manner, protecting it from unauthorized access, data corruption, or loss. The protocol may include measures such as data redundancy, backup mechanisms, and encryption at rest to ensure data integrity and availability.

4. Data Encryption Protocol:

The Data Encryption Protocol focuses on encrypting user identity information to ensure data security and confidentiality. It utilizes appropriate encryption algorithms, such as AES (Advanced Encryption Standard), to transform sensitive data into unreadable ciphertext. Encryption keys are used to encrypt and decrypt the data, ensuring that only authorized parties can access the information.

5. Backend Management Protocol:

The Backend Management Protocol is responsible for managing and maintaining data within the system. It includes tasks such as access control, user management, data backups, system monitoring, and performance optimization. The protocol ensures that only authorized personnel can access and manage the backend systems, and it defines procedures for data backups, disaster recovery, and system updates.

6. Authorization Management Protocol:

The Authorization Management Protocol ensures that third parties can access user identity information only after proper authorization. It defines the rules and processes for granting access rights, permissions, and restrictions to external entities requesting user data. The protocol ensures compliance with privacy regulations, includes consent management mechanisms, and provides oversight and auditing capabilities to monitor data access and usage.

7. Communication Protocol:

The Communication Protocol facilitates secure communication between the frontend and backend systems. It ensures that data transmitted between different components or parties is protected from unauthorized interception or tampering. Common communication protocols used include HTTPS (Hypertext Transfer Protocol Secure) and SSL/TLS (Secure Sockets Layer/Transport Layer Security).

8. Protocol Interaction:

Protocol Interaction defines the data exchange standards between banks and third parties to ensure secure and efficient data transmission. It includes specifications for the data format, message structure, and communication protocols used during interactions between different systems. The protocol defines the rules and procedures for initiating, validating, and processing data exchanges, ensuring interoperability and data integrity throughout the interaction.

2.3.3 Creator Economy

A Concepts

The Creator Economy in Web 3.0 refers to the ecosystem where individuals, content creators, artists, and influencers leverage decentralized technologies to monetize their creations and engage directly with their audience.

B Markets

Various Web 3.0 platforms have emerged specifically catering to the needs of creators. These platforms offer features such as NFT creation and trading, decentralized content distribution, direct fan engagement, and monetization options. Creators are exploring these platforms as alternatives to traditional centralized platforms, seeking greater control, ownership, and revenue potential.

The market is witnessing significant experimentation and innovation in the Creator Economy space. Creators, developers, and entrepreneurs are exploring new ways to leverage blockchain, smart contracts, and decentralized platforms to create novel revenue models, content formats, and fan experiences. This experimentation is driving the evolution and expansion of the Creator Economy ecosystem.

C Targets

This section is to illustrate the protocol stack design for creator economy based on blockchain platform.

D Protocols

The protocol stacks for the Creator Economy in Web 3.0 consist of various layers and components that work together to enable the creation, distribution, and monetization of digital content. Here's an illustration of the protocol stacks in Web 3.0 for the Creator Economy:

1. Tokenization Layer:

The tokenization layer involves protocols that enable the creation, management, and trading of digital assets, particularly non-fungible tokens (NFTs). These protocols define the standards and specifications for representing unique digital assets on the blockchain. Notable protocols in this layer include ERC-721 and ERC-1155 for Ethereum-based NFTs, as well as standards like NEP-11 for the NEAR Protocol.

2. Smart Contract Layer:

The smart contract layer consists of the protocols that facilitate the creation and execution of programmable contracts, also known as smart contracts. These contracts enable the automation and enforcement of rules and agreements between creators, consumers, and other participants in the Creator Economy. Ethereum's Solidity language and the EVM (Ethereum Virtual Machine) are prominent components of this layer.

3. Decentralized Finance (DeFi) Layer:

The DeFi layer encompasses protocols that enable financial services and applications within the Creator Economy. These protocols provide functionalities such as decentralized exchanges (DEXs), lending and borrowing platforms, stablecoins, and yield farming mechanisms. Examples include Uniswap, Aave, Compound, and MakerDAO. DeFi protocols offer opportunities for creators to access liquidity, earn interest, and engage in decentralized financial activities.

4. Content Distribution Layer:

The content distribution layer involves protocols that facilitate the decentralized distribution, discovery, and consumption of digital content. These protocols aim to provide alternatives to centralized platforms, ensuring content integrity, censorship resistance, and fair compensation for creators. IPFS, Arweave, and Filecoin are examples of protocols used for decentralized storage and content distribution.

5. Community Management and Governance Layer:

This layer comprises protocols that enable community management, engagement, and governance within the Creator Economy. It includes decentralized autonomous organizations (DAOs) that allow creators and community members to participate in decision-making, fund allocation, and project governance. DAOstack, Colony, and Aragon are notable protocols in this layer.

6. Identity and Reputation Layer:

The identity and reputation layer focuses on protocols that establish and manage digital identities for creators, users, and other participants. These protocols ensure authenticity, reputation tracking, and trust within the Creator Economy ecosystem. Examples include decentralized identity solutions such as uPort, Sovrin, and SelfKey.

2.3.4 DApp

A Concepts

DApp, short for Decentralized Applications, refers to distributed applications built using blockchain technology. These applications operate in a decentralized manner, possessing complete autonomy and independence from any third-party control. DApps utilize open-source protocols and user interactions are facilitated through smart contracts. They provide services in a decentralized manner, which greatly enhances the trustworthiness and security of the system.

B Markets

DApps have found applications in various industries, including finance, gaming, Internet of Things (IoT), healthcare, and more. Among these, blockchain gaming and finance have emerged as the mainstream sectors in the market. According to relevant data, as of December 31, 2019, there were over 6,000 DApps globally, primarily distributed across public blockchains such as Ethereum, EOS, and TRON. Ethereum stands as the largest DApp deployment platform worldwide, hosting over 3,000 DApps.

C Targets

This section is to introduce the protocols related Dapps.

D Protocols

1. Public Chain Protocols:

Public chain protocols are blockchain networks that are open to the public, allowing anyone to participate, validate transactions, and build decentralized applications (dApps) on them. Some prominent public chain protocols include:

- Ethereum: Ethereum is a decentralized, open-source blockchain platform that enables the creation of smart contracts and dApps. It employs a Turing-complete programming language called Solidity and utilizes the Proof of Work (PoW) consensus algorithm, although it is transitioning to Proof of Stake (PoS) with Ethereum 2.0.

- EOS: EOS is a blockchain platform designed for high scalability and performance. It aims to provide a user-friendly environment for developers to create dApps with features like parallel processing and delegated proof of stake (DPoS) consensus, where block producers are elected to validate transactions.

- TRON: TRON is a blockchain platform that focuses on the entertainment industry, allowing developers to build and deploy dApps for content sharing and distribution. It employs a delegated proof of stake (DPoS) consensus algorithm for transaction validation.

These public chain protocols provide a decentralized and transparent infrastructure for various applications, including decentralized finance (DeFi), gaming, supply chain management, and more.

2. Mining Types:

Mining is the process of validating transactions and adding them to the blockchain. It involves solving complex mathematical puzzles to secure the network and maintain consensus. Two primary mining types are widely used:

- Proof of Work (PoW): PoW is the original mining algorithm used by Bitcoin and many other cryptocurrencies. Miners compete to solve cryptographic puzzles, and the first miner to find a valid solution is rewarded with newly minted coins. PoW requires significant computational power and energy consumption.

- Proof of Stake (PoS): PoS is an alternative consensus mechanism where validators are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral. It eliminates the need for resource-intensive mining and reduces energy consumption. Validators are chosen randomly or in a deterministic manner, depending on the specific PoS implementation.

PoS aims to provide a more energy-efficient and scalable alternative to PoW. It is being adopted by various blockchain networks, including Ethereum, as part of their network upgrades.

Both mining types contribute to the security and integrity of blockchain networks and play a crucial role in achieving consensus among network participants to validate transactions and maintain the blockchain's immutability.

3. HK Web 3.0 Protocols

3.1 HK Open Blockchain Infra

3.1.1 Overview

HK Open Blockchain adopts an advanced modular and layered architecture design concept, sharing security, layered execution, and sharding storage, making each core module of the system highly scalable. Which also supports security and privacy through a built-in security mechanism like linux kernel design, using advanced cryptographic techniques such as secure multi-party computation and zero-knowledge proof to ensure that user assets and data are fully protected. In addition, it adopts a full-stack composable design concept, natively supporting cross-chain interoperability protocols, to achieve reliable connection and interaction between different blockchains and different protocol layers; compatible with the EVM virtual machine, fully compatible with most existing DAPP protocols.

Here is a more detailed explanation of the key features:

Layered Modularity

In response to the problem that the native scalability of mainstream blockchains is weak and the performance cannot support real financial scenarios, HK Open Blockchain adopts the concept of layered expansion and proposes a modular and layered innovative architecture consisting of settlement layer、execution layer and data availability layer. Through shared security, layered execution, and sharding storage, it ensures that the key services of blockchain infrastructure all have independent scalability capabilities.

Full stack composability

In response to the challenges of cross-chain difficulty and liquidity fragmentation between heterogeneous blockchains, HK Open Blockchain has been committed to building a natively composable blockchain infrastructure from the very beginning. It provides modular design and trusted cross-chain interoperability support from multiple levels, including contracts, systems, and protocols: At the contract level, it provides a runtime environment similar to the Ethereum virtual machine, which can seamlessly migrate DApps from the existing Ethereum ecosystem. At the system level, which achieves decoupling of the ledger layer, execution layer, and storage layer through layered design. This modular architecture not only improves scalability, but also allows different functional units on the chain to be combined as needed. At the underlying protocol level, HK Open Blockchain supports cross-chain interoperability between

heterogeneous chains and between different modules within the chain. This provides the foundation for cross-chain flow of assets and cross-chain invocation of DApps.

Security First

In response to the frequent occurrence of security issues at multiple levels, such as smart contract, cross-chain, and compiler vulnerabilities, HK Open Blockchain considers security from both economic and technical perspectives. By adopting a multi-layer, comprehensive protection endogenous (system) security mechanism, it designs a general security kernel and application layer security extension slot to provide basic protocol security and business customized security capabilities.

Verifiable Privacy

Currently, mainstream public chains are difficult to guarantee privacy due to the complete openness of data, while private chains have the problem of being unfriendly to regulation, and have gradually become a breeding ground for illegal activities. In order to balance privacy and compliance, HK Open Blockchain has launched a "verifiable privacy" technical solution. This solution uses a combination of secure multi-party computing, hierarchical architecture design, and transaction obfuscation techniques. By splitting and encrypting privacy data, it protects user information while also allowing regulators to perform necessary on-chain data verification, achieving a win-win situation for privacy protection and regulatory compliance.

3.1.2 Architecture

The HK Open Blockchain node consists of the following four types of roles:

Ledger

The core ledger layer is mainly used to achieve the purpose of shared security and is mainly used for asset issuance, transaction and settlement, and execution verification of layered services. Ensure the security of the entire architecture through large-scale decentralized nodes and robust consensus algorithms.

