Mainland vs Hong Kong: China's Dual-Chain Move

Table of Contents

Abstact

Based on a systematic review of domestic and foreign financial regulatory frameworks, this paper provides an in-depth analysis of the differentiated decision-making logic of traditional securities firms in the layout of blockchain public chains. The study finds that **regulatory boundaries are the primary variable determining technical architecture**, profoundly influencing the public chain deployment logic of Mainland securities firms, Hong Kong securities firms, and international securities firms.

The core conclusions of this study are as follows:

1. **Mainland Securities Firms: "Minimizing Compliance Costs"**: Constrained by "penetrating supervision" and data cross-border restrictions, Mainland securities firms do not possess the feasibility for self-developing public chains or accessing public chains in the short term. Their optimal solution lies in utilizing **Consortium Blockchain** technology, focusing on "cost reduction and efficiency enhancement" scenarios such as investment banking working paper storage and supply chain finance ABS (Asset-Backed Securitization). This meets hard compliance requirements such as the *Specification for Blockchain Electronic Data Deposit Application in the Securities Industry*, achieving low-cost digital transformation.

2. **Hong Kong Securities Firms: "Maximizing Business Value"**: Under the framework of licensing permissions and "sandbox supervision," Hong Kong securities firms lean towards **externally selecting mature public chains** (e.g., Ethereum, Solana, Pharos). Their core appeal lies in utilizing the mature liquidity ecosystem of public chains for Real World Asset (RWA) tokenization issuance, or using high-performance public chains to achieve atomic settlement, thereby seizing incremental markets in innovative businesses like tokenized funds and cross-border payments.

3. **International Securities Firms: "Defining Global Standards for Blockchain Finance"**: International leading institutions represented by JPMorgan Chase and fintech institutions represented by Robinhood are evolving towards **self-developed Layer 2 architectures**. They aim to become "super nodes" of the future blockchain financial network by controlling core technical standards and compliance interfaces.

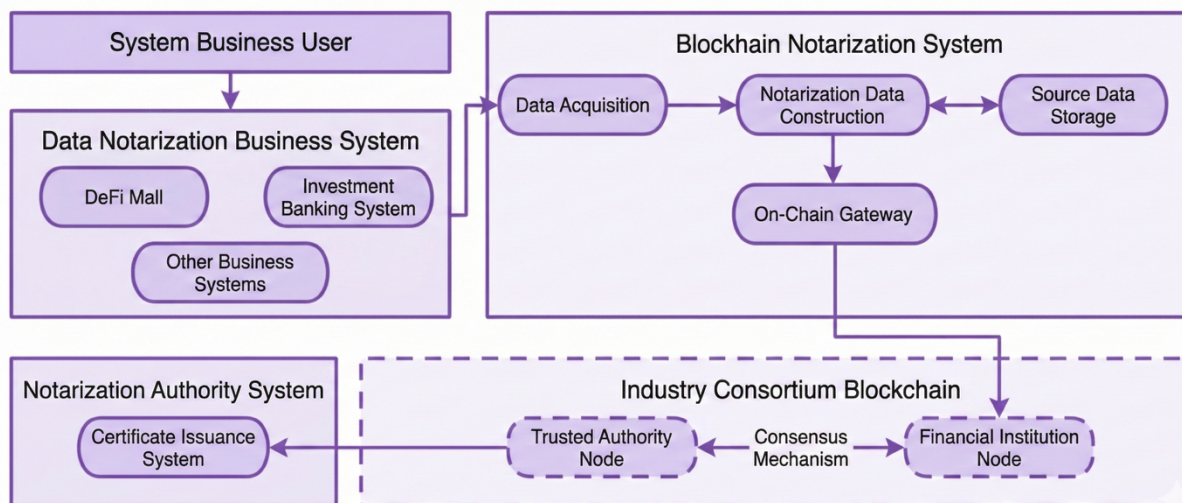# 01 Theoretical Analysis of Securities Firms' Public Chain Layout

As licensed traditional financial institutions, securities firms must prioritize regulatory constraints and business demands when deploying emerging businesses like blockchain domestically and abroad. This paper first analyzes the core matching points between current blockchain technology and securities business, as well as the regulatory policy guidance and frameworks for public chain deployment, laying a theoretical and policy foundation for the subsequent analysis of decision logic.

1.1 Internal Control and Compliance: Emphasizing Authenticity of Working Papers and Responding to Regulatory Requirements

Mainland securities firms are constrained by the CSRC's "penetrating and continuous supervision" requirements and must ensure the authenticity and traceability of investment banking working papers, asset management product operations, and transaction records. Blockchain technology can achieve data immutability through "hash on-chaining and timestamp solidification"—for example, after investment banking working papers are audited by lawyers and accountants, their hash values are stored on-chain in real-time (e.g., the Securities Industry Deposit Consortium Chain). Regulators can retrieve on-chain hashes at any time to compare with original working papers to verify authenticity. Simultaneously, smart contracts can automatically record working paper modification logs (e.g., modifier, time, content) to meet continuous supervision requirements.

Referring to the *Specification for Blockchain Electronic Data Deposit Application in the Securities Industry* [1] (T/SAC 004—2024) released by the Securities Association of China and pilot data, adopting the consortium chain architecture for deposit storage drove an overall processing efficiency increase of over 1/3 in GF Securities' Asset-Backed Securitization (ABS) business [2]. Furthermore, according to the China Banking Association, in the core "confirmation letter" (bank confirmation) link, blockchain platforms compressed the average response cycle from about 15 days to 2-3 days (with the fastest being minute-level) [3].

Figure 1: Blockchain Deposit Platform System Framework

Source: *Application Specification for Blockchain-Based Electronic Data Preservation in the Securities Industry*

1.2 Client Appropriateness Management: Achieving Traceability and Non-Repudiation of Client Actions

Securities firms must adhere to the principle of client appropriateness, ensuring that client actions (such as risk assessments and product subscriptions) are authentic, voluntary, and traceable. Blockchain technology can convert client operational behaviors (such as clicking confirm, signing) into on-chain transaction records containing "client identity ID, operation time, operation content," which are tamper-proof and traceable. For example, when a client subscribes to a private equity product, their risk assessment results, product prospectus reading records, and subscription confirmation operations are all stored on-chain. In the event of a subsequent dispute, on-chain records serve as legal evidence, avoiding the risk of clients "denying operations." Additionally, Distributed Identity (DID) technology can integrate client identity information across multiple platforms, achieving "one-time authentication, multi-scenario reuse," improving client experience while ensuring compliant management of identity information (conforming to the *Personal Financial Information Protection Technical Specification*[4]).

Figure 2: Cinda Securities and Client Transaction Contract Dispute Disclosed by China Judgements Online

Source: China Judgments Online

1.3 New Business Expansion Directions: Broadening the Boundaries of Investment Banking and Asset Management

Traditional securities business is limited to standardized assets like stocks and bonds. Blockchain technology can help securities firms expand into the tokenization of non-standardized assets (such as real estate, artwork, new energy facilities), providing clients with full-category asset allocation services. For example, Hong Kong securities firms can participate in RWA tokenization issuance (e.g., GCL Energy Technology's PV asset RWA financing of 200 million RMB)[5], offering clients opportunities for "small investments in high-value assets." Domestic securities firms can conduct digital asset credential circulation for accounts receivable via consortium chains, helping SMEs revitalize assets while providing fixed-income products to clients. Furthermore, the cross-border nature of public chains helps global top-tier securities firms break through regional network limitations—for instance, J.P. Morgan's Onyx platform (now named Kinexys) enables cross-border collateral settlement via blockchain[6], covering institutional clients in 20+ countries, effectively broadening the boundaries of cross-border business.

02 Regulatory Policy Systems for Securities Firms' Blockchain Business

Considering the significant differences between the financial regulatory systems of the Mainland and Hong Kong, as well as differing regulatory inclinations regarding blockchain and crypto-asset businesses, this paper analyzes the regulatory policy systems separately to improve the pertinence of the conclusions.

2.1 Mainland Policy System for Securities Firms' Blockchain Business

2.1.1 Policy Tone Analysis

(1) Prudent and Inclusive

Prudence is an inherent attribute of financial regulation. Regarding the emerging technology of blockchain, Mainland regulators first emphasize bottom-line thinking on risk to prevent systemic financial risks caused by technology applications. Inclusiveness reflects support for innovation, providing room for trial and error for securities firms' blockchain pilots, and avoiding a "one-size-fits-all" prohibition on the technology.

Blockchain technology has diverse application scenarios in securities business, with significant differences in risk levels and technical complexity across scenarios. Meanwhile, there are gaps in technical R&D capabilities and risk control levels among different securities firms. Based on this, Mainland regulators have effectively adopted a principle of tiered supervision, implementing differentiated supervision based on business risk levels and securities firm qualifications to avoid wasting regulatory resources while ensuring precise and effective regulation. In practice, there is a relatively large difference in regulatory approach between businesses involving simple data storage/info sharing (no fund flow), businesses with small-scale fund flows and limited impact, and businesses involving large-value fund flows, cross-market linkages, or innovative models.

(2) Emphasis on Technical Security and Data Compliance

Regarding technical security, regulators require blockchain systems to meet financial-grade security standards. The CSRC, in the *14th Five-Year Plan for Scientific and Technological Development of the Securities and Futures Industry*[7], clarified that securities firm blockchain systems must pass Level 3 or above National Network Security Grading protection, and core data must be encrypted using National Cryptography algorithms to prevent data leakage or tampering. Additionally, Mainland regulators require securities firms to establish emergency response mechanisms for blockchain systems, formulating contingency plans for node failures, cyber-attacks, and other emergencies to ensure continuous business operation.

Regarding data compliance, Mainland regulators strictly require securities firms' blockchain businesses to comply with the *Data Security Law* and *Personal Information Protection Law* [8][9], prohibiting illegal collection or use of client data. For example,

when using blockchain technology for client identity authentication, clear authorization must be obtained from the client, and client personal information must not be uploaded to public blockchain networks. Cases involving cross-border data transmission require filing through the national data cross-border security management platform to ensure data export security. Furthermore, Mainland regulators require securities firms to manage on-chain data by classification, implementing access control for sensitive data (such as client asset information and transaction records), allowing only authorized personnel to query and operate.

(3) Ideally Achieving Functionality to Serve the Real Economy

On the level of serving the real economy, Mainland regulators prioritize supporting securities firms in using blockchain technology to solve pain points in the real economy. For instance, in the field of supply chain finance, SMEs face difficulties and high costs in financing due to accounts receivable occupation. Securities firms use blockchain technology to digitize accounts receivable into divisible and circulating digital creditor rights certificates. SMEs can use these certificates to apply for financing from banks or securities firms, significantly shortening the financing cycle and reducing financing costs. This also aligns with the core tone of the entire Mainland financial system serving the real economy.

2.1.2 Regulatory Framework Analysis

(1) Top-Level Design Emphasizes Technology at the Core

Top-level design is the master plan of the regulatory framework, formulated by national-level departments such as the State Council, the People's Bank of China (PBOC), and the CSRC. It clarifies the strategic positioning, development goals, and regulatory principles of securities firms' blockchain business, providing guidance for the entire regulatory system. From the perspective of policy documents, top-level design is mainly implemented through "National Plans + Regulatory Guidance Opinions." The *14th Five-Year Plan for Digital Economy Development*[10] released by the State Council in 2021 explicitly proposed to "promote the compliant application of blockchain technology in the financial sector, and support institutions such as securities and insurance to use blockchain technology to optimize business processes and improve risk control capabilities," incorporating securities firms' blockchain business into the national digital economy development strategy and establishing its legal status and development direction. In 2022, the *FinTech Development Plan (2022-2025)*[11] jointly released by the PBOC, CSRC, and other departments further detailed the requirements, proposing to "establish regulatory rules for securities firms' blockchain business, standardize technology application scenarios, and prevent technical and financial risks," providing a basis for regulators to formulate specific policies.

(2) Multi-Departmental Collaborative Supervision, Forming Regulatory Synergy

The PBOC is responsible for regulating payment settlement and digital currency-related businesses involved in securities firms' blockchain operations, preventing risks such as money laundering and terrorist financing. For application scenarios involving Digital RMB (e.g., securities firms using Digital RMB for client fund settlement), the PBOC conducts special supervision to ensure the compliant use of Digital RMB. The CSRC, as the competent authority for the securities industry, assumes core regulatory responsibilities, responsible for formulating specific rules for securities firms' blockchain business (such as business access, risk prevention, compliance requirements), reviewing pilot applications from securities firms, conducting daily supervision and on-

site inspections, and penalizing violations. The Ministry of Industry and Information Technology (MIIT) is responsible for regulating the security and standardization of blockchain technology itself, leading the formulation of Blockchain Technology Architecture Security Requirements [12]. Securities firms' blockchain systems must also meet technical standards such as data encryption, node management, and smart contract security, and pass testing by third-party institutions recognized by the MIIT. The Cyberspace Administration of China (CAC) is responsible for regulating data security and network security involved in securities firms' blockchain business, preventing problems such as data leakage and cyber-attacks. For blockchain systems involving overseas nodes, the CAC also needs to review the compliance of cross-border data transmission to prevent data export risks.

(3) Local Pilot Logic

The Mainland habitually adopts the logic of local pilots first, gaining experience, and then rolling out nationwide for the promotion of major innovative technologies. The layout of blockchain technology in securities business is no exception. Such local pilots mainly rely on policy highlands such as "Free Trade Zones" and "FinTech Pilot Cities," which usually have the advantages of high policy flexibility, good industrial foundations, and concentrated securities firm resources. In June 2025, the Central Financial Commission issued the Opinions on Supporting the Acceleration of Shanghai as an International Financial Center [13], proposing to effectively maintain financial security under open conditions, use technologies such as blockchain, big data, and artificial intelligence to strengthen forward-looking research and timely judgment of risks. It aims to prevent and resolve cross-border financial risks and establish and improve a cross-border capital flow monitoring, early warning, macro-prudential assessment, and coordinated linkage system adapted to high-level opening up.

In summary, Mainland regulators highly emphasize technical compliance, data security, and the practical application value of blockchain technology. They require securities firms to focus on the needs of the real economy and their own business demands when deploying related businesses, and to conduct pilots appropriately in areas with policy incentives. It is recommended to focus on grasping this policy guidance.

2.2 Hong Kong Policy System for Securities Firms' Blockchain Business

2.2.1 Policy Tone Analysis

Hong Kong views blockchain and crypto-assets as key components of financial innovation but prioritizes investor protection, market integrity, and financial stability. The overall regulatory path is "innovation available, risk controllable," balancing technological development with systemic risk control through phased system design, clarifying licensing and compliance requirements, and leveraging regulatory sandboxes and cross-regulatory coordination.

(1) Balancing Innovation and Risk, Defining Compliance Baselines

Hong Kong regulation does not seek total liberalization or strictly prohibit technology implementation via bans. Instead, it judges based on "activity and risk." Different licensing, operational, and compliance requirements are imposed on different activities (spot trading, market making, custody, asset management, stablecoin issuance,

staking, etc.). Stricter access and continuous supervision are implemented for high-risk links (e.g., high-volatility token sales to retail, fiat exchange/payment functions).

This paper believes that in the process of conducting related businesses in Hong Kong, it is necessary to focus on clarifying the compliance baseline of Hong Kong regulators. First, the Securities and Futures Commission (SFC) explicitly proposed the "99.5% Principle," meaning the crypto asset industry currently accounts for only 0.5% of the total revenue of enterprises in its regulatory portfolio, so any innovation must be premised on not shaking the health of the traditional financial system[14]. The core mechanism is the liquidity segregation mechanism, requiring licensed brokers and funds to partner only with licensed Virtual Asset Trading Platforms (VATPs) to prevent risk spillover to the traditional market. Even if the "Global Order Book" is launched in 2025 to allow licensed platforms to share liquidity with overseas affiliated platforms, it still requires overseas platforms to deposit funds in advance, adopt payment-versus-delivery settlement, and establish real-time monitoring systems to ensure transaction security.

Investor protection is another compliance baseline of Hong Kong regulation. It requires strict access for retail investors, allowing licensed platforms to provide retail investors only with high-liquidity, low-risk virtual assets (such as non-security tokens included in mainstream indices), and requires a 12-month trading record (the 2025 new regulations have exempted this restriction for professional investors). Platforms need to pass KYC and risk assessments to ensure that recommended investment products match the client's risk tolerance and retain the right to refuse high-risk transactions. The 2025 new regulations allow professional investors to trade virtual assets without trading record requirements, including more innovative tokens, but platforms still need to ensure asset transparency and compliance.

In addition to the above two points, Hong Kong regulation also requires relevant financial institutions to operate with licenses. That is, all crypto-asset trading platforms, stablecoin issuers, and custody service providers must obtain licenses from the SFC or the HKMA and pass the "fit and proper" assessment (including financial soundness, management experience, and compliance records).

(2) Dynamic Assessment of Global Developments

Given the cross-border nature of crypto-assets, Hong Kong regulation emphasizes continuous tracking of the movements of the UK, Singapore, the EU, the US, and international organizations (FATF, IOSCO, etc.), and making localized adaptations: absorbing mature practices (such as trading platform licensing, stablecoin reserve rules, high AML/CFT standards) while retaining local flexibility (e.g., differentiated treatment of market service objects and business models). Regulators typically achieve dynamic adoption through public consultation, pilots, and phased implementation. This involves many overseas laws and regulations, which this paper will not discuss one by one due to space limitations.

(3) Emphasis on Substance Over Form

Hong Kong regulation clearly states that regulation is not determined by labeled names, but by the economic and legal substance of the business ("Same Activity, Same Regulation"). For example, if a "tokenized security" or "token with security properties" appears, it will be handled according to the securities rules and offering/distribution regulations of the *Securities and Futures Ordinance* (SFO); if a token actually performs

payment and settlement functions, banking/payment regulations and specific stablecoin rules must be considered to reduce arbitrage space.

2.2.2 Regulatory Framework Analysis

Based on our summary and review of regulatory policies, Hong Kong is gradually building a framework for securities firms' blockchain business regulation composed of "Dual Core Regulators + Clear Standards by Scenario + Continuous Promotion via Regulatory Sandbox."

(1) Dual Core Regulatory Bodies: Securities and Futures Commission (SFC), Hong Kong Monetary Authority (HKMA)

Dual core regulatory bodies refer to two main regulatory agencies/functions in the regulatory system: one is the Securities and Futures Commission (SFC), and the other is the Hong Kong Monetary Authority (HKMA). Both perform their respective duties, divide regulatory responsibilities, and maintain coordination.

The SFC is the main regulatory body for Hong Kong's securities and futures markets, regulating virtual assets or trading platforms existing in the form of securities or futures based on the *Securities and Futures Ordinance* (SFO) and relevant regulations[15]. Specific functions include: Requiring licenses for Virtual Asset Trading Platforms (VATPs) operating in Hong Kong or providing services to Hong Kong investors. According to the SFC website, "Centralized Virtual Asset Trading Platforms" must obtain regulatory approval if they provide services to Hong Kong investors. Formulating operational guidelines for VATPs, setting requirements for platform eligibility, conduct, internal control, customer asset custody, anti-money laundering/counter-terrorist financing (AML/CFT), network security, and client appropriateness. Providing regulatory circulars and guidelines for asset managers, funds, and distribution products containing virtual asset exposure.

The HKMA is Hong Kong's central bank and banking regulator, primarily responsible for regulating banks, payment systems, stored value facilities, stablecoin issuance, and related financial infrastructure. Its functions are reflected as follows: Formulating a specific regulatory regime for stablecoin issuance. According to the HKMA website, the "Stablecoin Issuer Regulatory Regime" takes effect on August 1, 2025, implementing a licensing system. Also, formulating regulatory guidelines for banks or authorized institutions (AIs) engaging in virtual asset-related services (such as custody, staking, lending), collaborating closely with the SFC.