Base

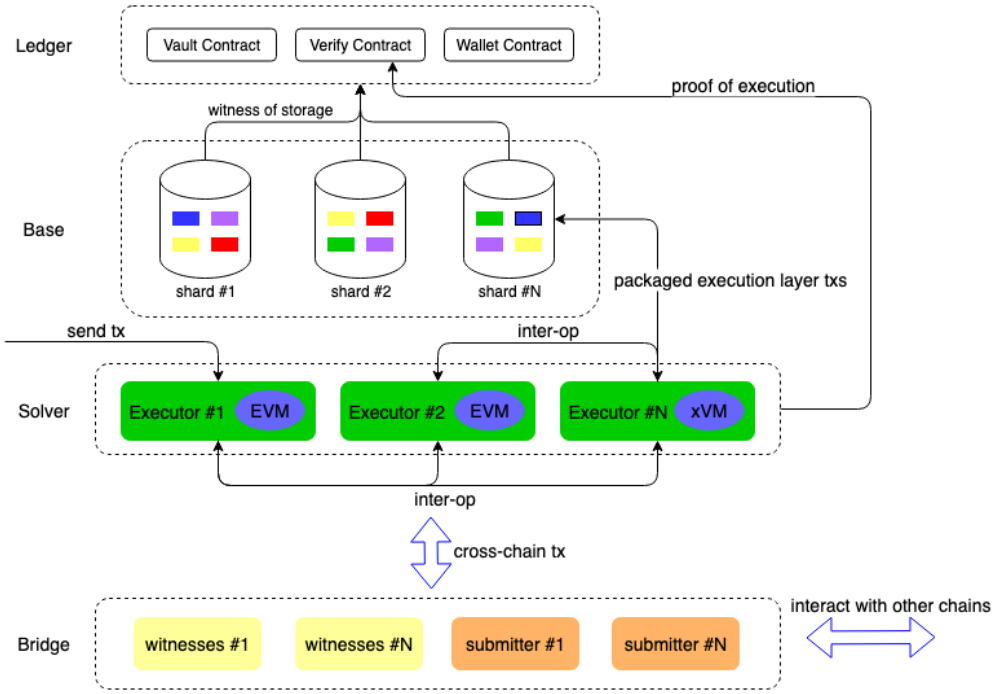
The data availability layer, mainly used to ensure the data availability of the execution layer. It uses data sampling, zero-knowledge proof and other technologies to store proof information and status change data from the execution layer.

Solver

Business execution layer, mainly used to improve execution efficiency, and execute specific businesses in parallel through EVM-compatible executors. At the same time, due to layered execution, special services such as privacy protection and native execution can also be provided.

Bridge

Cross-chain layer, mainly used for cross-chain transfer of assets and cross-chain messages. HK Open Blockchain natively supports cross-chain component communication and rapid verification, ensuring the security and credibility of the cross-chain process. At the same time, the cross-chain layer includes various roles such as challengers, submitters, witnesses, etc. to ensure the security of the cross-chain transaction process.



3.1.3 Key Components

Consensus

The consensus component serves as the settlement layer to ensure the security of the system. This layer protocol adopts asynchronous Byzantine consensus algorithm, asset-oriented smart contract engine, efficient and flexible storage, hardware acceleration and other technologies to improve its scalability.

Executor

The execution component is composed of multiple executors (EVM and other VM), and distributes the execution logic of the business to each executor. The execution layer uses a zero-knowledge proof mechanism to only submit the necessary verification information to the settlement layer, and can pass the business design and optimize using specific optimization methods. The scale of a single business node is controllable. Different businesses can use different execution layers for parallel execution to achieve linear expansion.

Governance

The governance component realizes native governance capabilities through system contracts, which improve governance efficiency through the combination of on-chain and off-chain governance, allowing community members to more conveniently conduct governance and supervision, ensuring the security and stability of the network.

Storage

The storage component uses a sharded storage engine to store only key data from each execution layer, such as transaction history and status changes. Cryptographic commitments, data compression, and hardware acceleration are used to ensure the security of stored data. Besides, technologies such as zero-knowledge proofs and erasure coding are used to avoid full-network storage.

Cross-layer Channel

Cross-layer channels are a native hierarchical extension component of HK Open Blockchain, used to support trusted communication between different layer components of HK Open Blockchain, such as between L1 and L2, and between L2 and L2, etc.

Cross-chain Channel

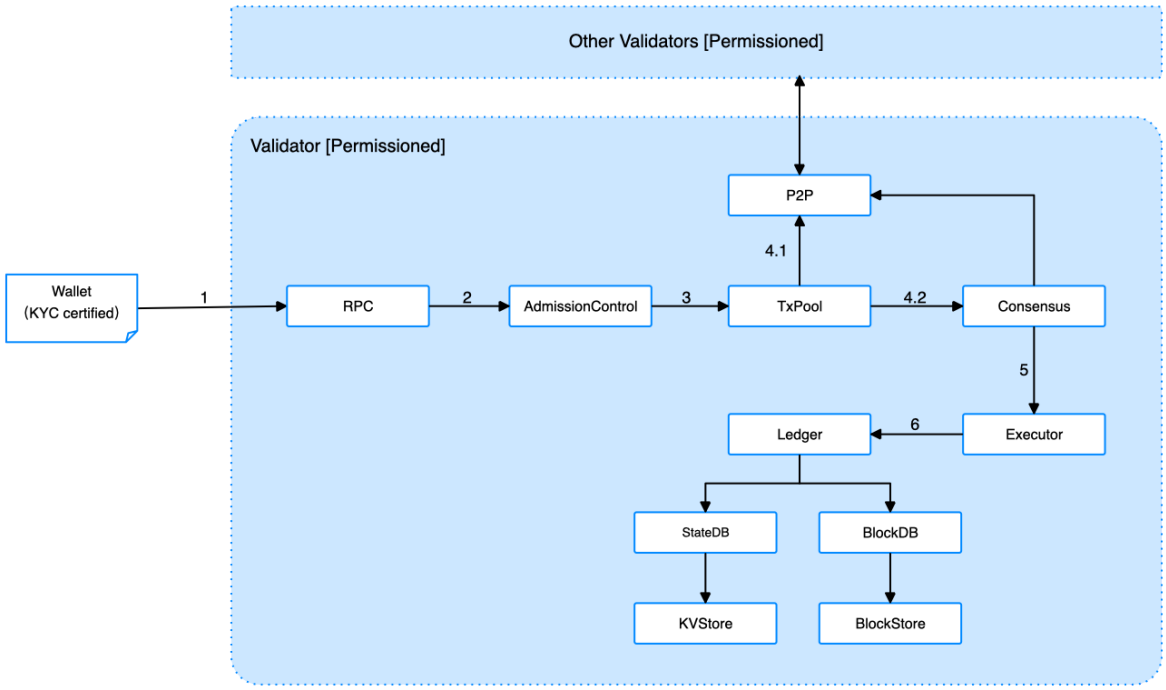
The cross-chain channel of the HK Open Blockchain facilitates communication and interoperability with other blockchains. It is primarily divided into three layers: the protocol layer, the transmission layer, and the data layer. The protocol layer encapsulates interfaces for cross-chain operations involving blockchain assets, blockchain messages, and protocol governance-related operations. The transmission layer converts cross-chain messages from each chain into standardized, universal cross-chain data packets and facilitates trusted transmission through distributed off-chain nodes. Finally, the data layer preserves cross-chain-related data, ensuring the reliability and sequence of cross-chain messages.

3.1.4 Workflow

The core processes of internal transactions on HK Open Blockchain are divided into three categories: ledger layer transactions, full-layer transactions, and cross-chain transactions.

3.1.4.1 Ledger Layer Transactions

One way for users to interact with HK Open Blockchain is by sending transactions to the settlement layer component Ledger. The diagram below illustrates the processing flow of a transaction within the settlement layer component Ledger of HK Open Blockchain:



1. Prepare wallet account: Some preparation work needs to be done before sending a transaction. The account used to send a transaction to the DAPP may need to be certified on the official HK Open Blockchain KYC platform, and the account must hold a certain amount of chain tokens to be able to pay for the gas fees.

2. Submit transaction: End users can directly construct raw blockchain transactions via a wallet (e.g. MetaMask) or a DAPP, then sign it with a private key (usually also done with the help of a wallet) and send it to HK Open Blockchain validators.

3. Receive transaction: The RPC interface module of Ledger nodes is responsible for receiving transaction requests submitted by end users. To be compatible with the Ethereum ecosystem, HK Open Blockchain implements most Ethereum RPC interface specifications, while also providing additional customized governance service interfaces. To prevent DoS attacks, the RPC interface module has flow control capabilities. When transaction requests exceed the system processing limit, the request will be rejected directly; transactions within the processing capability will be forwarded to the internal access control service for subsequent processing.

4. Validate transaction: The access control component will validate the security of the submitted transactions, mainly including validity checks on the transactions themselves and may conclude

KYC checks on the signing addresses of the transactions. Illegal transactions that fail validation are discarded directly, while valid transactions are cached in the transaction pool pending packaging.

5. Consensus on transaction: For transactions entering the transaction pool, Ledger node will perform two operations: 1) Forward the transaction to neighboring nodes in the blockchain network via the network service; 2) If the validation node is the primary node of the consensus nodes, it will periodically take out batches of transactions from the transaction pool and initiate consensus proposals. After that, the consensus algorithm executes multiple rounds of consensus steps to make most validation nodes in the network agree on the order of the batch of transactions.

6. Execute transaction: Batch transactions (blocks) confirmed by the consensus algorithm will be input into the executor for execution. Executor invokes different executors to process transactions based on the transaction type. System contracts are invoked to process system transactions, while the EVM virtual machine is invoked to process ordinary transactions. After executing the transactions, the changes to the ledger world state are generated, and the executor sends the world state changes along with the block to the ledger module.

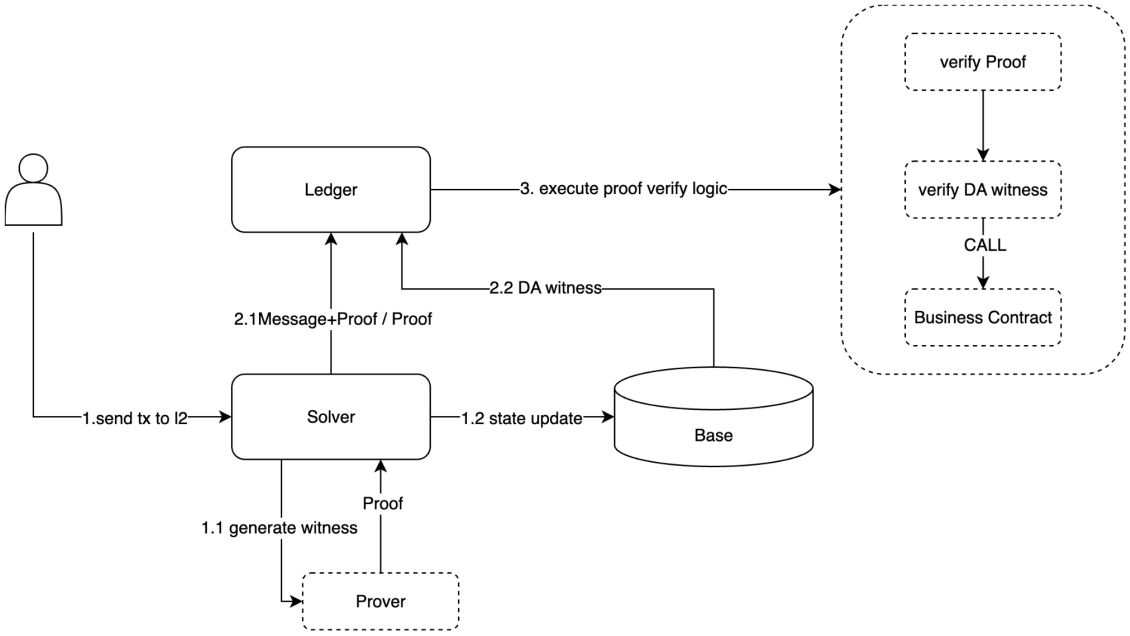
7. Persist state: According to the different data types of the changes, the ledger module invokes different underlying storage engines to store the data. World state changes are persisted via the underlying KV database, while block data is stored using the underlying sequential database.

3.1.4.2 Full layer transactions

Instead of directly interacting with the settlement layer component Ledger of HK Open Blockchain, users can send transactions directly to the execution layer component (Solver) of HK Open Blockchain for processing to achieve lower confirmation latency and higher processing performance. The diagram below illustrates the processing flow of a transaction within the execution layer component Solver of HK Open Blockchain, as well as the process of reaching final transaction confirmation through interactions between layers:

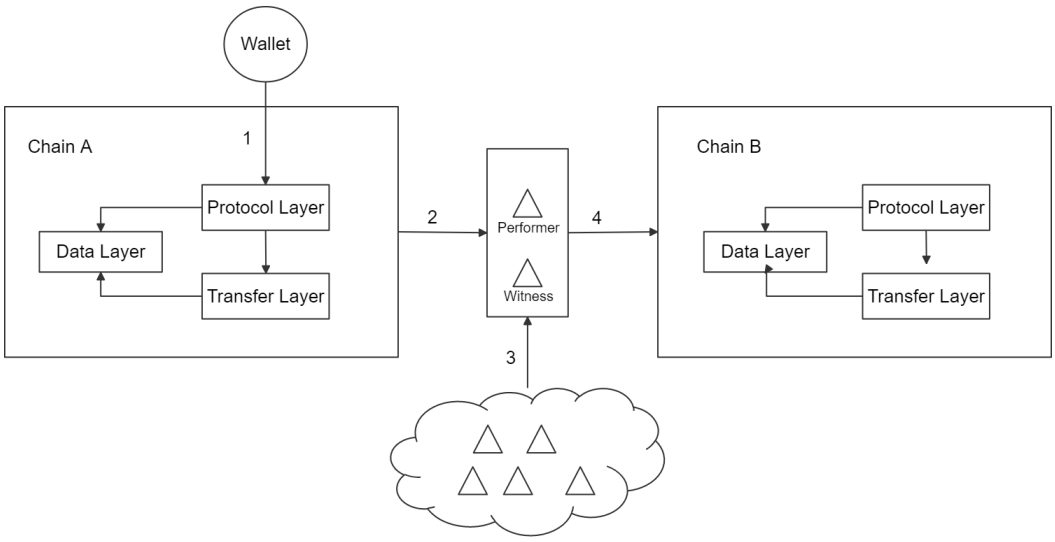
1. Consistent with the direct interaction flow with the consensus layer Ledger described above, users need to prepare a private key that can be used to send transactions in advance. After the user signs the transaction with the private key, the transaction is sent to a Solver in HK Open Blockchain:
   a. After receiving the transaction, Solver executes the transaction using the corresponding virtual machine (EVM, zkEVM...) and then submits the execution intermediary information to the execution proof service Prover.
   b. Prover generates an execution Proof, then sends the execution Proof back to Solver, which submits the execution Proof to Ledger.
   c. Solver submits state changes/transaction lists to the data availability service Base. Base stores these state data on demand and generates storage proofs (witnesses).

2. Solver periodically submits execution Proofs to Ledger, and Base periodically submits storage proofs (witnesses) to Ledger.
3. Ledger verifies the transaction execution Proofs and data availability proofs (witnesses), to finalize the transactions. If there are calls to business contracts, the related business contracts are invoked.



3.1.4.3 Cross-chain transactions

For users, wishing to access other blockchains from the HK Open Blockchain or wanting to access the HK Open Blockchain through other blockchains, the following process can be followed to achieve this:



1. First, the user needs to have a wallet capable of interacting with blockchains. Through the wallet, users can use the cross-chain protocol layer of the HK Open Blockchain to send cross-chain transactions, including assets and messages. Users can also generically call contracts or applications on the chain that have already used cross-chain interfaces to initiate cross-chain transactions.

2. After passing through the protocol layer, transactions are wrapped and events are emitted by contracts in the transmission layer. The protocol layer handles the logical operations of cross-chain transactions and related fee collection, while the transmission layer is primarily responsible for the transmission of cross-chain transactions, ensuring that transaction packages are accurate, error-free, and executed strictly in order.

3. In the off-chain environment, distributed relay nodes receive cross-chain events emitted by the source chain. These distributed relay nodes are divided into three roles based on the consensus of both the source and target blockchains: Witnesses, Performers, and Challengers. Performers send the cross-chain transaction package and its proofs to the target chain, Witnesses send credentials verifying the proofs to the target chain, and Challengers oversee the credentials submitted by Witnesses to ensure that malicious behavior does not occur.

4. After receiving the transaction submitted by the executor, the transmission layer of the target chain compares the proofs included in it with the credentials submitted by the witnesses. If the verification is successful, it confirms that the transaction is valid and reliable. Subsequently, the transmission layer submits the transaction to the protocol layer to execute the necessary cross-chain operations on the target chain.

3.1.5 Economics

To incentivize node operators to provide better service quality and maintain a more robust blockchain system, HK Open Blockchain natively supports a token settlement system, and combines an advanced service quality evaluation system with a dynamic gas fee adjustment mechanism to achieve a stable and robust economic model.

3.1.5.1 Native Token

HK Open Blockchain's native token plays multiple important roles, including payment, incentive, and governance. When users interact with the HK Open Blockchain, they need to use the native token to pay, and the specific amount of payment will be determined by the blockchain's unique dynamic gas fee adjustment mechanism. In addition, validators will also be rewarded with native tokens after successfully proposing blocks, and the number of tokens they hold will directly affect their income. In addition, only users holding native tokens are eligible to vote on key blockchain decisions, and the number of tokens they hold will determine their weight in the vote.

3.1.5.2 Gas price

Gas is the unit of payment for services on HK Open Blockchain. To prevent DDoS attacks, reduce the storage pressure on the chain, and ensure the stable operation of the system during network peaks, we have designed a dynamic gas price adjustment mechanism based on the supply and demand relationship of the network. When the gas limit of a block is used more than 50%, the gas price will be increased, and vice versa.

Algorithm 1 Gas price automatic adjustment

Require: G_i is the initial gas price, G_c is current price, G_p is parent block price, U_p is the transactions used percentage

Ensure: given G_p and U_p, return G_c

if Genesis block **then return** $G_c = G_i$

end if

$G_c = G_p * (1 + (U_p - 50\%) \times 2 \times 12.5\%)$

3.1.5.3 Income Distribution

The potential income of node operators mainly comes from gas fees, which are closely related to the quality of service provided by the node during operation and the number of native tokens held. More specifically, the gas fee income generated by each block belongs to the block-producing node. However, the selection rules for block producers are directly affected by the quality of service provided by node operators during operation and the number of native tokens held.

At the same time, node operators also have the opportunity to participate in derivative services composed of native tokens and obtain income from related financial activities. For example, node operators can inject liquidity into the native token, thereby obtaining corresponding economic returns.

This diversified potential income method not only allows node operators to obtain gas fees through the provision of high-quality services, but also allows them to actively participate in financial activities in the ecosystem, providing them with more opportunities and motivation for their participation in the HK Open Blockchain.

3.1.5.4 Service quality assessment

The HK Open Blockchain will continuously evaluate the service quality of network nodes. When problems such as network instability, malicious block production, and delayed work occur during the operation of a node, The economic engine module will dynamically reduce its block production probability, thereby reducing its gas income. If service quality problems occur multiple times in a period of time, the corresponding punishment mechanism will be triggered.

3.1.6 Foundation

In order to ensure the long-term and healthy development of HK Open Blockchain, it is recommended to establish a non-profit foundation jointly organized by the Hong Kong Web 3.0 Association, universities, research institutions, and large enterprises. The mission of the foundation is to promote the global development of HK Open Blockchain, a digital financial infrastructure, and to make it an important support tool for the financial and social system. It will also provide support and encouragement to the HK Open Blockchain community, and assist the community in developing tools that can solve problems in new ways. This will make a positive contribution to the long-term development and widespread application of HK Open Blockchain. Foundation will work hand in hand with the community to promote the development of blockchain technology, and provide more efficient, secure, and transparent solutions for the financial and social system.

Governance

HK Open Blockchain composed of nodes from multiple organizations. Since the participants do not fully trust each other and there are objectively existing conflicts of interest and differences in ideas, there will inevitably be disagreements and disputes, which need to be resolved through governance to reach a consensus.Any individual or organization with the hardware requirements to run an HK Open Blockchain node can apply to become a node operator and participate in the HK Open Blockchain governance process in the future.

Under the guidance of the foundation, node operators first jointly elect a governance committee, which includes a technical committee and a comprehensive business committee. The governance committee is responsible for the actual governance of the blockchain network. Among them, the technical committee is responsible for technical governance, such as version upgrades, bug fixes, and smart contract reviews. The technical committee makes decisions through meetings and consultations off-chain, and then proposes proposals on-chain for committee members to vote on. Only when the vote meets certain conditions, the proposal will be accepted and synchronized to all blockchain nodes, and the nodes will automatically execute

the corresponding proposal. The comprehensive business committee is responsible for matters other than technology, including compliance checks, marketing, and economic mechanisms.

Through the mechanism of governance committee proxy governance, HK Open Blockchain ensures the perfect balance between the fairness of blockchain members' participation in governance and the efficiency in the distributed governance process.

3.2 Digital Assets over HK Chain

3.2.1 Overview

Digital assets refer to assets that exist in digital form and have economic value. With the widespread adoption and continuous development of blockchain technology, the types and applications of digital assets are constantly expanding. The most well-known category is cryptocurrency, which can be broadly classified into two types: native coins and tokens. These cryptocurrencies ensure the security and anonymity of digital currency through blockchain mainnets and cryptographic algorithms. Examples of native coins include BTC and ETH, which have their own blockchain networks, while tokens such as UNI, AAVE, and DAI are built on the Ethereum ERC20 standard. The ERC20 protocol was established in 2015 and officially standardized by September 2017. The protocol defines a set of basic interfaces for fungible tokens, including token symbols, supply, transfer, authorization, etc. Developers can create, deploy, and manage these tokens more easily. As a result, the development process for project tokens becomes more standardized and streamlined, lowering the entry barrier and improving the security and quality of token contracts. It also enables interoperability among different tokens on the Ethereum network. This means that tokens compliant with the ERC-20 standard can be easily exchanged, transferred, and traded within the Ethereum ecosystem. Various wallets, exchanges, and smart contracts can support these tokens, facilitating fast and convenient cross-border payments worldwide. This has led to the emergence of innovative financial applications and business models such as decentralized finance (DeFi) and Flash Loans.

Non-fungible tokens (NFTs) are another category of unique digital assets. Each NFT represents a specific item or artwork and can include art, music, in-game items, and more. Successful applications in areas such as provenance tracking and copyright protection have further driven the development of digital assets. This has given rise to personalized digital avatars with unique characteristics in the metaverse. These digital representations can be used in gaming, virtual social interactions, virtual reality, and other fields, thereby expanding the realm of unique digital assets within the metaverse.

The integration of traditional assets with blockchain has given rise to a new track known as Real World Assets (RWA). Real-world assets, such as real estate, equities, and bonds, which possess tangible value in the physical world, can now be digitized and tokenized through

blockchain technology. This enables more accurate and efficient recording of digital ownership of real assets, eliminates the need for central intermediaries in the transfer and storage of digital assets, and maps the value onto the blockchain. As a result, traditional financial markets can benefit from increased liquidity and reduced transaction costs while also providing more investment opportunities. In particular, Especially for DeFi, the digitization of RWA can provide more asset types for DeFi and expand the market size of DeFi.

HK Open Blockchain is committed to building a next-generation Web 3.0 blockchain empowerment platform for digital assets. With a multi-tiered, modular architecture, it constructs a native, composable blockchain infrastructure at various levels including contracts, systems, protocols, and cross-chain interoperability. This comprehensive framework provides support and protection for the issuance, management, and application scenarios of different digital assets by users.

3.2.2 Key Digital Asset Protocol

As an Ethereum equivalent blockchain, HK Open Blockchain natively supports standardized asset types compatible with Ethereum. In this chapter, we will explain the digital asset issuance standards supported on HK Open Blockchain and provide examples of typical use cases.

Fungible Token

Fungible Tokens originated from the advent of Bitcoin as a divisible and interchangeable digital asset. Bitcoin itself is a type of fungible token that can be divided into smaller units of equal value. However, with the development of the Ethereum platform, developers began creating various fungible tokens with different functionalities and purposes. The most common ones are tokens representing digital currencies like stablecoins such as USDT and DAI, which are pegged to fiat currencies. Fungible tokens are also used in crowdfunding (ICO), reward programs, gaming assets, and loyalty point systems. They play a significant role in the encrypted economy, providing an efficient, secure, and trusted way to create, trade, and facilitate the flow of digital assets. HongKong Blockchain supports the following standard protocols for FT (Fungible Token) digital assets.

HRC20

HRC20 is the foundational protocol for fungible tokens on HongKong Blockchain, similar to Ethereum's ERC20 protocol. It supports basic operations such as token transfer, authorization, and balance inquiry. From a user perspective, HRC20 functions as a unit of measurement on HongKong Blockchain. It can represent credit scores within the platform, application points, bank balances, or even company equity.
Tokens like UNI and MKR, which are well-known, are typical examples of ERC20 assets issued on the Ethereum network. Users can trade these tokens on centralized digital asset exchanges

such as Binance and Coinbase, or on decentralized exchanges like Uniswap and Curve. This facilitates token interoperability and broad application.