The SFC and HKMA have different focuses; the former leans towards "Securities - Trading Platform - Asset Management" scenarios, while the latter leans towards "Banking / Payment / Stablecoin / Payment Infrastructure" scenarios.

(2) Clear Standards by Scenario: Differentiated Regulation from Trading Platforms to Stablecoins

Based on our summary analysis of relevant regulatory policies from the SFC and HKMA, the regulatory standards of Hong Kong financial regulators for various business scenarios are organized as follows.

Virtual Asset Trading Platform (VATP): When a platform provides trading services to Hong Kong investors (especially centralized matching, automated matching engines, token trading + custody), it must apply for a license from the SFC. The *VATP Guidelines* (2023 edition) list many standards: eligibility, conduct, internal control, network security, client asset segregation, market manipulation prevention, continuous

disclosure, etc.[16]. Furthermore, the SFC website clarifies: VATPs must perform safe custody, KYC/AML, transaction monitoring, prevention of market abuse, accounting and auditing, and network security. Below is the list of licensed and applying platforms periodically published in "Hong Kong Licensed Virtual Asset Trading Platforms" for reference[17].

Figure 3: List of licensed virtual asset trading platforms in Hong Kong

Company Name	trading platform	Central Number	Authorization Date
OSL Digital Securities Limited	OSL Exchange	BPJ213	December 15th, 2020
Hash Blockchain Limited	HashKey Exchange	BPL992	November 9th, 2022
Hong Kong Virtual Asset Exchange Limited	HKVAX	BPW549	October 3, 2024
Hong Kong Digital Asset EX Limited	HKbitEX	BPO721	December 18th, 2024
Accumulus GBA Technology (Hongkong) Co., Limited	Accumulus	BUA970	December 18th, 2024
DFX Labs Company Limited	DFX Labs	BUN619	December 18th, 2024
EXIO Limited	EX.IO	BUT670	December 18th, 2024
Panthertrade (Hong Kong) Limited	PantherTrade	BUY578	January 27th, 2025
YAX (Hong Kong) Limited	YAX	BUT913	January 27th, 2025
Bullish HK Markets Limited	Bullish	BUQ956	February 18th, 2025
Hong Kong BGE Limited	BGE	BSI739	June 17th, 2025

Source: Hong Kong Securities and Futures Commission official website

Crypto Asset Custody / Token Lending / Staking: Hong Kong financial regulators have issued special guidance for banks and institutions engaging in staking services (i.e., locking client virtual assets in blockchain validation mechanisms to earn rewards). For example: internal control requirements, client asset segregation, conflict of interest management, and secure infrastructure requirements. In addition, regulators are currently consulting on a proposed "Virtual Asset Custodian / Trading / Intermediary" licensing regime.

Stablecoin Issuance: Stablecoins (especially fiat-referenced stablecoins) are a regulatory focus. HKMA policy documents state that from August 1, 2025, stablecoin issuers must be licensed. Issuers must meet capital requirements, hold high-quality liquid reserve assets, have redemption mechanisms, and are prohibited from paying interest on the token itself.

Asset Management: If a fund or asset management product holds virtual assets, the SFC requires managers to assess five core dimensions: valuation, liquidity, custody, security, and audit, and disclose relevant risks.

Product Design, Lending/Financing, Derivatives (Pending Regulation): Regulators are currently also consulting on regulatory proposals for scenarios such as virtual asset trading, lending, staking, derivatives, and tokenized assets. The SFC / FSTB issued a consultation on "VA Dealers & VA Custodians" in 2025[18].

(3) Continuous Promotion via Regulatory Sandbox

The SFC's regulatory sandbox mechanism, since its launch in September 2017, has become a core tool for promoting innovation in FinTech and virtual assets. Under the ASPIRe virtual asset regulatory roadmap framework, the mechanism has been continuously upgraded, forming a dynamic regulatory system covering diverse scenarios such as virtual asset trading platforms, RWA tokenization, and cross-border settlement[19].

The SFC regulatory sandbox is open to two types of entities. The first type is licensed institutions, such as virtual asset trading platforms that have already obtained SFC Type 1 (Securities Trading) or Type 7 (Automated Trading Services) licenses. The second type is start-ups, which need to demonstrate technological innovation, compliance commitment, and market value, such as projects optimizing securities settlement processes through blockchain technology. During the testing period, participants can conduct business within limited user scope, transaction scale, and geographical restrictions, while reporting data in real-time to the SFC (such as smart contract audit results, user complaint records) and undergoing stress tests to assess risk controllability.

The HKMA's Fintech Supervisory Sandbox (FSS) and Fintech Facilitation Office (FFO), although not established exclusively for crypto-assets, are applicable to related innovative businesses. The Fintech Supervisory Sandbox (FSS), launched in September 2016[20], allows banks and their partnering technology companies (tech companies) to conduct pilot trials of their fintech initiatives involving a limited number of participating customers without fully complying with the HKMA's regulatory requirements. This arrangement enables banks and tech companies to collect data and user feedback to improve new initiatives, thereby accelerating the launch of new technology products and reducing development costs.

Regarding the tokenization direction, the HKMA held the launch ceremony for the Project Ensemble Sandbox (Sandbox) on August 28, 2024[21], and announced that the first phase of trials will cover four main tokenized asset use case themes, marking a significant step forward in the practical application of tokenization technology in the financial industry. After fully considering industry intentions, market development trends, and the potential impact of innovative development, the first phase of Sandbox trials will cover the tokenization of traditional financial assets and real-world assets, focusing on four themes: fixed income and investment funds, liquidity management, green and sustainable finance, and trade and supply chain finance. To consolidate Hong Kong's status as an international financial center and open up new economic fields with an innovative spirit, the HKMA will continue to actively communicate with the industry to understand their interest in tokenization development and jointly develop and identify new themes and use cases related to tokenization.

Figure 4: Eddie Yue, Chief Executive of the Hong Kong Monetary Authority, delivering the opening remarks at the launch ceremony of the Ensemble Project Sandbox

Source: Official website of the Hong Kong Monetary Authority (HKMA)

Considering that this field features rapid technological iteration and novel regulatory challenges like staking, DAOs, and tokenized assets, this combination of sandbox testing and phased deployment allows regulators to observe first, correct later, and then promote.

In summary, Hong Kong financial regulators have a more positive attitude towards securities firms' public chain layout. Although currently experiencing some cooling due to certain window guidance, we predict that as the progress of the crypto-asset industry in the US, Singapore, and other countries accelerates, there is still an expectation of moderately relaxing regulatory boundaries. Under this regulatory framework, securities firms and blockchain developers need to actively meet the regulatory compliance baseline regarding licensing access and investor protection, and conduct differentiated public chain development for different businesses. To further enhance competitiveness, it is recommended to actively layout in frontier directions involved in the regulatory sandbox to effectively seize the opportunity.

03 Decision Logic Analysis of Securities Firms' Public Chain Layout

Based on the theoretical and policy analysis above, combined with the current business practice of domestic and foreign securities firms, we will categorize and discuss the public chain layout decision logic of Mainland securities firms, Hong Kong securities firms, global leading securities firms, and fintech securities firms.

3.1 Mainland Securities Firms' Public Chain Layout Decision Logic: Compliance First, Consortium Chains Adapt to Short-term Needs

Considering the attitude and logic of Mainland regulation, the public chain layout decision of Mainland securities firms is mainly constrained by three major factors: "strong policy constraints, weak business demand, and high cost inputs." The core logic is to satisfy compliance requirements with the lowest cost, and not to consider public chain layout in the short term. Specifically:

3.1.1 Compliance Priority: Highly Emphasizing the Rigid Constraint of Regulatory Boundaries

Mainland regulation of blockchain technology is based on the tone that consortium chains are the compliant path. Securities firms' layout of public chains faces two major compliance obstacles: First, the conflict between decentralization and regulation. The decentralized nature of public chain nodes makes it difficult for regulators to implement penetrating management, which is inconsistent with the CSRC's requirements for real-time monitoring and controllable risk. Second, data cross-border risks. Global nodes of public chains may lead to the exit of client data and business data, violating the requirement of "local storage of important data" in the *Data Security Law*. In contrast, the "node controllable, data regulatable" characteristics of consortium chains perfectly adapt to Mainland compliance requirements—for example, the Securities Industry Deposit Consortium Chain only allows licensed securities firms and regulatory agencies as nodes, and data is stored on domestic servers, meeting dual requirements of penetrating supervision and data security.

3.1.2 Business Value Anchoring: Precise Solution to Key Traditional Business Pain Points

Mainland securities firms' current blockchain business is concentrated in scenarios such as data deposit, investment banking working paper management, and client appropriateness tracing. The core requirements of these scenarios are data immutability and traceability, which consortium chains can fully satisfy without relying on public chains. For example, in investment banking working paper deposit, the hash value of the working paper can be put on-chain through the consortium chain, allowing regulators to verify authenticity at any time, avoiding the problems of easy tampering with traditional paper working papers and easy loss of electronic working papers. In client appropriateness management, putting client risk assessment and product subscription operations on-chain realizes "operation non-repudiation," effectively

reducing the client dispute rate. In asset management product net value disclosure, real-time on-chaining of product net value data allows investors to query via the consortium chain, improving information transparency and reducing investor complaint rates.

These scenarios do not involve areas where public chains excel, such as "global liquidity and high-concurrency transactions." The technical performance of consortium chains is sufficient to adapt, and the technical advantages of public chains cannot be converted into business value.

3.1.3 Resource Constraints: Achieving Technological Optimization Under Hard Cost Constraints

Self-developing a public chain or external selection involves high costs, while Mainland securities firms' blockchain business has not yet formed a profit model, limiting resource input. From the cost structure perspective, self-developed public chain costs include technical teams (blockchain engineers, security experts), infrastructure (node servers, O&M), and compliance certification (multi-departmental filing, auditing), requiring large annual investment and continuous iteration, making it difficult to recover costs in the short term. Although the cost of external selection is lower than self-research, it requires paying public chain Gas fees, technical adaptation fees (such as smart contract modification), and compliance audit fees, and faces policy risks. Compared with the above two, consortium chains have lower costs. Multiple securities firms jointly build (such as the Securities Industry Deposit Consortium Chain) to share R&D costs, and it fully meets regulatory requirements.