HRC777

HRC777 is another important protocol for fungible tokens on the HongKong Blockchain, equivalent to Ethereum's ERC777 protocol. It supports user programming of tokens. Initially, for security considerations, HRC20 required users to authorize applications before making payments through third-party software. However, this usage method increased user complexity and transaction fees. To solve this problem, HRC777 allows users to program their own tokens. For example, users can create whitelists or blacklists of approved users, eliminating the need for software authorization every time they use the tokens. This programmable approach greatly improves the usability and flexibility of tokens.

Non-Fungible Token

Non-fungible tokens (NFTs) are unique and non-replaceable digital assets. Each NFT has a unique identifier and metadata that record its creator, owner, history, and other relevant information. These pieces of information are stored on the blockchain, creating an immutable and verifiable record. Initially, NFTs were primarily used in the field of digital art and collectibles, such as CryptoKitties, CryptoPunks, Beeple, and others. These NFTs allow for a direct and secure connection between digital artists and collectors, enabling them to better express and appreciate their creations. Moreover, NFTs provide a new paradigm for asset verification, ownership transfer, the creator economy, and decentralized identity in the digital world. The HongKong Blockchain supports the following standard NFT digital asset protocols.

HRC721

HRC721 is the foundational protocol for non-fungible tokens (NFTs) on the HongKong blockchain, equivalent to Ethereum's ERC721 protocol. It enables basic operations such as token transfer, authorization, and balance inquiry. From a user's perspective, HRC721 tokens can represent unique and indivisible assets, such as collectibles, lottery tickets, contracts, and agreements. The HRC721 standard ensures the uniqueness of assets by assigning a distinct TokenID to each token.
In Ethereum, projects like Bored Ape Yacht Club and Azuki are widely recognized NFT initiatives. Users can purchase or sell their NFT assets on decentralized exchanges such as Opensea and Rarible.

HRC1155

HRC1155 is another important token protocol on the HongKong blockchain, equivalent to Ethereum's ERC1155 protocol. It allows for the mixing of both fungible and non-fungible tokens. As the blockchain ecosystem continues to grow, many software platforms require not just HRC20 assets but also HRC721 assets. Deploying a separate contract for each type of asset

would undoubtedly increase development costs, usage costs, and add burden to the blockchain. Therefore, HRC1155 provides a mixed protocol that allows for both HRC20 and HRC721 support within a single contract. This mixed protocol significantly improves token usability and flexibility while lowering costs.

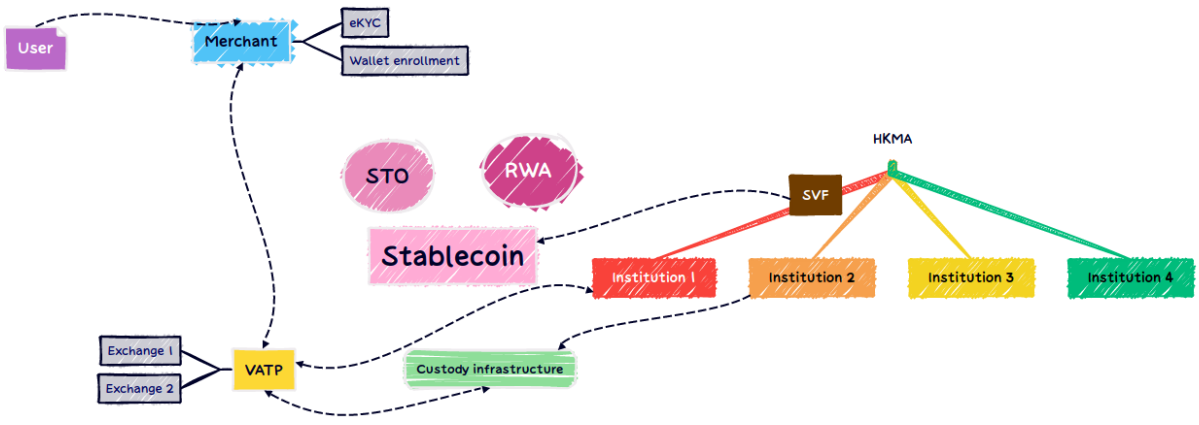
3.2.3 Key Digital Assets

Stable coin

In order to allow users to enter the blockchain world more conveniently, there needs to be a connecting medium between real-world currencies and tokens in the blockchain world, and this medium is what we call stablecoins. Usually, stablecoins are anchored to a certain legal currency or precious metal, such as the U.S. dollar or gold. Such anchoring makes its value highly stable. Of course, there are also some algorithmic stablecoins that use economic models and cryptography technologies. To protect the value of stablecoins. The USDT issuance of Tether, a well-known stable currency project, has exceeded 80 billion US dollars.

RWA

RWA, which stands for Real World Asset Tokenization, is the process of converting the value of tangible or intangible assets, along with any associated rights, into digital tokens. This enables the digital ownership, transfer, and storage of assets without the need for a central intermediary. The value is mapped onto the blockchain and can be traded. Unlike stablecoins, RWA's anchoring medium is not limited to currency but encompasses all tangible assets in real life, such as real estate, insurance, and artwork.



3.3 Stablecoin- RWA

The development of Web3.0 in Hong Kong should integrate both virtual and real scenarios, utilizing blockchain technology to provide new paths for the digitization and tokenization of Real World Assets (RWAs) such as stablecoins, bonds, private loans, trade finance, real estate, carbon credit certificates, and precious metals. This approach promotes the fusion of the virtual economy and physical assets. The digitization and tokenization of RWAs inject liquidity, diversity, and stability into the real economy, expand the categories of assets, and increase the scale of funds. The introduction of blockchain technology breaks the constraints of the traditional financial system, enabling assets to be digitized and unique, narrowing the distance between traditional finance and new finance, meeting users' personalized financial needs, and thereby creating more value and returns. To better understand and study the tokenization of real-world assets, Thomas Zhu innovatively summarized a "RWA 2+4" research methodology, including two types of tokens (security tokens and utility tokens) and four cores (legal regulation, financial framework, technical tools and data application).

Firstly, security tokens represent the ownership or profit rights of assets or enterprises, and their value is usually directly related to the performance of the assets or enterprises they represent. Buyers of this type of token usually expect to get returns through asset appreciation or profit distribution. On the other hand, utility tokens provide the right to use a service or resource and put the data generated in the token process on the chain. Understanding the characteristics and differences of these two tokens is crucial for correctly evaluating and investing in RWAs. In September 2022, a study by the Boston Consulting Group (BCG) estimated that the scale of tokenized real-world assets would reach 16 trillion US dollars by 2030[1]. Coincidentally, in March 2023, Citibank released a hefty 162-page report[2] fully explaining the specific path to achieving a billion users and tens of trillions of dollars in digital assets in Web3.0. Citibank believes that by 2030 there will be 4 to 5 trillion US dollars of tokenized real-world assets, and blockchain-based trade finance transaction volume will reach 1 trillion US dollars. The report believes that almost anything of value can be tokenized, and the tokenization of financial and real-world assets could be the "killer application" for blockchain to achieve a breakthrough.

[1] https://www.bcg.com/publications/2022/relevance-of-on-chain-asset-tokenization
[2] https://icg.citi.com/icghome/what-we-think/citigps/insights/money-tokens-and-games

Secondly, we need to focus on four core aspects: legal regulation, financial framework, technological tools, and data application.

Law is the foundation of RWA, determining what assets can be tokenized and the rules to be followed in the tokenization process. As a global financial center, Hong Kong has a comprehensive securities law system and unique advantages to promote compliant Security Token Offering (STO). Firstly, Hong Kong's Securities Ordinance comprehensively regulates the issuance and circulation of all types of securities assets such as stocks and bonds. The financial assets that RWA needs to tokenize, such as stocks, bonds, and funds, have clear legal definitions in the Hong Kong market. Secondly, the Hong Kong Securities and Futures Commission (SFC) has established comprehensive standards for securities issuance and listing review. RWA STO needs to link assets such as equity and debt of enterprises, these underlying assets need to comply with the SFC's disclosure and approval provisions to ensure quality. This provides RWA with a standardized choice of base assets. Finally, Hong Kong has established a strict investor suitability management system. The STO of RWA can choose to issue to qualified investors or ordinary investors based on the complexity of the underlying assets, preventing ordinary investors from buying complex and high-risk RWA products. Overall, the legal system of the Hong Kong securities market provides institutional guarantees for the steady development of RWA business.

Financial framework of RWA defines the specific structure of asset tokenization and trading. This includes asset evaluation, audit and confirmation of rights, token issuance and trading, and related risk management, among others. Hong Kong has rich experience and world-leading scale in debt and equity financing. Hong Kong's investment banks and audit institutions can provide professional valuation and audit services for RWA's underlying assets, determine the quality and clear ownership of assets, and provide a foundation for token issuance. Hong Kong's compliant licensed virtual asset trading platforms can ensure that RWA tokens are issued and traded publicly and fairly. The professionalism and rich experience of the Hong Kong financial system has built an effective financial framework to ensure the fairness and transparency of the tokenization and trading of real assets, enabling the tokenization business of RWA to be regulated and healthily developed.

Technology is the tool for RWA, providing the technological means to achieve tokenization and trading. This includes blockchain technology, smart contract technology, oracles, cross-chain,

and related security and privacy protection technologies, etc. Since Hong Kong issued the virtual asset development policy statement on October 31, 2022, excellent blockchain technology companies from around the world have been actively setting up in Hong Kong. On September 19, 2023, at the "2023 Shanghai Blockchain International Week·9th Global Blockchain Summit," Peter Yan, the CEO of Hong Kong Cyberport Management Co., Ltd., stated that Cyberport now has more than 190 Web 3.0 related companies, including very important underlying blockchain infrastructure companies and enterprises. Such as zCloak, a digital identity and privacy computing infrastructure company, and Safeheron, a professional digital asset custody solution provider.

Data is the driver of RWA, which can provide important information about assets and markets, supporting investment decisions and market analysis. The new investment method of RWA tokenization not only provides investors with a wider range of investment choices but also brings a wealth of data and information to the market, such as transaction data and user behavior data, etc. These data form a powerful driving force, greatly enhancing the ability of asset operators and investors to understand market dynamics, predict market trends, manage investment risks, etc. However, the scale and complexity of this data also pose challenges to data management and application. Traditional data processing and analysis methods are often unable to cope with this situation, which is where data analysis and artificial intelligence technology come into play. In June 2023, the National Internet Information Office and the Innovation, Technology, and Industrial Bureau of the Hong Kong Special Administrative Region Government signed a Memorandum of Understanding on Promoting Cross-border Data Flow in the Guangdong-Hong Kong-Macao Greater Bay Area (hereinafter referred to as the "Memorandum"). "Signing the Memorandum of Cooperation on Cross-border Data Flow in the Guangdong-Hong Kong-Macao Greater Bay Area on the occasion of the 26th anniversary of Hong Kong's return to the motherland is conducive to strengthening cross-border data flow between the mainland and Hong Kong, fully leveraging the basic role of data, promoting the innovative development of the digital economy in the Guangdong-Hong Kong-Macao Greater Bay Area, and supporting Hong Kong to better integrate into the national development strategy." The National Internet Information Office posted related news on its official website.

In summary, the "RWA 2+4" research method summarized by the author provides a comprehensive framework for the combination of virtual and real in Hong Kong's Web3.0, helping everyone understand and study RWA from different angles. Through this framework,

everyone can better understand the mechanism of RWA, assess the value of RWA, and discover the opportunities and challenges of RWA.