Therefore, under high costs and unclear profitability, even thinking from a market-oriented perspective, Mainland securities firms will naturally choose the low-cost path of consortium chain cooperation and will not consider public chain layout for the time being.

3.2 Hong Kong Securities Firms' Public Chain Layout Decision Logic: Innovation Driven, External Selection Adapts to Business Needs

Considering the attitude and logic of Hong Kong financial regulation, the public chain layout of Hong Kong securities firms aims at quickly entering innovative businesses and obtaining incremental revenue. The decision logic is to obtain licenses and technical capabilities with controllable costs, with external selection of public chains being the optimal solution. Specifically:

3.2.1 Compliance Basis: Regulatory Attitude Towards the External Public Chain is the Core Entry Ticket

Hong Kong's regulation of securities firms' blockchain business centers on licensing management. Securities firms need to obtain corresponding licenses first, then choose adapted technical paths. External docking with mature public chains can reduce compliance costs in specific scenarios, but attention must be paid to the SFC's regulatory boundaries. On one hand, if a securities firm uses a public chain, it still needs to prove compliance through third-party security audits (such as smart contract vulnerability detection) and risk disclosure, while warning of risks such as "51% attacks, on-chain data irreversibility" of public chains in product documents. On the

other hand, public chain ecosystem compliance tools need to meet localization requirements. Specifically, they must first meet the FATF Travel Rule standards and pass Hong Kong local compliance tests. Simultaneously, they need to connect with the securities firm's internal KYC/AML processes and suspicious transaction reporting mechanisms (such as binding on-chain address risk scores with client identity information) to meet the requirements of the *Anti-Money Laundering Ordinance*.

Figure 5: License requirements for various businesses by Hong Kong financial regulatory authorities		
Business Type	**Core required licenses**	**Additional requirements/instructions**
Virtual asset trading business	Class 1 (securities trading)+Class 7 (automated trading services) license	Need to apply for "Virtual Asset Service Additional Permission" from SFC, and cannot directly use traditional Class 1 license
Virtual asset custody	Upgraded Class 9 (Asset Management) License	Need to meet technical requirements such as "separation of hot and cold wallets, multiple signatures"
Advisory services for tokenized securities issuance	Category 6 (Institutional Financing Opinion) License	Additional compliance plan for virtual assets needs to be submitted
Stablecoin issuance	Stablecoin issuer license	You need to apply separately to the Hong Kong Monetary Authority and meet the requirements of "100% reserve certificate, smart contract suspension mechanism", etc
Source: Hong Kong Monetary Authority, Hong Kong Securities and Futures Commission		

In actual operation, Hong Kong securities firms mostly adopt the form of docking public chains through licensed exchanges (such as OSL, Hashkey) rather than directly accessing public chain nodes. For example, GF Securities Hong Kong chose the Ethereum Layer 2 extension network HashKey Chain to conduct tokenized securities business. HashKey Chain, as the associated infrastructure of a licensed virtual asset exchange (HashKey Exchange), meets the SFC's regulatory requirements for tokenized securities, effectively shortening the issuance and listing cycle of tokenized securities products and significantly reducing compliance costs[22].

3.2.2 Compliance Basis: Regulatory Attitude Towards the External Public Chain is the Core Entry Ticket

(1) Asset Tokenization Business: Emphasizing On-chain Ecosystem Maturity

Asset tokenization refers to the process of registering and circulating traditional financial assets (such as bonds, stocks, fund shares, real estate equity, etc.) in a blockchain form. For securities firms, this process is not only a technical issue but also involves compliance, liquidity, and custodial capability. Therefore, in this type of business, securities firms pay more attention to the ecological maturity and institutional acceptance of the public chain. There are three main points to focus on.

First is the completeness of the developer and application ecosystem. An active developer community can continuously provide smart contract tools, security audit services, and application innovations. For example, Ethereum's leading position in token

standards (ERC-20, ERC-1400, ERC-3643, etc.) gives it a clear advantage in the field of security tokens.

Second is compliance compatibility capability. Asset tokenization often needs to meet requirements such as investor whitelists, KYC verification, and transfer restrictions. Choosing a public chain that supports permission management and programmable compliance logic can effectively reduce regulatory friction. For example, some Hong Kong institutions adopt Ethereum-based permissioned layer solutions to ensure that tokenized assets only circulate among compliant investors.

Finally, liquidity and interoperability. Mature public chains usually have extensive DeFi ecosystems and cross-chain bridges, enabling tokenized assets to possess potential secondary market liquidity and supporting docking with services like stablecoins and custody wallets, thereby enhancing the market attractiveness of assets.

(2) Settlement and Clearing Business Emphasizes Public Chain Performance

Unlike asset tokenization, clearing and settlement business emphasizes transaction efficiency and system reliability. In tokenized securities or virtual asset trading, securities firms need to ensure that funds and assets can achieve atomic delivery-versus-payment (DvP) to avoid settlement risks. This places high demands on public chain performance. Specifically, the settlement and clearing system needs to possess high throughput (TPS) to support institutional-level batch transactions; low confirmation latency to ensure fund transfer and asset delivery are completed almost in real-time; network stability and security to prevent congestion, rollbacks, or chain fork events leading to settlement failure; and predictable transaction costs so that securities firms can accurately calculate fees and control operating costs.

Therefore, in settlement and clearing scenarios, high-performance public chains (such as Solana, Pharos, Avalanche, or Ethereum-based high-performance Layer 2 solutions like Arbitrum) receive more attention from securities firms. Some securities firms even consider adopting hybrid architectures, using dedicated subnets for links with high performance requirements to balance performance and compliance.

Due to space limitations, this paper focuses on explaining public chain selection requirements in two specific business scenarios. Demands in other business scenarios can be referred to in the explanation of business practice details in the final chapter of this paper.

3.2.3 Actively Participating in Innovation: Pre-emptive Layout in Regulatory Sandbox is a Plus

Under Hong Kong's current fintech regulatory framework, the regulatory sandbox provides a mechanism for financial institutions to test innovative businesses in a controlled environment. For securities firms intending to conduct blockchain-related businesses, entering the sandbox means being able to test innovative functions including tokenized securities issuance, on-chain clearing and settlement, digital identity verification, and compliant custody under the supervision of regulators. Through sandbox experiments, securities firms can not only verify technical feasibility but also understand in advance the specific requirements of regulation on business processes, data security, and client protection.

On the level of crypto-asset trading platform compliance, the SFC's sandbox is a key stage for platforms to obtain formal licenses. For example, after HashKey Exchange passed the sandbox test in 2022, it became one of the first licensed platforms,

currently supporting spot trading of Bitcoin, Ethereum, etc., and exploring derivatives business. HKbitEX was approved in December 2024, with its sandbox testing focusing on cross-chain asset exchange and institutional-grade custody services, with user asset scale reaching 1 billion HKD during the testing period[23]. The SFC requires platforms to verify key metrics such as order matching efficiency and cold/hot wallet separation mechanisms within the sandbox.

On the RWA level, the sandbox is also a key implementation stage for subsequent tokenization. For example, GCL Energy Technology's PV power station RWA raised 200 million RMB through token issuance in sandbox testing, with an expected annualized return exceeding 5%, and realized cross-border settlement time shortening from 3 days to minute-level.

Securities firms adopting external mature public chains have a natural advantage in sandbox testing but need to pass additional compliance modifications (such as node real-name authentication) to meet Hong Kong regulatory requirements. Since external public chains already have stable technical architectures, extensive ecological support, and auditable security foundations, securities firms can quickly complete access and verification, shortening the cycle from proof of concept to actual deployment. This approach helps securities firms to lead in establishing compliant and feasible business models during the stage of gradual regulatory opening, seizing market opportunities. At the same time, through continuous testing and feedback in the sandbox, securities firms can also influence the formation of regulatory policies and promote industry standardization and system improvement.

3.3 International Leading Securities Firms and Fintech Securities Firms' Public Chain Layout Decision Logic: Layer 2 Architecture Self-Research, Controlling Core Standards

Considering the space relationship of the whole article and research completeness, this paper only simply summarizes the public chain layout situation of international leading securities firms and fintech securities firms, rather than a systematic logical analysis and discussion.

In the context of global financial digital transformation, more and more international leading securities firms and fintech securities firms are beginning to actively deploy blockchain and public chain infrastructure. Compared to early simple participation in tokenization projects or utilizing third-party public chains to deploy applications, the strategies of these institutions are significantly upgrading: they tend to self-develop Layer 2 architectures or sidechain systems on top of existing mainstream public chain ecosystems (such as Ethereum), thereby controlling key standards, reducing compliance risks, and occupying a core position in the future digital asset settlement network.

First, from the perspective of technical architecture and controllability, leading financial institutions generally hope to balance open ecosystems with autonomous control. Although mainstream public chains (such as Ethereum, Solana) have mature ecosystems and sufficient liquidity, their open, transparent, and immutable characteristics mean that transaction privacy, data sovereignty, and performance predictability are difficult to fully meet institutional-level needs. By self-developing Layer 2 architectures (such as schemes based on ZK-Rollup, Optimistic Rollup, or

Validium), securities firms can achieve graded management of on-chain data visibility, retaining the open attribute of interoperability with the mainnet while ensuring compliance, privacy, and security control through an independent settlement layer. This architecture can support the concept of "Regulated Open Finance," providing a technical foundation for financial institutions to achieve compliant innovation in the public chain ecosystem.

Second, from the perspective of compliance and regulatory adaptation, self-developed Layer 2 architectures can more flexibly embed regulatory interfaces and compliance controls. When facing different market regulatory systems, international securities firms need to dynamically implement requirements such as KYC/AML (Know Your Customer/Anti-Money Laundering) mechanisms, transaction traceability, and permission management. If relying entirely on external public chains, these functions often need to be implemented through additional middleware or whitelist contracts, presenting problems of operational complexity and regulatory inconsistency. By self-developing Layer 2 networks, institutions can embed compliance logic at the underlying protocol layer, achieving "Compliance by Design," thereby more efficiently connecting with financial regulators in various countries, especially possessing significant strategic value under the EU MiCA Act, US SEC regulatory expansion, and Hong Kong and Singapore tokenization regulatory frameworks.

Finally, from the perspective of ecosystem and standard competition, international leading securities firms are more concerned with controlling the discourse power of future digital financial infrastructure. The competition in blockchain is ultimately not just about performance and cost, but about who can define and lead key interfaces and asset mapping standards. Through self-developing Layer 2, securities firms can establish an institutional-grade standardized protocol layer, such as Tokenized Asset Registry standards, Settlement Messaging Formats, and On-chain KYC Frameworks. When more and more assets and institutions run based on these standards, the party developing Layer 2 becomes the standard setter and network hub of the "next-generation financial infrastructure."

For example, Goldman Sachs and JPMorgan have respectively promoted the docking of internal blockchain systems (such as GS DAP, Onyx) with external ecosystems and are actively researching how to be compatible with the Ethereum ecosystem; while fintech securities firms like Robinhood are researching high-speed trading and cross-chain clearing solutions based on Layer 2. The common logic of these actions is: through self-developing interoperable Layer 2 systems, master the core standards and pricing power of the next-generation financial network.

04 Typical Cases: Practice Verification of Decision Logic

This paper effectively responds to the public chain layout logic of international leading securities firms, Hong Kong securities firms, and Mainland securities firms discussed in Chapter 3 through three examples: JPMorgan Chase, CMB International, and Huatai Securities. The specific analysis is as follows.

4.1 Self-Research Evolution Case: JPMorgan's "Private Chain - Consortium Chain - Layer 2" Path

4.1.1 Private Chain Stage Mainly for Business Exploration

In the early stage of blockchain technology, JPMorgan first chose the R&D mode of Private Blockchain. The core goal of this stage was to reduce innovation risk while ensuring data security and privacy. Through the private chain, JPMorgan could conduct experiments such as transaction settlement, asset custody, and smart contract testing in an internal closed environment, ensuring that new technology would not have uncontrollable impacts on core business systems.

JPMorgan's private chain mode mainly focused on three cores: security and privacy control, performance and scalability, and business model verification: all nodes were controlled by the bank internally, ensuring transaction data and sensitive information were not accessed externally; meanwhile, the characteristic of limited internal nodes allowed the private chain to achieve high TPS (Transactions Per Second), meeting the needs of large-value payments and transaction settlements; additionally, the bank could verify the automation potential of complex business processes like cross-border payments, internal clearing, and derivatives trading through the private chain, laying the foundation for subsequent external expansion.

JPMorgan's "JPM Coin" was one of the exploration results in this stage. It is a digital currency built on the Quorum (JPMorgan's open-source enterprise version of Ethereum) private chain, used to optimize cross-border payments and instant settlement, significantly improving capital flow efficiency. [24]

4.1.2 Consortium Chain Stage Mainly Focuses on External Collaboration and Standardization

After successful private chain verification, JPMorgan extended technology application to cross-institution scenarios, entering the consortium chain stage. JPMorgan's core practices in the consortium chain mode included inter-bank settlement and clearing, smart contract standardization, and compliance assurance: achieving real-time settlement and asset transfer among multiple banks through the consortium chain, reducing intermediate links and improving transparency; meanwhile, formulating reusable smart contract templates on-chain to reduce technical friction in multi-institution collaboration; additionally, meeting regulatory requirements of different jurisdictions through node permissions, data sharding, and audit mechanisms.

The application of the Quorum consortium chain further reflected the strategic nature of JPMorgan's technological evolution. By extending the successful experience of the internal private chain to external partners through the consortium chain, it achieved business scale and gradually shaped the blockchain standards of the financial industry.

4.1.3 Layer 2 Architecture Self-Research Stage Emphasizes Scalability and Accessibility

With the development of the blockchain ecosystem and the rise of DeFi and digital asset markets, JPMorgan realized that relying solely on private chains and consortium chains was difficult to meet larger-scale transaction and innovation needs. Thus, its technology strategy evolved to the Layer 2 (Second Layer Scaling Solution) stage[25]. The core value of Layer 2 is: achieving efficient transaction processing on top of the main chain (Layer 1) while maintaining security and the final settlement's capability of the main chain.

JPMorgan's core R&D points in the Layer 2 stage include high-performance transaction processing, compatibility with public chains, and compliance & regulatory controllability: achieving high TPS transactions through technologies like state channels and Rollups to reduce on-chain congestion and fee costs; meanwhile, Layer 2 can access public chains or consortium chains, providing broader liquidity and cross-ecosystem access capabilities for its financial products; additionally, necessary permission controls and audit capabilities can still be retained on Layer 2 to meet compliance requirements of different countries and regions.

This Layer 2 architecture not only supports high-frequency businesses like cross-border payments, digital asset trading, and securities settlement but also provides technical preparation for future docking applications of Digital RMB or Central Bank Digital Currencies (CBDC). JPMorgan's Layer 2 evolution shows its active embrace of the blockchain open ecosystem while maintaining financial security and regulatory compliance, achieving a balance between innovation and stability.

4.2 Consortium Collaboration Case: Trusted Reporting of Huatai Securities Investment Banking Business Quality to SAC

4.2.1 Case Background

The Securities Association of China (SAC) launched the Investment Banking Business Self-Regulatory Platform[26], covering five major functions: investment banking business electronic working paper directory management, electronic working paper random inspection, investment banking business conduct management, sponsor representative practice behavior information management, and investment banking quality evaluation. Securities firms can report investment banking business data to the SAC through the "Zhenglian Chain" (Securities Alliance Chain) blockchain infrastructure. The Investment Banking Business Self-Regulatory Platform is integrated by the SAC based on the working paper supervision system and quality evaluation system, gathering five core functions including supporting the SAC's investment banking business electronic working paper directory management, electronic working paper random inspection, investment banking business conduct management, sponsor

representative practice behavior information management, and investment banking quality evaluation work.

Figure 6: Reporting workflow for investment banking working papers via blockchain technology

Source: Guidelines on the Development of an Electronic Management System for Investment Banking Working Papers of Securities Companies

According to the consultation draft, regarding working paper directory information, the reporting method was modified to interact directly with Zhenglian Chain nodes or IPFS (InterPlanetary File System). Some project information fields and project member information were simplified, while the reporting working paper directory structure requirements remained unchanged. Securities firms need to report projects undertaken since January 1, 2021, according to the requirements of the *Guidelines for the Construction of Electronic Management Systems for Investment Banking Business Working Papers of Securities Companies*[27]. Project types for reporting are detailed in the data dictionary project types. Securities firms are allowed to prioritize reporting working paper directory information before reporting complete project information, and subsequently supplement complete project information.

Huatai Securities actively responded to the call of the Securities Association of China and participated in the "Securities Industry Alliance Chain" project launched by the SAC, aimed at improving the technological supervision capability of the securities industry through blockchain technology, promoting digital transformation, and forming a co-built, co-governed, and shared industry digital ecosystem. The quality of investment banking practice is one of the important standards for measuring the investment banking business capabilities of securities companies. To adapt to the needs of the registration-based system reform and implement relevant requirements of the

CSRC, in 2022, the Investment Bank Cloud Business System took the lead in joining the Zhenglian Chain application, completing the docking of the practice quality evaluation system with the Zhenglian Chain. Using the characteristics of traceability and immutability of blockchain technology, practice quality self-assessment information is reported to the SAC according to standards, enhancing regulatory transparency and efficiency.[28]

4.2.2 Innovation Achievements

Huatai Securities deployed Securities Industry Alliance Chain nodes and IPFS nodes in its internal computer room to join the Zhenglian Chain network. The investment banking business system only needs to dock with the internal node to carry out real-time data reporting, building a penetrating supervision model based on blockchain. This realized the electronic archiving of the entire chain and full cycle of investment banking business supervision, achieving full traces and automatic collection functions realized by technologies such as full-process automation robots, effectively improving the convenience of use of the company's investment banking business evaluation system and improving reporting efficiency.

In terms of business innovation, through the reasonable use of automatic collection functions and the reasonable setting of system validation rules, this system avoids the working mode of purely manual filling, uploading, and checking whether files are complete and pass validation. It effectively improves the consistency and accuracy of relevant information and the completeness of working paper files, reducing the risk of regulatory penalties caused by missing working paper files. After the project went online, a total of more than 900 projects were reported in 2023, completing more than 1500 reporting tasks. Compared with traditional methods, it greatly improved reporting efficiency and regulatory efficacy.

4.2.3 Industrial Value

This system is a case of financial institution business deposit reporting and filing to regulators, applicable to application scenarios with demands for improvement in regulatory efficacy, solving pain points and difficulties such as untimely, inaccurate, and non-standard reporting. The functions of this system can meet the quality evaluation specification requirements of the Securities Association of China, filling the gap of online collection, review, and reporting to the association by investment banking personnel, saving manpower for project team members and quality control review. At the same time, it can effectively save time costs for financial institutions and regulatory departments, improve the accuracy and timeliness of obtaining various quality evaluation data and files, and improve reporting efficiency.

4.3 External Selection Case: CMB International and Solana Collaboration on Tokenized Fund

4.3.1 Background and Demand

On August 8, 2025, CMB International (CMB International), a subsidiary of China Merchants Bank, announced a partnership with Singapore digital exchange DigiFT and Solana public chain service provider OnChain to tokenize a USD Money Market Fund mutually recognized in Hong Kong and Singapore. It issued the token CMBMINT on-chain. Notably, this is the first appearance of a tokenized fund spanning multiple

jurisdictions, and being led by an Asian financial giant will provide a very good compliance sample for subsequent multi-region cooperative RWA. [29]

Behind this fund tokenization project, forces from multiple parties in traditional finance and the blockchain field gathered. CMB International Asset Management provided high-quality fund assets and regulatory compliance guarantees, DigiFT provided the on-chain issuance and trading platform, and OnChain was responsible for underlying technology deployment and public chain distribution support. The three parties worked together to achieve the on-chain issuance of the traditional money market fund.