As one of the pioneers and most successful fields in the digitization of RWA, stablecoins have successfully integrated the convenience of digital assets with the stability of mainstream financial assets. They act as a measure of value for digital asset transactions, providing a "gateway" and "safe harbor" for digital asset investors, and are playing an increasingly important role in the international payment system in the real world. Moreover, stablecoins are a key foundation for the tokenization of RWA, and the advancement of RWA tokenization will also provide more diversified value support and reserve sources for stablecoins. Therefore, stablecoins have become a bridge linking digital assets and mainstream financial systems. At present, digital assets such as Bitcoin and Ethereum have been gradually recognized as having characteristics of value storage and hedging assets, but these types of assets have large price volatility and cannot realize monetary functions such as a measure of value, medium of exchange, and payment method, so they are difficult to use in payment scenarios. While stablecoins have advantages such as programmability and decentralization, they also have solid value support to make the market price more stable, playing the role of currency in the digital world.

As an international financial center and a global Web3.0 development center, Hong Kong should accelerate the release of the Hong Kong dollar stablecoin regulation and license framework. The author believes that Hong Kong can refer to the stablecoin regulations of the European Union and Singapore. The EU bill is the "Markets in Crypto-Assets Regulation (MiCA)[3]" and Singapore's stablecoin framework is the "Response to Public Consultation on Proposed Regulatory Approach for Stablecoin-related Activities" by Monetary Authority of Singapore (MAS)[4]. As the world's first relatively complete stablecoin regulatory schemes, they have made provisions for the issuance, circulation, capital/own equity regulation, reserve management, information disclosure regulation, consumer protection, etc. of stablecoins, but there are certain differences in regulatory concepts and specific regulatory requirements between the two. Both of them mostly refer to the existing financial regulatory system. But MiCA has more regulatory restrictions, and the MAS stablecoin framework is relatively more open and flexible. Specifically, MiCA only allows stablecoins pegged to the euro, and they must be issued by credit institutions;

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114

[4] https://www.mas.gov.sg/publications/consultations/2022/consultation-paper-on-proposed-regulatory-approach-for-stablecoin-related-activities

the Singapore framework allows multiple major currencies as pegging objects, and the issuing entity can also be a non-banking institution approved. In terms of reserve management, MiCA has more requirements for the range and composition of reserve assets, and the requirements of the MAS framework are more principled and flexible. In addition, MiCA has clear regulations on the governance, operation and risk management of stablecoins, and the MAS framework is relatively more principled. But both of them have made clear requirements in terms of consumer protection and monitoring of the stability of stablecoins themselves. It can be seen that although the two have different regulatory concepts, they are both actively promoting the construction of the global stablecoin regulatory framework, providing beneficial exploration and reference for the Hong Kong stablecoin framework.

Here is a summary of the risks in stablecoin operations:

- Native Issuer Risk： The primary risk faced by native issuers stems from insufficient collateral assets. For any form of collateralized stablecoin, it is crucial for the issuer to reserve sufficient assets as support. This relates to whether users can exchange at a 1:1 price at any time.

- Cross-chain Bridge Risk: When users use cross-chain bridges to perform cross-chain operations for stablecoins, there is a certain risk. The cross-chain bridge first locks the user's stablecoin on the source chain, then issues a corresponding amount of stablecoin to the user on the target chain. If the stablecoin on the target chain is issued by the cross-chain bridge itself, once the cross-chain bridge suffers a cyber attack or other security incidents, the stablecoin issued on the target chain will lose its asset support, leading to its value becoming unpegged.

- Centralized Exchange Risk: When users want to transfer stablecoins from one chain to another, they need to go through a centralized exchange for transfer. Users first send stablecoins to the exchange, then the exchange mints a corresponding amount of stablecoin on the target chain on behalf of the user. During this process, if the stablecoin on the target chain is issued by the centralized exchange itself, when the exchange over-issues or has insufficient collateral assets, it will lead to the depegging risk of the

stablecoin on the target chain. The value of the final stablecoin obtained by the user will be affected.

- Short-term Speculative Risk: The stablecoin market has speculative behavior for optimizing short-term investment returns. These investors target minor price fluctuations of stablecoins at the second or minute level. When they expect the stablecoin price may adjust slightly, speculators choose to buy or sell a large amount of stablecoin selectively, causing the price to experience significant fluctuations in the short term. Then the speculative funds quickly exit the market. This frequent pattern of pushing up and then selling off leads to severe short-term price fluctuations in the stablecoin market.

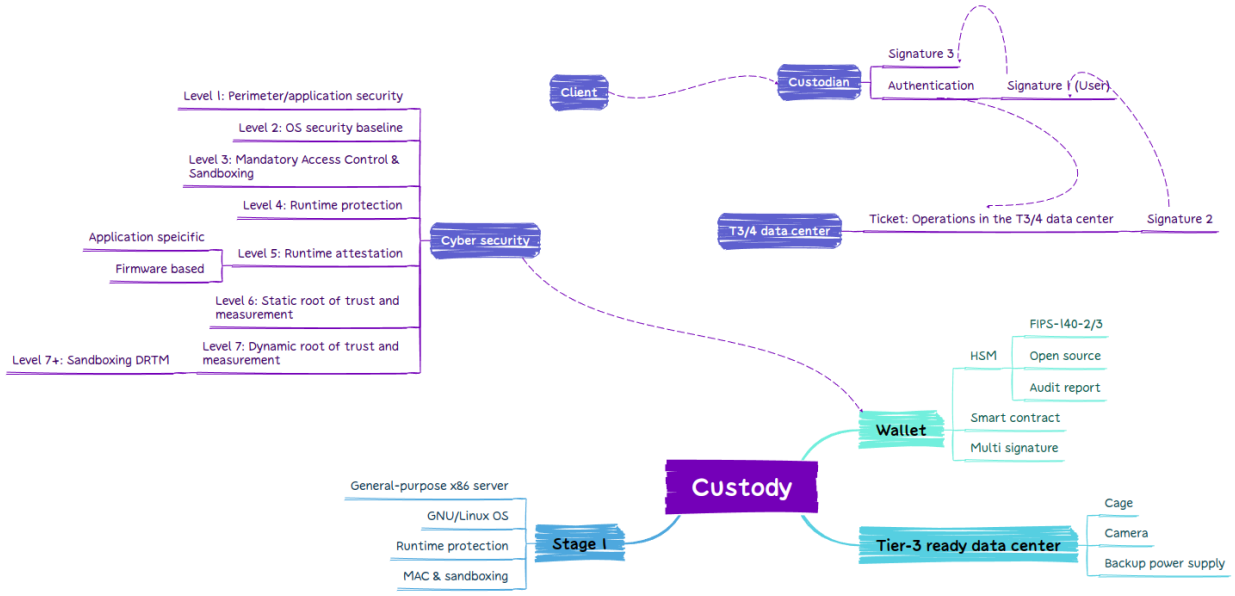
- Hacking Attack and Vulnerability Risks:
    - Exploitation of smart contract vulnerabilities: Many stablecoins rely on smart contracts for issuance and management. Vulnerabilities in smart contracts can be discovered and exploited by hackers, disrupting the stablecoin system and causing user asset losses.
    - Theft of private keys or issuer accounts: Hackers can steal the private keys or accounts of stablecoin issuers through phishing, intrusion, and other means. After gaining stablecoin management privileges, they can cause deflation or malicious over-issuance.
    - Exploitation of cross-chain technology: In the cross-chain transfer of stablecoins, hackers can perform double-spending attacks, forge cross-chain records, and other methods through cross-chain bridges and other technologies, jeopardizing the security of cross-chain asset transfers.
    - Deceiving users into participating in scam projects: Hackers can launch fraudulent stablecoin projects under the guise of stablecoins, misleading users into participating and causing asset losses.
    - Invasion of trading platforms: Hackers can invade stablecoin trading platforms through technical vulnerabilities, directly steal user assets, and cause platform paralysis.
    - Attacking nodes to disrupt the network: Hackers can attack nodes, disrupt the operation of the stablecoin network, and even lead to consequences such as forks.

Hong Kong should actively build a RWA business ecosystem based on the Hong Kong dollar stablecoin. Firstly, Hong Kong needs to issue a stablecoin pegged to the Hong Kong dollar as soon as possible to provide a stable value transfer medium for RWA business. At the same time, it should formulate comprehensive RWA securitization and STO regulatory policies, clarify the range of assets that security tokens can peg and the requirements for information disclosure to protect investors' rights and interests. Establish RWA token issuance and trading platforms in on-exchange markets such as the Hong Kong Stock Exchange to enhance liquidity. Encourage financial institutions such as banks, insurance companies, and funds to fully utilize their professional capabilities to participate in RWA business. At the same time, Hong Kong should strengthen cooperation with Singapore, the European Union, and other places in the field of RWA tokenization business to jointly expand the market. Through education and training, accumulate professional talents needed for RWA tokenization business. Building an open, standardized, and dynamic RWA tokenization business ecosystem based on the Hong Kong dollar stablecoin will effectively enhance Hong Kong's digital economic strength, serve the healthy development of financial technology, and promote the deep integration of Hong Kong in the virtual and real domestic and foreign realms.

4. Web 3.0 Security & Regulation

In February 2023, the Securities and Futures Commission (SFC) launched a public consultation aimed at defining the regulatory requirements for licensed virtual asset trading platform operators. The results of this consultation were published in a document titled "Consultation Conclusions on the Proposed Regulatory Requirements for Licensed Virtual Asset Trading Platform Operators" on May 23, 2023.

This document outlines the minimum requirements for cybersecurity, with a particular focus on the custody infrastructure and trading platforms. While there is a level of overlap between the state-of-the-art technology and the SFC's longstanding minimum requirements, this document goes a step further by incorporating additional industry best practices for reference. This chapter serves as a comprehensive resource for virtual asset trading platforms, offering them insights into not only regulatory obligations but also the gold standard in cybersecurity practices within the industry. This dual focus aims to ensure both regulatory compliance and optimal protection against potential cybersecurity threats.



4.1 Infrastructure Security

This infrastructure security specification aims to provide guidelines and best practices for securing an IT infrastructure. This document will cover various aspects of infrastructure security, including operating system security baselines, runtime protection, access control mechanisms, sandboxing, attestation, and network firewalls.

4.1.1 Linux Security Baseline

4.1.1.1 CIS (Center for Internet Security)

The CIS provides a set of security configuration benchmarks for Linux systems. These benchmarks are designed to help organizations improve their security posture by hardening their systems according to industry best practices. Key CIS recommendations include:

- Regularly applying software patches and updates
- Configuring system logging and auditing
- Implementing strong user authentication and authorization controls
- Disabling unused services and protocols
- Ensuring proper file and directory permissions

4.1.1.2 STIG (Security Technical Implementation Guide)

The STIG is a standardized security configuration guide developed by the United States Department of Defense (DoD). The STIG provides security hardening guidelines for various platforms, including Linux. Key STIG recommendations include:

- Ensuring proper system and application patch management
- Configuring SELinux or AppArmor for mandatory access control
- Implementing strong password policies and account lockout mechanisms
- Securing network services and protocols
- Enforcing the principle of least privilege

4.1.2 Runtime Protection

Runtime protection involves monitoring and protecting applications and services during their execution. Key runtime protection measures include:

- Using intrusion detection and prevention systems (IDPS) to monitor and block malicious activities
- Implementing runtime application self-protection (RASP), WAF (Web Application Firewall), HIDS/EDR (end-point) to detect and prevent attacks at the application level
- Monitoring system and application logs for signs of suspicious activity
- Regularly scanning for vulnerabilities and applying patches as needed

4.1.2.1 Linux kernel runtime protection

To more effectively prevent Linux kernel 0-day or N-day vulnerabilities, defense against the exploit vectors are more widely applicable than defense against specific vulnerabilities. That is, even if there are vulnerabilities, they are difficult to exploit. The following are several aspects of what Linux kernel runtime protection can achieve:

ROP (Return-Oriented Programming) mitigation

PaX RAP of PaX/GRsecurity, KCFI (after v6.1) of the upstream Linux kernel, PA and Shadowstack on the ARM platform, and VED's wCFI. Among them, only VED uses the implementation method of kernel modules, which is weaker than PaX RAP and Shadowstack.

The current version of KCFI on x86 only implements backward indirect call CFI. VED ensures that functions commonly used for privilege escalation can only be called by a small number of code segments in the kernel segment, and implements incomplete forward address checking. In addition, the runtime context check adopted by LKRG/VED can also prevent some ROP.

Post-exploitation/Rootkit prevention

Checking the integrity of the kernel code segment, loadable modules, and critical data during runtime can detect whether the kernel has been contaminated or illegally implanted with loadable modules, thereby preventing rootkit implantation in the kernel. Both LKRG and VED have implemented this type of function. VED's wcfi can also prevent kernel module calls to privilege escalation functions and privilege escalation operation via rootkit.

Data corruption protection

Strengthening commonly used data structures for vulnerability exploitation: VED performs integrity checks on data structures that are frequently used for vulnerability exploitation, such as addresses and lengths, which can prevent some information leaks, UAF, ROP, etc. PaX/GRsecurity implements AUTOSLAB to comprehensively check memory through the mechanism of the slab.

Security module’s self-protection mechanism

Regularly performing integrity checks and runtime state checks on the security module itself can prevent vulnerability exploitation after the security module is unloaded.

4.1.2.2 Mandatory Access Control

Mandatory access control (MAC) is a security model that enforces access control policies based on the classification of information and the clearance of users. Two common MAC implementations are SELinux and AppArmor:

- **SELinux (Security-Enhanced Linux)**: A Linux kernel security module that enforces access control policies for processes, files, and network resources.
- **AppArmor**: A Linux kernel security module that provides application-level access control using profiles.

Both SELinux and AppArmor should be properly configured and used to enforce strict access control policies.

4.1.2.3 Sandboxing

Sandboxing is a security mechanism that isolates applications or processes in a restricted environment to limit their access to system resources and other applications. Key sandboxing techniques include:

- Using containerization technologies (e.g., Docker, Kubernetes) to isolate applications and their dependencies

- Implementing virtualization technologies (e.g., KVM, Xen) to create isolated virtual environments
- Utilizing seccomp (secure computing mode) to restrict system calls made by processes

4.1.3 Runtime Attestation

Runtime attestation is the process of verifying the integrity and authenticity of applications and services during their execution. Key runtime attestation techniques include:

Runtime attestation is the process of verifying the integrity and authenticity of applications and services during their execution. Its key techniques include Integrity Measurement Architecture (IMA) in the integrity subsystem in the Linux kernel, Trusted Platform Module (TPM) implementation for hardware-based attestation, and remote attestation and :

- Implementing Trusted Platform Module (TPM) for hardware-based attestation
- Using Remote Attestation to verify the integrity of applications and services running on remote systems
- Leveraging Intel Software Guard Extensions (SGX) or ARM TrustZone for hardware-assisted secure execution

In this specification, remote attestation is selected as the default runtime attestation solution considering the security of the verification environment and the flexibility of the attestation management. And in the attestation process, the integrity of running applications and services is verified by a remote system using the IMA measurement values and the TPM output.

Key Components

- Trusted Platform Module (TPM): A standard (iso/iec 11889) for the security cryptographic processor. The latest TPM 2.0 specification is developed by the Trusted Computing Group (TCG). TPM chip is a microprocesser hardware integrated in the motherboard that complies the TPM standard.

- Integrity Measurement Architecture (IMA): Linux kernel built-in subsystem for system integrity measurement. It usually works with the TPM hardware to prevent the measurement process from tampering.

- Mandatory access control (MAC): The measurement policy of IMA can be enhanced using the LSM specific policies implemented in the MAC components, including SELinux and SMACK (Simplified Mandatory Access Control Kernel).

- Verifier: The application located in a remote node where the hashes of attested files are compared and verified.

- Keylime: A remote attestation and runtime integrity measurement solution based on TPM and IMA. The attestation operation depends on the agent, verifier, registrar, and command-line tool.

Workflow

1. Measured Boot: Measured Boot is a prerequisite to enable measured boot as a critical step of overall runtime attestation. It secures the system components in the booting process from being modified by malicious behavior which happens before IMA takes over the system-wide measurement.
    a. With the coreboot firmware, measured boot starts from the IBB (Initial Boot Block) which works as an S-CRTM (Static Core Root of Trust for Measurement).
    b. In UEFI, secure boot is implemented and enabled by default by most vendors.

2. IMA Enabling: The function of IMA measurement is enabled from the kernel command line. The option is added to the GRUB configuration file to make it persist after the rebooting.

3. IMA Measurement Policy Configuration: SELinux object is applied in the rules of the IMA policy to specify what files should be measured and therefore achieves a fine-grained policy control. The SELinux should have been enabled in the system. In addition, the context of the files to be measured is distinguishable from those not to be measured.

4. Deployment Environment The deployment of remote attestation requires both the attested machine and the remote verifier machine to be in good and secure status, as instructed in this specification.

In addition, to minimize the attack surface, the system should be in the following status before the deployment:

1. Measured boot has already been enabled

2. Packages on the system have been installed from a reliable source through a secure network channel and their digital signatures are verified.

3. Extended Hash: On the machine to be attested, the extended hash of the files covered under the measurement is obtained from the TPM PCR-10 register. It has the same value as the aggregated hash calculated from the runtime measurement list under a good integrity environment. Before the hash value is sent to the remote verifier through the network, it should be signed in TPM using Attestation Key (AK), which is also generated in TPM. The extended hash does not leave TPM before signing to avoid being modified maliciously during the attestation process.

4. Remote Verifier On the remote verifier, the good hash value of attested files is retrieved from a trusted source or generated from the files obtained from a trusted source and should be stored securely.

5. Verification Method It is possible for the remote verifier to verify the integrity by simply examining the static PCR extended hash, known as the golden value, and checking if it matches the aggregate value pre-calculated from the good file hashes. However, this method suffers from the nondeterminism issue. In other words, a slight variation on any measured files due to system change can finally create a different PCR extended hash, although the other integrity-critical files are in good status. This issue is particularly common when the IMA policy is not fine-grained enough.

A more practical approach is comparing good hashes of only those integrity-critical files to the runtime measurement list obtained from the attested system. To ensure the list is not modified by malicious behavior, further verification is required to ensure its aggregated hash matches the PCR extended hash. Since the PCR extended hash is signed by AK, its integrity can be verified by checking the signature.

4.1.3.1 Runtime Attestation Framework

This specification recommends applying existing attestation framework instead of developing a solution of one’s own.

As a recommendation, Keylime is a remote attestation and boot measurement framework on the GNU/Linux platform based on TPM and IMA. The project is hosted by the Cloud Native Computing Foundation (CNCF) and in active development by the community. Also, it is available on all major GNU/Linux distributions.

Keylime provides the following features that are helpful for the deployment of a secure and practical runtime attestation environment.

1. Main components: Keylime framework consists of four core components in terms of agent, verifier, register, and tenant. The agent is deployed on the machines to be attested to collect necessary measurement information for attestation. On the remote node, the verifier performs actual verification of measurement value, and the register is responsible for the agent node registration. The tenant is a command-line tool for users to manage the Keylime efficiently.

2. Measured boot: Keylime support measured boot verification by examining the validation of PCR value extended during the booting process.

3. Secure Payload: The secure payload is a mechanism for the remote note to send confidential data used by the agent to the attested machine, such as configuration files, keys, and scripts, in a secure way. An especially useful use case of the secure payload is that a customized action on the attested machine can be triggered when the verification is failed on a remote verifier.

4. Allow List: To avoid the nondeterminism issue in the measured boot attestation, instead of using static PCR values, Keylime involves a policy engine to verify UEFI Event log. Furthermore, the allowlist mechanism is provided, by which only the specified files are measured in the attestation. It is achieved by comparing the runtime measurement list obtained from the agent machine with the good hashes in a local allowlist.

Overall, with a mature solution broadly applied by users and actively maintained by the community, the attack surface created by programming mistakes and misconfigurations could be reduced to a large extent.

4.1.4 HSM (Hardware Security Module)

To ensure the security and integrity of digital assets, we propose a solution involving Hardware Security Modules (HSMs). HSMs are dedicated cryptographic devices designed to protect sensitive information and perform cryptographic operations. This solution will provide a secure environment for key generation, seed generation, and handling of virtual assets.

Key Components

1. **Hardware Security Module (HSM)**: A dedicated, tamper-resistant device for secure key management and cryptographic operations.
2. **Key Management System (KMS)**: A centralized system for managing cryptographic keys, access controls, and policies.
3. **Application Layer**: Software applications and APIs for interacting with the HSM and KMS, as well as performing virtual asset transactions.

Workflow

1. **Key Generation**: The HSM is used for generating and storing private keys. This ensures that the keys are never exposed outside the secure environment of the HSM.
2. **Seed Generation**: The HSM generates a cryptographically secure seed, which can be used to derive additional keys or as a recovery method for the primary key.
3. **Access Control**: Access to the HSM and KMS is protected by strong authentication mechanisms, such as multi-factor authentication and role-based access control. This ensures that only authorized personnel can access the sensitive data and perform operations on the HSM.
4. **Transaction Signing**: When a virtual asset transaction is initiated, the application layer communicates with the HSM to sign the transaction using the appropriate private key. This ensures that the private key is never exposed to the application or network, providing a high level of security for the transaction.
5. **Auditing and Monitoring**: All operations on the HSM and KMS are logged and monitored for any suspicious activity or potential security breaches. This helps to detect and prevent unauthorized access or manipulation of the cryptographic keys and sensitive data.

4.1.4.1 HSM options

We do not recommend any products, but there are several aspects that require attention.

1. FIPS 140-2/3 Certification: This certification ensures that the HSM meets stringent security requirements and provides sufficient protection for sensitive data and cryptographic operations.

2. Performance: it depends on the use-case, e.g: DeX custody might need greater need for high-speed signature than CeX.

3. Scalability: HSM should be easily integrated into existing environments and scaled to support growing needs.

4. Ecosystem: Tools, libraries, and services for managing and interacting with the HSM, making it easier to implement and maintain the digital custody solution.

5. Transparency: The advantage of transparency brought by open source is obvious, and auditability is a prerequisite. Increasing the frequency of audits under this prerequisite will significantly reduce the risk of vulnerabilities and backdoors.

Last but not least, ask for a 3rd-party security audit report from the HSM vendor if the HSM is not open source.

Model	Type	FIPS-140 certification	Open source implementation	Public audit report	Cryptographic APIs	Restful API	Performance	Storage
Thales Luna PCIe HSM A700	PCI HSM	FIPS 140-2 Level 3	N/A	N/A	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL	N/A	RSA-2048: 1,000 tps	?
Thales Luna USB HSM	USB HSM	FIPS 140-3 Level 3	N/A	N/A	PKCS #11	N/A	RSA-4096: 8 tps	?
ProtectServer 3 External	Network HSM	FIPS 140-2 Level 3	N/A	N/A	PKCS#11, CAPI/CNG, JCA/JCE, JCProv, OpenSSL	YES	RSA-2014: 3500 tps	?
IBM 4769	PCI HSM	FIPS 140-2 Level 4	N/A	N/A	PKCS #11	N/A	?	?
YubiHSM 2 FIPS	USB HSM	FIPS 140-2 Level 3	N/A	N/A	PKCS#11, native libraries (C and Python)	No	RSA-2048-PKCS1-SHA256: 8	127 RSA2048 or 255 ECC
NitroKey NetHSM	Network HSM	N/A	??	??	PKCS#11	Yes	??	??