4.3.2 Business Analysis

The underlying asset being tokenized is the CMB International USD Money Market Fund (CMBMINT). This is a USD-denominated money market fund established in February 2024. 70% of the funds are invested in low-volatility instruments such as short-term high-quality USD deposits, treasury bills, and commercial paper, and 30% are invested in non-USD-denominated short-term deposits and high-quality money market instruments, aiming for capital preservation and stable returns overall.

Since its establishment, the fund has performed excellently. As of July 31, 2025, it ranked first among similar money market funds in Bloomberg Asia Pacific. Being a Hong Kong-Singapore mutual recognition fund, the fund accepts supervision from both places, and its investors are positioned as qualified professional investors. Therefore, the current project first limits subscription of fund tokens to accredited investors in Singapore through the DigiFT platform to ensure participants meet local regulatory requirements (depending on the degree of regulatory opening in the future, it may expand to institutional clients in Hong Kong and other jurisdictions).

OnChain embedded the entire tokenization process into its self-developed on-chain capital market infrastructure, providing comprehensive technical support. First, in terms of compliance architecture and asset tokenization security, OnChain introduced a "Transfer Hook" mechanism based on the Solana Token-2022 standard, ensuring fund tokens can only be redeemed through the contract, putting an end to private transfers, thereby strengthening transaction compliance.

Simultaneously, it adopts a dual-standard architecture of SPL and Token-2022, ensuring compatibility with other on-chain assets while possessing flexible liquidity programming capabilities, and avoiding traditional fund settlement delays through a real-time net value anchoring mechanism. Secondly, in the subscription and redemption links, OnChain built a full-link security protection system, separating core functions such as fund management, liquidity pools, and token minting into different PDA addresses through permission isolation to prevent single-point risks. It strictly limits key operators through a whitelist mechanism, including fund company access and large transaction approval. It also introduces real-time asset and permission scanning, bidirectional net value calculation, and net value update time limits in the full link to ensure price stability and account accuracy.

Finally, in liquidity management, OnChain designed a layered liquidity architecture, specifically meeting instant redemption needs through an independent redemption pool (redeem_cash_pool) to avoid liquidity runs; meanwhile, providing dual modes of instant redemption and delayed redemption, intelligently allocating based on liquidity conditions within the pool, and ensuring principal safety under extreme market conditions through a multi-account asset isolation mechanism, thereby achieving a near T+0 fund arrival experience.

4.3.3 Industrial Value

As an on-chain version of a Hong Kong-Singapore mutual recognition fund, CMBMINT adopted an innovative and robust mode in its regulatory compliance architecture. The fund itself is still regulated by the Hong Kong SFC and the Monetary Authority of Singapore (through the mutual recognition mechanism), while the issuance and trading of tokens are conducted under the platform of Singapore licensed institution DigiFT. This "dual regulation" architecture ensures that the underlying assets and trading environment are in a legal and compliant state. At the same time, the smart contract of the fund token has undergone strict security audits and introduced risk reserve and proof of reserve mechanisms to ensure on-chain assets are safe, transparent, and fully backed.

4.4 Ant Group Case: Full Stack Layout from Consortium Chain to Public Chain Services

4.4.1 AntChain: Reconstructing Supply Chain ABS with "Dual-Chain Connect"

In the Mainland market, AntChain reconstructed the trust mechanism of traditional supply chain finance through the "Dual-Chain Connect" (Shuang Lian Tong) platform, effectively solving the pain points of difficulty in confirmation and circulation faced by SMEs. The core of this model lies in using consortium chain technology to convert the credit of core enterprises into divisible and circulating digital creditor rights certificates, enabling capital flow, information flow, and logistics to achieve "three flows in one" on-chain, compressing the financing efficiency of supply chain end enterprises from traditional months to seconds. For securities firm investment banking, this architecture significantly reduces due diligence costs in Asset-Backed Securitization (ABS) business, ensuring the authenticity of the trade background of underlying assets through the immutability of on-chain data, achieving a transformation from entity credit to on-chain digital credit.

In addition, AntChain constructed a "Trust Base" connecting the physical world and digital finance through the fusion of "IoT + Blockchain" in its technical architecture. By implanting "AntChain Inside" modules, the operation data of physical assets (such as photovoltaic panels, charging piles, warehousing equipment) can be put on-chain in real-time, ensuring the uniqueness and real operating status of underlying assets. Typical cases include Ant Digital Technologies joining hands with GCL Energy Technology to promote energy intelligence, realizing the digitization and valuation of photovoltaic assets through blockchain technology, successfully supporting related RWA financing projects, and providing a solid technical path for securities firms to conduct innovative ABS business based on IoT data.

4.4.2 Jovay: RWA Exclusive Compliant Layer 2

Jovay adopted the positioning of "institutional-grade compliance" from the beginning of its design. It does not issue native tokens itself, thereby eliminating the compliance concerns of traditional financial institutions regarding token-related businesses. It aims to solve the pain points of high gas fees and transaction congestion on the Ethereum mainnet. By providing financial-grade high-concurrency processing capabilities and deterministic settlement services, it provides an efficient and controllable on-chain execution environment for institutions to issue and manage real-world asset tokens.

In the strategic architecture of "Two Chains and One Bridge," Jovay plays the key role of "Capital and Transaction Hub." It connects seamlessly with the Mainland's AntChain (Asset Chain) through a trusted cross-chain bridge, enabling physical assets verified by IoT to be mapped as digital assets on the Jovay chain and directly dock with the liquidity of the global Web3 market. In the green financing case of Towngas, Jovay successfully supported the RWA tokenization issuance of energy assets. Its sub-second transaction confirmation speed and atomic settlement capability ensured the precise execution of complex financial instructions, providing the most core trading infrastructure for securities firms to conduct cross-border asset securitization.

4.4.3 ZAN: Focusing on Web3 Compliant Infrastructure Services

Targeting Hong Kong and overseas markets, Ant Group launched the compliance-oriented Web3 technology brand ZAN. Its strategic positioning is not to repeat the construction of underlying public chains, but to serve as an infrastructure service provider connecting traditional finance and the Web3 ecosystem. Given the strict requirements of Hong Kong regulation on Virtual Asset Trading Platforms (VATPs) and RWA businesses regarding anti-money laundering and fund tracing, ZAN encapsulates the identity authentication and risk control capabilities accumulated by Ant in the traditional finance field into standardized services. It provides institutions with one-stop compliance solutions including Electronic Know Your Customer (eKYC), on-chain transaction Know Your Transaction (KYT), and smart contract audits, helping financial institutions securely access the public chain ecosystem without touching underlying complex technologies.

In specific business practice, ZAN's technical services have become an important bridge connecting Mainland high-quality assets with overseas funds. In the RWA scenario, through the "Two Chains and One Bridge" architecture, ZAN assists institutions in mapping Mainland physical asset data (such as new energy facility operation data) to Hong Kong under a compliance framework, supporting asset tokenization issuance and cross-border financing. Meanwhile, as a technology partner, ZAN actively supports the compliance construction of mainstream licensed virtual asset exchanges in Hong Kong. By providing high-concurrency, low-latency node services and full-link security protection, it effectively reduces the technical threshold and compliance risk for institutions to conduct Web3 innovative businesses.

4.4.4 Advantage Analysis of Ant System Technology Selection

The core advantage of the Ant system technology selection lies in its construction of the strategic synergy capability of "Two Chains and One Bridge," perfectly adapting to the rigid needs of securities firms conducting cross-border business under a dual regulatory environment. On the Mainland side, its self-developed consortium chain architecture fully supports National Cryptography algorithms and Xinchuang (IT Application Innovation) standards, ensuring that supply chain finance and working paper deposit businesses comply with the *Data Security Law*; on the Hong Kong side, its compliance components can seamlessly dock with mainstream public chain ecosystems like Ethereum. This closed-loop architecture of "Assets Inside, Capital Outside" allows securities firms to connect with global liquidity through Hong Kong while compliantly utilizing high-quality Mainland entity assets, avoiding the regulatory fragmentation risk that a single technology path might face.

From the perspective of underlying technology performance and security, AntChain possesses high concurrency processing capabilities verified by "Double 11" massive

transactions, able to support financial-grade high-frequency settlement needs, solving the performance bottleneck of traditional blockchains. At the same time, its unique "IoT + Blockchain" full-stack technical capability can provide penetrating trust guarantees from physical hardware to on-chain assets for securities firms' RWA business, which is more difficult to forge or tamper with compared to pure software-type public chain solutions. This "hard technology" barrier combined with deep financial risk control genes gives Ant system technical solutions a natural competitive advantage and compliance premium when facing complex financial scenarios requiring penetrating supervision.

05 / Core Technical Points for Public Chain Practice in Domestic and Foreign Securities Firms' Related Businesses

From Chapter 2 to Chapter 4, this paper first analyzed the theoretical logic of securities firms' blockchain business layout and fully studied the regulatory guidance and frameworks of Mainland and Hong Kong regulators for securities firms' public chain layout. Subsequently, based on the above theoretical + regulatory policy analysis, combined with securities firms' businesses, the decision logic for domestic and foreign securities firms' public chain layout was given.

To supplement subsequent practice details, Chapter 5 of this paper focuses on discussing: if relevant securities firms and blockchain technology developers need to lay out such businesses, what R&D directions and technical details need to be focused on during the specific business development process.