4.1.5 Networking Firewall

A network firewall is a security device that monitors and controls network traffic based on predefined security rules. Key network firewall best practices include:

- Implementing both ingress and egress filtering to control incoming and outgoing traffic
- Regularly reviewing and updating firewall rules to ensure proper access control

- Using network segmentation to isolate sensitive systems and applications
- Deploying intrusion detection and prevention systems (IDPS) to monitor and block malicious network activities

4.1.6 Hardware/Firmware supply chain risks

In March 2023, Micro-Star International (MSI) suffered significant attack orchestrated by the Money Message ransomware group. Unfortunately, this is not just another random leak. The aftermath revealed a leak of internal data, including highly sensitive information such as the BootGuard private key. This key, integral to Intel's hardware trust and cryptographic key management system, signifies an exploit vector can't be fixed easily, allowing for bypassing of the primary security mechanism in specific device models. Additionally, the leaked data also exposed the UEFI firmware image signing key, further exacerbating the severity of the breach. The BootGuard security mechanism, alongside CPU Microcode and CSME, forms the foundation of Intel's core security mechanisms. It serves as a critical integrity protection mechanism rooted in the hardware trust system, while the UEFI firmware acts as a vital low-level software component within the computer system. The compromise of BootGuard, whether through successful attacks via vulnerability (e.g: CVE-2020-8705) or acquisition of the private key from OEM/ODM manufacturers, enables threat actors to exploit UEFI implementation flaws, configuration errors, and other vulnerabilities to achieve bypass numerous established security measures and mitigations, e.g: SMM_BWP, BWE/BLE, PRx hardware security mechanisms, SecureBoot and kernel security mitigation technologies such as HCVI, PatchGuard, kASLR, KDEP, SMEP, SMAP. Furthermore, mainstream antivirus software and EDR/XDR systems become ineffective, granting attackers persistent control over the compromised device. OEM vendors usually would only suggest you upgrade to the latest firmware but it's far from "acceptable" under the circumstances. To mitigate these risks, several strategies should be considered:

- It's crucial to strengthen protection at the OS level. This can be achieved through the implementation of OS hardening (See runtime protection section). At the firmware level, a recommended approach is to consider transitioning from UEFI to coreboot. Coreboot represents the next-generation firmware and empowers users to become OEM manufacturers themselves. This paradigm shift gives users the right to perform hardware security provisioning, effectively granting them control over the entire supply chain. By embracing coreboot, users align with the principles of self-sovereignty, reducing the inherent security risks associated with the supply chain and vulnerabilities. On the other hand, it's easier to achieve trusted computing (See runtime attestation section) by integrating a security payload alongside with coreboot.

- Leveraging trusted computing in a comprehensive manner. Trusted computing is a powerful concept, but it presents a delicate balance. If users have the right and capability for secure provisioning, trusted computing becomes an ally, enhancing security and trust. With coreboot, you're able to control the secure provision for a number of hardware security features, e.g: TXT/CBnT, TPMv2, SGX/TDX, SEV/SEV-SNP, etc. However, if users lack control and transparency as UEFI, they may

fall into the trap of treacherous computing, as discussed by Richard Stallman. MSI's leaked materials put all x86 users to a risky position as the OEM signing has been compromised. However, if a user possesses their own key, the situation becomes entirely different.

- Continuous security monitoring and auditing of both the OS and firmware (below-OS). Regular assessments and audits help identify vulnerabilities, detect potential threats, and implement timely mitigations.

4.1.7 Node specifications

The hardware for the node should adhere to the following requirements:

Off-the-shelf Hardware: The node should utilize readily available off-the-shelf components. This includes options such as mini-PCs, embedded compute nodes, workstations, and typical 1U/2U/4U servers.

Coreboot Supported Hardware: Only hardware that is compatible with the Coreboot firmware should be considered due to secure provisioning is a must to mitigate the supply chain risk as described in Section 4.1.6. This encompasses both ARM64 and x86_64 architectures, allowing for a wide range of hardware options to meet the requirements.

Firmware Packages: The firmware for the node should consist of the following components:

- Binary Blobs: For x86_64 architecture, the firmware should include the Firmware Support Package (FSP). For ARM64 architecture, it should include the Trusted Firmware-A (TF-A). These binary blobs provide essential hardware initialization and support functionalities.
- Coreboot Firmware Framework: The firmware should be built upon the Coreboot firmware framework. Coreboot is an open-source firmware that provides a customizable and lightweight boot environment.
- Linux-based Payload: The firmware should incorporate a Linux-based payload, such as Linuxboot, Vaultboot, heads, or similar options. This ensures a secure and versatile platform for running various software applications.

By adhering to these hardware specifications, the node can leverage a wide range of off-the-shelf hardware options while utilizing the Coreboot firmware framework and a Linux-based payload for a secure and flexible computing environment.

4.2 System Design Security

Web 3.0 presents new challenges for the security and governance of the Internet ecosystem. When designing Web 3.0 software systems, the following are considerations for key technologies in terms of security:

4.2.1 Blockchain Security

1. Consensus Algorithm Security: Selecting appropriate consensus algorithms and ensuring their security to prevent malicious nodes from attacking the blockchain network. For example, Proof of Work (PoW) and Proof of Stake (PoS) are common consensus algorithms that require security analysis and evaluation.
2. Protection against 51% Attacks: Ensuring that no single entity or group of entities can control more than 51% of the computational power to prevent manipulation of the blockchain network.
3. Smart Contract Security Audit: Conducting comprehensive security audits of smart contracts to identify and mitigate potential vulnerabilities and security risks. This involves reviewing aspects such as input validation, boundary checks, permission controls, and code logic. When vulnerabilities or security issues are discovered in smart contracts, they should be promptly fixed and upgraded through mechanisms such as introducing upgrade mechanisms, using proxy contracts, or self-destructing contracts.
4. Prevention of Double Spending and Transaction Rollback Attacks: Employing suitable encryption techniques and consensus mechanisms to ensure the immutability of transactions and the irreversibility of transaction history in the blockchain.
5. Data Privacy Protection: Ensuring sensitive data is appropriately encrypted and protected during storage and transmission on the blockchain to prevent unauthorized access and leakage. Utilizing privacy protection technologies such as zero-knowledge proofs, homomorphic encryption, and ring signatures to safeguard user privacy and sensitive data while maintaining verifiability and auditability.
6. Decentralized Identity Verification: Integrating decentralized identity systems and employing distributed identity verification and authentication mechanisms to protect user identity information and personal data, while reducing reliance on centralized identity verification services.
7. Open Source Code Auditing: Open source code auditing is a crucial means to ensure blockchain security. By making source code openly available, it encourages community participation in security audits to discover and fix potential vulnerabilities and security risks.

4.2.2 Network Security

1. Secure Communication Protocols and Encryption: Employ secure communication protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), along with robust encryption techniques. This ensures the confidentiality, integrity, and authenticity of network communications, mitigating the risks of data leakage and man-in-the-middle attacks.

2. Intrusion Detection Systems and Firewalls: Implement comprehensive intrusion detection systems (IDS) and firewalls to actively monitor network traffic, identify potential threats, and prevent unauthorized access. This includes detecting and mitigating Distributed Denial of Service (DDoS) attacks, malicious traffic, and intrusion attempts.
3. Secure Authentication and Access Control: Implement strong authentication mechanisms, such as multi-factor authentication (MFA) and strong passwords, to verify the identities of users and ensure that only authorized individuals can access the system and its resources. Additionally, enforce granular access control policies to limit privileges and reduce the attack surface.
4. Security Updates and Vulnerability Management: Establish a proactive approach to security updates and vulnerability management. Regularly update and patch systems, applications, and network devices to address known vulnerabilities. Implement a system for monitoring and assessing emerging threats, and promptly apply security patches and fixes to mitigate potential risks.
5. Security Monitoring and Incident Response: Implement real-time security monitoring tools and techniques to detect and respond to security incidents promptly. This includes monitoring network traffic, system logs, and event data for anomalies or suspicious activities. Develop an incident response plan to outline procedures for handling security incidents, including containment, investigation, and recovery.
6. Employee Training and Awareness: Conduct regular training programs to educate employees about network security best practices, such as recognizing phishing attempts, practicing good password hygiene, and avoiding suspicious downloads. Promote a culture of security awareness throughout the organization to enhance overall network security posture.

4.2.3 Cryptocurrency Security

1. Secure Wallet Management: Provide secure wallet storage and management, including cold wallets (offline storage) and hot wallets (online storage), to prevent private key leakage and unauthorized access.
2. Private Key Protection: Employ secure key generation and storage methods, such as hardware wallets or secure elements, to safeguard the security of private keys.
3. Prevention of Transaction Tampering and Double Spending: Utilize cryptographic signatures and verification mechanisms to ensure the integrity of transactions and prevent double-spending attacks.
4. Legitimacy Verification and Traceability: Implement effective blockchain transaction validation mechanisms to ensure the legitimacy of transactions and provide traceable transaction history, mitigating the risks of money laundering and other illegal activities.
5. Multi-factor Authentication: Implement multi-factor authentication (MFA) mechanisms to enhance the security of cryptocurrency transactions and account

access. This can include utilizing biometric authentication or additional verification methods beyond passwords.

6. Secure Smart Contracts: Conduct thorough security audits and testing of smart contracts to identify and address vulnerabilities, minimizing the risks of exploit and malicious activities.
7. Regular Security Audits: Perform regular security audits and assessments of cryptocurrency systems and platforms to identify and address any vulnerabilities or security weaknesses.
8. Ongoing Security Education and Awareness: Promote ongoing education and awareness among cryptocurrency users regarding best practices for security, including the importance of strong passwords, phishing prevention, and caution when interacting with unknown or suspicious entities.

4.2.4 Distributed Architecture Security

Distributed architecture security refers to the measures and practices implemented to ensure the security and integrity of a distributed architecture system. In a distributed architecture, various components and services are spread across multiple nodes or systems, often connected through a network. The goal of distributed architecture security is to protect the system from unauthorized access, data breaches, malicious attacks, and other potential security risks.

4.2.4.1 Distributed Digital Identity (DID)

Distributed digital identity refers to storing individuals' or entities' identity information in a distributed network to achieve a more secure and decentralized identity verification and management. When ensuring the security of distributed digital identity, several factors need to be considered:

1. Identity Authentication and Access Control: Implement robust identity authentication mechanisms to ensure that only authorized users can access and manage their identity information.
2. Data Privacy Protection: Utilize encryption technology and privacy protection measures to ensure the confidentiality and integrity of personal identity information.
3. Decentralized Identity Management: Utilize distributed ledger technology to ensure decentralized storage and management of identity information, reducing single points of failure and attack risks.
4. Identity Ownership and Control: Ensure that users have ownership and control over their identity information, enabling them to authorize access and revoke permissions.

4.2.4.2 Distributed Autonomous Organization (DAO)

Distributed Autonomous Organizations (DAOs) are decentralized organizational forms realized through smart contracts and blockchain technology, and their security is of utmost importance. When ensuring the security of DAOs, several factors need to be considered:

1. Smart Contract Security Audits: Conduct comprehensive security audits of DAO's smart contracts to identify and rectify potential vulnerabilities, security risks, and potential attack vectors.
2. Member Identity Verification: Implement effective member identity verification mechanisms to ensure that only legitimate members can participate in and execute DAO operations.
3. Security of Voting and Decision-making: Ensure the security and fairness of the voting and decision-making process, preventing malicious manipulation and attacks.
4. Fund Management and Security: Adopt multi-signature and secure wallet management to ensure the security of DAO funds and prevent unauthorized fund transfers.

4.2.4.3 Distributed Finance (DeFi)

Distributed Finance (DeFi) is a decentralized financial system built on blockchain technology, and its security is crucial for user trust and adoption. When ensuring the security of distributed finance, several factors need to be considered:

1. Smart Contract Audits and Security: Conduct comprehensive security audits of DeFi protocols and smart contracts to identify and rectify potential vulnerabilities and attack surfaces.
2. Fund Security and Risk Mitigation: Implement secure wallet management, multi-signature, and risk management mechanisms to ensure the security of user funds and mitigate potential risks.
3. Liquidity and Compliance: Ensure the liquidity and compliance of the DeFi system, adhering to relevant financial regulations and compliance requirements, preventing money laundering and illegal fund flows.
4. Insurance and Security Funds: Establish insurance mechanisms and security funds to mitigate potential losses and safeguard against hacker attacks.

4.2.4.4 Distributed Application (DApp)

Distributed Applications (DApps) are applications that run on a blockchain, and their security is a prerequisite for user trust and widespread adoption. When ensuring the security of DApps, several factors need to be considered:

1. Smart Contract Security Audits: Conduct comprehensive security audits of DApps' smart contracts to identify and rectify potential vulnerabilities and security risks.
2. User Data Privacy Protection: Employ encryption technology and privacy protection measures to ensure the confidentiality and security of user data.
3. Prevention of Malicious Application Attacks: Implement secure coding practices and security audits to prevent malicious applications from causing harm to users.