5.1 Mainland Securities Firms: Recommended to Focus on Two Consortium Chain Business Directions: Electronic Deposit and Transaction Traceability

Under policy frameworks such as the *Specification for Blockchain Electronic Data Deposit Application in the Securities Industry* (T/SAC 004-2024), *Guidelines for Construction of Blockchain and Distributed Ledger Technology Standard System*[30], and *Evaluation Rules for Financial Applications of Blockchain Technology*[31] (JR/T 0193-2020), securities firms' public chain layout needs to center on "Compliance First, Scenario Landing," where electronic deposit and transaction traceability are the most urgent internal compliance demand scenarios. Both types of scenarios need to closely follow policy technical requirements and business operation pain points, detailing implementation from dimensions of technical selection, process design, privacy protection, and audit traceability, ensuring compliance with regulations while solving actual business problems.

5.1.1 Electronic Deposit: Landing with "Compliant Verifiability, Secure Controllability" as Core

Electronic deposit is a foundational compliance scenario for securities firms, covering key data such as investment banking working papers, client agreements, and transaction vouchers. Policy explicitly requires it to meet three core goals: "Tamper-proof, Traceable, Privacy Protection." In practice, implementation details need to be disassembled from three levels: technical architecture, process design, and compliance validation:

(1) Technical Architecture Level

Policy clarifies that securities firm deposit must use consortium chains, and nodes must be "authorized access." In practice, this consortium chain node should include three types of core roles. Core nodes are securities firm headquarters and local branches, responsible for business data on-chaining and consensus participation; node access needs to pass "qualification review + technical verification." Credibility nodes need to dock with local courts, notary offices, and judicial appraisal centers; nodes need to synchronize on-chain deposit data in real-time, using dedicated line encrypted communication to ensure deposit data has judicial validity. Regulatory nodes need to reserve access interfaces for the CSRC and local securities bureaus, supporting real-time queries of deposit data by regulatory departments; interface calls need dual-factor authentication.

On the level of cryptographic algorithms and key management, emphasis is on compliant algorithms + hardware secure storage. Policy requires cryptographic algorithms to conform to GM/T 0111-2021. In practice, algorithm selection and key control need to be detailed. Data hashing needs to use the SM3 algorithm to process deposit data (such as investment banking working paper files). Digital signatures need to use the SM2 asymmetric encryption algorithm. Securities firm node private keys are stored in Hardware Security Modules (HSM) to avoid soft encryption leakage risks. Key backup needs to adopt "off-site three-copy" backup, stored respectively in securities firm headquarters, off-site disaster recovery centers, and cooperative bank vaults; backup media must conform to National Password Administration certification.

On the ledger design level, emphasis is on dual guarantees of tamper-proof + traceability. The ledger needs to contain a "Block Header + Block Body" structure. In practice, field design and data synchronization rules need to be clarified. Mandatory fields in the block header include Previous Block ID (32-bit hash), Timestamp (accurate to milliseconds, docking with National Time Service Center), Merkle Tree Root (containing all transaction hashes), and Block Height (auto-incrementing sequence). New nodes need to synchronize full historical data, using "breakpoint resume + hash verification" during synchronization. If the network is interrupted, synchronization continues from the last successfully synced block height after recovery. After synchronization is complete, the local Merkle Tree Root must be compared with other nodes; if inconsistent, re-synchronization is required.
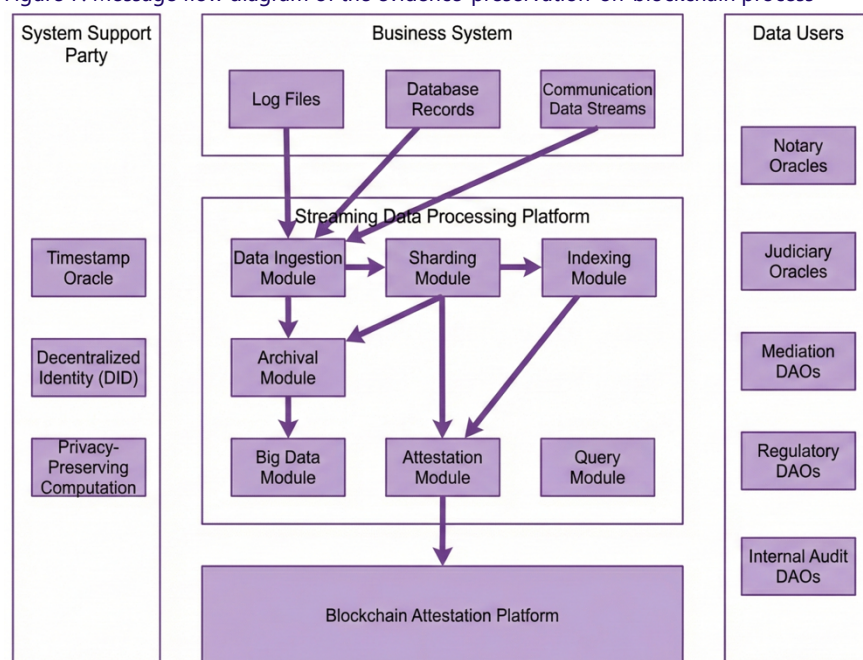
(2) Process Design Needs to Cover the Full Link of "Data Construction - On-chaining - Certification"

Deposit data construction needs to adopt dual processing of structuring + de-identification. Policy requires deposit data to be "compliant, complete, de-privatized." In practice, templates need to be designed according to business scenarios. Investment banking working paper deposit template fields need to include "Project Number, Working Paper Name, Working Paper Hash, Uploader, Upload Time," where "Project Issuer Information" needs to be de-identified.

On-chain mechanisms are selected on demand. Policy allows "real-time, asynchronous, scheduled batch" on-chaining. In practice, matching is based on data characteristics. Real-time on-chaining is often suitable for key data like investment banking working papers and major transaction vouchers, with on-chain response time ≤ 1 second, using "distributed transaction + compensation mechanism"; if on-chaining fails, auto-retry 3 times (interval 10 seconds); if failed again, trigger SMS alert to the O&M team. Scheduled batch on-chaining is suitable for client browsing logs and non-critical operation records, processed in batches every 5 minutes, with batch size not exceeding

1000 items/batch; data integrity needs to be verified before on-chaining (e.g., matching log count with hash).
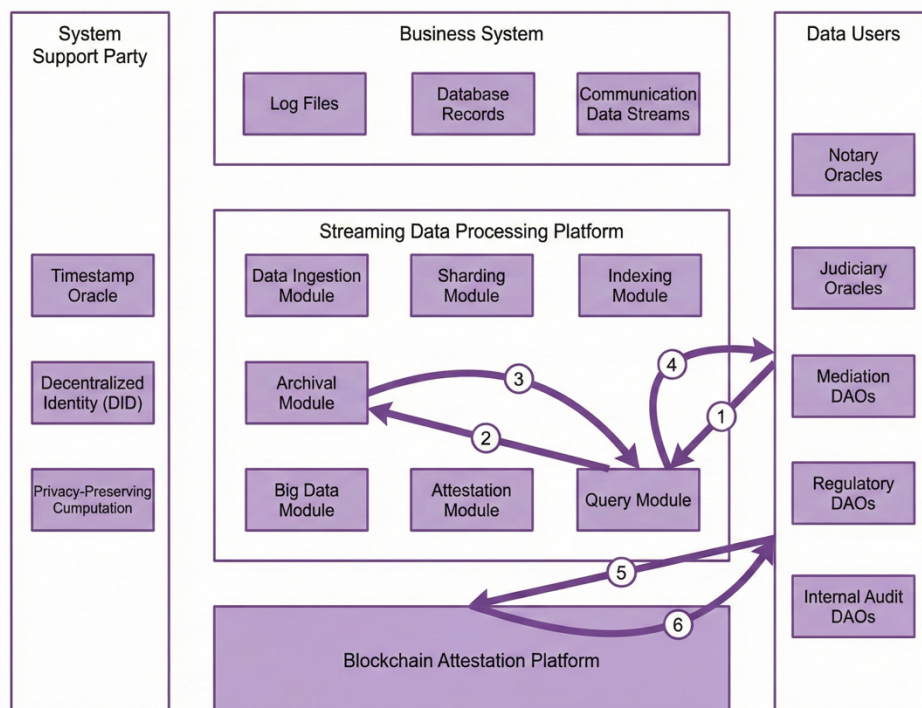
Figure 7: Message flow diagram of the evidence-preservation-on-blockchain process

Source: Application Specification for Blockchain-Based Electronic Data Preservation in the Securities Industry

The certification link needs to dock with credibility institutions (such as courts, notary institutions, arbitration institutions, auditing institutions, judicial appraisal centers, etc.) to ensure verifiability. Policy requires certification data to "originate directly from the consensus ledger." In practice, the certification process needs to be simplified. During certification, the user submits an application on the securities firm APP, uploading "ID + Business Voucher." The system automatically verifies the association between the applicant and the deposit subject (e.g., client agreement deposit needs to match client account). Certification records need to include "Applicant, Application Time, Report Number, Verification Node," kept for ≥ 6 years (conforming to *Securities Law* archive retention requirements), supporting retrieval by regulatory departments.

Source: Application Specification for Blockchain-Based Electronic Data Preservation in the Securities Industry

(3) Compliance Validation Needs to Embed Privacy Protection and Audit Logs

Privacy protection needs to adopt a method of graded processing of sensitive data. According to policy documents, deposit data needs to distinguish "Sensitive/Non-sensitive." High-sensitivity data (such as client mobile numbers, bank card numbers) need to adopt "Anonymization + Encrypted Storage"; only hashes are stored on-chain, original text needs to be encrypted with SM4 algorithm, and keys are autonomously managed by clients (e.g., via APP key vault). Medium-sensitivity data (such as transaction amounts) need to use "De-identification," e.g., amount displayed as "100*** Yuan," with complete data only visible to regulatory nodes. Non-sensitive data (such as project names): can be put on-chain in plaintext, but data source must be annotated (e.g., "Securities Firm Investment Bank Dept 1").