4. Prevention of Network Attacks and Data Tampering: Implement network security measures such as firewalls and encrypted communications to prevent hacker attacks and data tampering.
5. User Authentication and Authorization: Implement robust user authentication and authorization mechanisms to ensure that only authorized users can access and perform sensitive operations.

4.2.5 Data Processing Security for Privacy Protection

1. Distributed Data Processing Technology: Employ advanced distributed data storage and processing techniques, such as decentralized storage and computing, to ensure robust security and data integrity throughout transmission and storage processes.
2. Encryption Technology and Data Protection: Implement state-of-the-art encryption algorithms to safeguard sensitive data, ensuring its confidentiality and protection. Additionally, employ techniques such as data anonymization, data masking, and access control to minimize the risk of sensitive data exposure.
3. Compliance and Data Protection Regulations: Adhere strictly to applicable data protection laws and privacy regulations, such as the General Data Protection Regulation (GDPR), to ensure compliance, legality, and transparency in the handling of user data. Provide transparent data processing mechanisms and empower users with choices and control over their personal information.

4.3 Application Security

Web 3.0 offers endless possibilities at the application layer. The concept of the metaverse aligns perfectly with the principles of Web 3.0. The notion of creator economy has gained significant prominence and relevance within the Web 3.0 context. The creator economy refers to the ecosystem and economic model that empowers content creators, artists, influencers, and other individuals to monetize their creative output directly and engage with their audience in new ways. In this section, we will specifically focus on the security considerations at the application layer for the metaverse and the creator economy. This discussion can be extended to address security concerns in other applications as well.

4.3.1 Metaverse applications

The metaverse is an immersive digital realm that expands upon and simulates the physical world, allowing users to create, interact, and trade digital assets within its virtual environment. It is constructed using technologies such as blockchain, virtual reality, augmented reality, and artificial intelligence.

The metaverse offers an open platform where users can engage in a wide range of activities, with their identities, data, and assets at the core of the virtual experience. Users can create personalized avatars, participate in virtual social networks, engage in transactions involving digital assets like artwork, virtual properties, and cryptocurrencies, take part in virtual economic

activities such as gaming and virtual commerce, and even immerse themselves in virtual reality experiences.

4.3.1.1 Virtual World Construction

Metaverse applications include creating environments, scenes, and maps for virtual worlds. These virtual worlds can be simulations based on the real world or entirely fictional spaces. Building virtual worlds involves designing and developing virtual landscapes, buildings, objects, and other elements to create an interactive and immersive environment. There are some security factors about virtual world construction:

1. Preventing malicious code injection and vulnerability exploitation in the virtual world
2. Controlling and managing access permissions within the virtual world to prevent unauthorized modification and destruction
3. Implementing secure storage and protection mechanisms for virtual assets to prevent theft or tampering of virtual objects and scenes

4.3.1.2 User Interaction and Socialization

Metaverse applications provide features for user interaction and socialization, allowing users to communicate, collaborate, and interact in various ways within the virtual world. This can include real-time voice and video communication, instant messaging, social media features, multiplayer gaming, and cooperation to facilitate socialization and collaborative experiences among users. The security factors include:

1. Authentication and authorization mechanisms to protect user account security and prevent unauthorized access
2. Preventing the creation and use of fraudulent and fake accounts
3. Monitoring and managing user-generated content to prevent the spread of malicious content and inappropriate behavior

4.3.1.3 Economy and Digital Assets

Metaverse applications often involve economic systems and management of digital assets. Users can buy, sell, trade, and own virtual currencies, digital goods, virtual land, and other digital assets. These digital assets can hold value within the virtual world, and users can acquire and manage wealth through economic interactions and trading activities. The security factors include:

1. Secure transaction and asset transfer mechanisms, including safeguarding the security of digital currency and virtual goods transactions
2. Preventing fraudulent and false transactions, as well as risks of theft and tampering of virtual assets
3. Secure digital wallet and asset storage mechanisms to prevent loss or theft of digital assets

4.3.1.4 Creation and User-Generated Content

Metaverse applications encourage users to create and contribute content. Users can design and create virtual objects, characters, artwork, game levels, storylines, and also write code and scripts to implement custom functionality. User-generated content enriches the virtual world experience and provides opportunities for participation and interaction among other users. The security factors include:

1. Reviewing and auditing user-generated content to prevent the spread of malicious code, malicious links, or inappropriate content
2. Preventing copyright infringement and piracy, protecting the rights of user-created content
3. Preventing abuse of malicious scripts and code to protect user and system security

4.3.1.5 Cross-Platform and Interoperability

Metaverse applications often possess cross-platform and interoperability capabilities, allowing users to access and participate in the virtual world across different devices and platforms. This can include desktop computers, mobile devices, virtual reality headsets, and other interactive devices. Additionally, metaverse applications may also enable interoperability with other applications and platforms through open standards and protocols, facilitating cross-application and cross-platform functionality and data exchange. The security factors include:

1. Secure device and platform access, including security management for mobile devices, virtual reality headsets, etc.
2. Secure data exchange and communication protocols to ensure confidentiality and integrity of data transfers across applications and platforms
3. Mitigating the risks of malicious attacks or data breaches from other applications and platforms

4.3.2 Creator Economy

Web 3.0 has greatly facilitated and empowered the creator economy. The advancements in Web 3.0 technologies, such as blockchain and decentralized platforms, have provided creators with enhanced opportunities for ownership, control, and monetization of their work. Web 3.0 enables creators to leverage smart contracts, non-fungible tokens (NFTs), decentralized marketplaces, and other tools to establish direct relationships with their audience, receive fair compensation, and maintain greater creative independence.
Some examples of creator economy applicationw as following may face the potential security vulnerabilities and risks.

4.3.2.1 Decentralized Content Creation Platforms

Security issues: Fake and low-quality content, copyright infringement, user data leakage
Methods to address:

1. Implement content moderation mechanisms and quality controls, including manual review and automated filtering algorithms, to reduce the spread of fake and low-quality content
2. Implement copyright protection measures, such as digital rights management technologies and watermarks, to prevent copyright infringement
3. Enhance privacy protection for user data using encryption techniques and de-identification methods to ensure the security and privacy of user data

4.3.2.2 Decentralized Marketplaces and Auction Platforms

Security issues: Transaction fraud, fake auctions, contract vulnerabilities
Methods to address:

1. Introduce transaction verification mechanisms, such as multi-signature and trusted third-party authentication, to ensure the authenticity and reliability of transactions
2. Establish a trust rating system to rate and verify users and their transaction behavior, providing more accurate trust assessments
3. Regularly conduct security audits of smart contracts to identify and fix potential vulnerabilities and errors

4.3.2.3 Social Media and Community Platforms

Security issues: Malicious user behavior, user data privacy breaches
Methods to address:

1. Introduce identity verification and trust mechanisms to ensure the authenticity and credibility of users
2. Strengthen protection against social engineering and network attacks, including educating users on how to identify malicious activities and guard against network attacks
3. Utilize encryption techniques and privacy protection measures to safeguard user data privacy and security

4.3.2.4 Decentralized Music/Video Platforms

Security issues: Music/Video copyright infringement, fake NFTs, smart contract vulnerabilities
Methods to address:

1. Implement copyright protection measures, such as digital rights management technologies and smart contract-based copyright verification, to ensure the legality and ownership of music works
2. Strengthen oversight and verification mechanisms in the NFT marketplace to prevent the presence of fake NFTs
3. Enhance privacy protection for user data using encryption techniques and de-identification methods to ensure the security and privacy of user data
4. Conduct regular security audits and testing of smart contracts to ensure their security and reliability

5. Development and Prospects of Web 3.0 in HK

Recently, Hong Kong's policies regarding Web 3.0 have been implemented since the release of the "Policy Statement on the Development of Virtual Assets in Hong Kong" by the Financial Services and the Treasury Bureau on October 31, 2022. The policy statement outlines the Hong Kong government's stance and direction on Web 3.0, emphasizing the alignment of legal and regulatory frameworks with market development to foster Hong Kong's position as a global hub for Web 3.0. The policy statement also sets the future direction for policies relating to stable coins and tokenized real-world assets (RWA).

As of today, the policies outlined in the policy statement have been progressively implemented. Within less than a year, various regulatory and other departments have been gradually carrying out the policies. Following its status as a financial center, Hong Kong has the potential to quickly become a global hub for Web 3.0 in the future.

5.1Trusted Decentralized Networking towards 6G

There is a profound interrelationship between trusted decentralized networks and Web 3.0 as they mutually support and drive the future development of the internet. The objective of a trusted decentralized network is to establish a decentralized, secure, privacy-preserving, and highly reliable network environment. This is achieved through the adoption of distributed network architecture, encryption technologies, smart contracts, and other means. Such a network model reduces the risk of independent failures in centralized architectures, making the network more robust and reliable while providing enhanced security and user data protection. It provides a strong technological foundation and support for Web 3.0. Distributed network architecture and encryption technologies ensure secure data transmission and storage, safeguarding user privacy. Smart contract technology, on the other hand, offers an automated and programmable execution environment for decentralized applications within Web 3.0. Additionally, the high network reliability and fault tolerance of trusted decentralized networks provide stable and dependable infrastructure for applications and services in Web 3.0.

Meanwhile, the technology industry and academic community in Hong Kong have undertaken multiple key research projects focused on 6G. The industry firmly believes that by leveraging Hong Kong's research advantages and promoting collaborative research and cooperation with counterparts from various regions, they can contribute to the global development of 6G.
6G technology refers to the sixth generation of mobile communication technology, which aims to further advance wireless communication. While 6G technology is still in the research and planning phase, some concepts and key technological directions have emerged. Compared to 5G, it has some concepts and potential advantages: higher data rates, lower latency, greater network capacity, expanded coverage, enhanced security and privacy protection, emphasis on intelligence and adaptability and utilization of ultra-high frequencies.

There are several aspects of alignment between the new features of 6G and the requirements of a trusted decentralized network. A trusted decentralized network aims to establish a

decentralized, secure, and privacy-preserving network environment with high network reliability, and the new features of 6G provide strong support for achieving these goals.

1. Firstly, 6G introduces higher-level security features such as identity authentication, encryption technologies, and secure transmission protocols to meet the network security requirements of a trusted decentralized network. These features protect user data and prevent malicious attacks.
2. Secondly, 6G offers low-latency communication and high data transmission rates, fulfilling the real-time interaction and large-scale data transmission needs of a trusted decentralized network. This facilitates fast response in decentralized applications and services.
3. Thirdly, the enhanced edge computing capabilities of 6G provide more efficient data processing and storage for a trusted decentralized network. By distributing computing tasks to edge nodes closer to end devices, the network can alleviate the load on centralized servers, improve data processing efficiency, and support edge services and applications in a decentralized context.
4. In addition, the powerful connectivity density of 6G meets the connection requirements of large-scale devices and users in a trusted decentralized network. Network slicing technology enables flexible resource allocation and management based on different application and service needs.
5. Furthermore, 6G's focus on global coverage and seamless roaming caters to the global application demands of a trusted decentralized network, allowing users to smoothly transition between different networks.
6. Lastly, the intelligent sensing and adaptability of 6G enable intelligent decision-making and optimization in a trusted decentralized network. The network can adjust and optimize based on network conditions and requirements, providing high-quality services and user experiences.

6. Conclusion

Although the development of Web 3.0 is still in its exploratory phase, the fundamental technological framework and development direction of Web 3.0 have begun to take shape. Governments worldwide are highly attentive to the development of Web 3.0 and are progressively pushing for the formulation of development policies and the enhancement of regulatory systems. Serving as a traditional international hub for finance, trade, and shipping, Hong Kong acts as a bridge connecting mainland China, Southeast Asia, and global markets. Financial technology has become one of the significant development directions for driving Hong Kong's advancement. Furthermore, Hong Kong boasts several world-renowned universities, national key laboratories, and branches of national engineering and technical research centers, renowned for their exceptional academic and research capabilities, providing a solid foundation for the innovation of Web 3.0 technologies. With diverse initiatives driven by the Hong Kong government, complemented by legal and regulatory systems aligned with market development, Hong Kong has the potential to swiftly become a global center for Web 3.0, following its success as a financial center.

7. Reference