Audit logs need to guarantee full-link traceability. Policy requires the deposit behavior process to be traceable. In practice, three types of logs need to be recorded. The first type is operation logs, which need to contain "Operation User, Operation Time, Data ID, Operation Type (Add/Modify/Delete)," and logs must be tamper-proof (using blockchain deposit). The second type is system logs, which need to record system behaviors like node synchronization, algorithm calls, and key updates, retained for ≥ 6 months. The third type is audit logs, which need to generate deposit compliance reports periodically (monthly), containing "On-chain Data Volume, Certification Count, Abnormal Data Volume," automatically pushed to the compliance department.

5.1.2 Transaction Traceability: Landing with "Full-Link Concatenation, Compliance Validation" as Core

Transaction traceability is a key scenario for securities firms to prevent compliance risks, covering businesses such as public fund entrusted order placement, stock trading, and investment advisory services. Policy requires transaction processes to be traceable and operational behaviors to be trackable. In practice, landing needs to be achieved through "Data Concatenation, Compliance Validation, Performance Guarantee."

(1) Adopting Unique Coding Rules for Transaction Links during Data Concatenation

Policy clarifies that chain data needs to "have logical cross-check relationships." In practice, unified coding rules and data models need to be designed. Specifically, the unique coding rule for transaction links points out the coding format as "Client Account (12 digits) + Business Type (2 digits, e.g., 01=Fund Order, 02=Stock Trading) + Date (8 digits) + Random 6 digits", for example "622600000001012024520123456". This code runs through the entire transaction process, and data in each link is associated with this code, ensuring that traceability can "check the whole chain with one click."

Figure 9: Evidence-preservation model for public mutual fund entrusted order-placement operations

Level 1 Classification	Level 2 Classification	Level 3 Classification
Attestation Entity Info	Entity Basic Details	--
	Entity Node Details	--
Attested Data Details	Client Account Details	--
	Product Details	Login Events
	Transaction Lifecycle Events	Browsing History
		Suitability Checks
		Agreement Signatures
		Order Placements

Source: Application Specification for Blockchain-Based Electronic Data Preservation in the Securities Industry

(2) Adopting Real-time Rule Check + Post-event Traceability during Compliance Validation

Real-time compliance validation refers to the system automatically verifying compliance before the transaction goes on-chain to avoid non-compliant transactions. The first item is appropriateness matching check; if the client risk level is lower than the product risk level, the system automatically intercepts the order and triggers a manual review process. The second item is transaction limit check; if the client's single-day entrusted amount exceeds the regulatory limit, the system automatically prompts, requiring client confirmation before going on-chain. The third item is identity check; placing an order requires verifying the client's digital signature (SM2). If the signature is invalid, on-chaining is refused, ensuring the operator is the client themselves.

Post-event traceability functions need to be designed with multi-dimensional query functions in practice. The first item is Client-side Query; clients can query "Traceability Records of Last 1 Year" in the APP, displaying operation time, key data (after desensitization), and hash value for each link, supporting download of traceability reports. The second item is Employee-side Query; account managers can query transaction traceability records authorized by clients to answer client questions. Queries need to record "Employee ID, Query Time, Client Authorization Voucher." The third item is Regulator-side Query; regulatory departments can query full volume data (including un-desensitized information) through dedicated interfaces. Interfaces need to conform

to "IP Whitelist + Dual Factor Authentication," and query records are put on-chain in real-time.

(3) Meeting High Concurrency, Low Latency Needs in Performance Guarantee

Policy documents have clear requirements for transaction performance. In practice, technical optimization is needed for guarantees. In transaction throughput optimization, "Data Sharding + Parallel Consensus" can be adopted, sharding by "Client Account Tail Number" (e.g., 0-9 for 10 shards). In query performance optimization, local caching (Redis Cluster) can be established for high-frequency queried transaction data (e.g., records of the last 3 months), with cache expiration time set to 1 hour and query response time ≤ 500 ms; historical data (exceeding 3 months) adopts "Indexing + Archiving," establishing indexes by "Date + Business Type," querying the index first then calling archived data to avoid full volume scanning. Abnormal recovery guarantee is also relatively important. If nodes lose power or network fluctuates, missing transaction data needs to be automatically synchronized after recovery. Synchronization adopts "Incremental Sync + Hash Verification" to ensure data is consistent with other nodes after recovery; meanwhile, the system needs to record "Abnormal Time, Affected Transaction Count, Recovery Time" and generate an anomaly report to submit to the compliance department.

In summary, securities firms' public chain layout in electronic deposit and transaction traceability scenarios needs to avoid "technology for technology's sake" and must closely adhere to three cores. First is policy alignment; all technical selections (such as algorithms, chain types) and process designs (such as certification, traceability) need to correspond to the *Specification for Blockchain Electronic Data Deposit Application in the Securities Industry* and *Evaluation Rules for Financial Applications of Blockchain Technology* to ensure every step has a policy basis. Second is business adaptation; avoid excessive technicalization. For example, deposit templates need to fit the actual needs of investment banking and brokerage businesses without increasing the operational cost of frontline employees (e.g., automatically capturing working paper hashes without manual upload). Finally, risk controllability; establish a risk control system of "Pre-event Verification, In-process Monitoring, Post-event Audit" to ensure risks are discovered and disposed of early.

5.2 Hong Kong Securities Firms: Parsing Business and Technical Requirements under Five Major Innovation Scenarios

Hong Kong securities firms should rely on the advantages of policy support and mature ecosystems, focusing on external selection, corresponding to different innovative businesses. Their corresponding specific practice points are as follows:

5.2.1 Asset Tokenization

Business logic is that traditional securities, bonds, fund shares, or physical assets (such as gold, real estate, carbon emission rights) realize digital, divisible, and traceable tokenized forms through blockchain, supporting compliant issuance and secondary market circulation. Representative projects include: GF Securities (HK) × HashKey Chain: First end-to-end on-chain tokenized security. UBS × Ethereum: Issuance of Hong Kong's first tokenized warrant. HSBC × Tokenised Gold, etc. [32]

Figure 10: Sorting out the technical requirements related to asset tokenization

Technical/Compliance Requirements	Corresponding public chain characteristics
① Compliance auditable, KYC integrated	Public chains need to support Permitted Layers (such as Sub network or Whitelisted Smart Contracts)
② High reliability asset custody	Requires multi signature, account abstraction (AA), and institutional level wallet mechanism
③ Accurate settlement and programmable rules	To support smart contract security standards (ERC-1400, ERC-3643, etc.)
④ High throughput and low gas cost	Public chains need to have scalability, such as Solana, Polygon, Avalanche subnets

Source: Relevant regulatory documents from the Hong Kong Securities and Futures Commission and the Hong Kong Monetary Authority

5.2.2 Crypto Asset Trading and Clearing

Business logic is securities firms directly achieving trade matching, clearing, settlement, and fund delivery (atomic settlement) on the blockchain, reducing traditional custody links and improving transparency. Representative projects such as HashKey Exchange (Licensed VATP) × HashKey Chain / Ethereum. OSL × Polygon and Ethereum ecosystem.

Figure 11: Technical Requirements for Digital Asset Trading and Clearing

Technical/Compliance Requirements	Corresponding public chain characteristics
① Real time settlement capability	High TPS and low latency (such as Solana, Aptos)
② Data traceability and tamper proof	On chain native transaction log integrity Merkle proof
③ Institutional level privacy protection	Support ZK or privacy layer (zkEVM, Aztec, zk Rollup solutions)
④ Regulatory Node	Enable regulatory nodes to view real-time partial on chain data (most commonly Ethereum Layer 2 or consortium chain extensions)

Source: Relevant regulatory documents from the Hong Kong Securities and Futures Commission and the Hong Kong Monetary Authority

5.2.3 Crypto Asset Trading and Clearing

Business logic is that securities firm client information, compliance records, and investor type verification realize shared and verifiable identity management through on-chain credentials (Verifiable Credential) or Soul-Bound Tokens (SBT). Representative projects like HKMA × Hong Kong Cyberport × Financial Institutions cooperation "Digital Identity Sandbox." HashKey ID × Financial Institution public chain access pilot.

Figure 12: Technical Requirements for Customer Identity and Compliance Verification

Technical/Compliance Requirements	Corresponding public chain characteristics
① Revocable/Updated Identity Certificate	Support controllable SBT and VC standards (EIP-4973)
② Confidentiality and Minimum Disclosure	Capable of ZKP technology (Polygon ID, zk Sync, Linea)
③ Regulatory cooperation	Must support regulatory interface (on chain/off chain bridge for KYC)
Source: Relevant regulatory documents from the Hong Kong Securities and Futures Commission and the Hong Kong Monetary Authority	

5.2.4 Cross-Institution Settlement and Tokenized Payment

Business logic is that when securities firms issue or trade tokenized assets, they need to complete cash settlement directly on-chain (Tokenised Deposit or CBDC delivery), reducing time differences and credit risks. Representative projects such as: HSBC Tokenised Deposit Project (Chain-based cash management based on corporate clients). Project mBridge (HKMA × PBOC Digital Currency Institute × BIS).

Figure 13: Sorting out the technical requirements related to cross institutional settlement and tokenized payments

Technical/Compliance Requirements	Corresponding public chain characteristics
① Support stablecoins linked to central banks or commercial banks	Public chains need to be compatible with the CBDC/Regulated Stablecoin protocol
② Atomic Delivery (DvP) Mechanism	Native support for atomic swap/conditional settlement is required
③ Traceable and settlement controllable	Need to have regulator node or token freezing functionality
Source: Relevant regulatory documents from the Hong Kong Securities and Futures Commission and the Hong Kong Monetary Authority	

5.2.5 Client Rights and Fund Management

Business logic is digitizing fund shares, shareholder registration, and dividend distribution processes through blockchain to improve registration efficiency and transparency. Representative projects such as: Asia Allied Infrastructure × HSBC × HashKey RWA Pilot. Franklin Templeton × Stellar and Polygon fund tokenization precedents have demonstration significance for Hong Kong securities firms.

Figure 14: Technical Requirements for Customer Equity and Fund Management

Technical/Compliance Requirements	Corresponding public chain characteristics
① Controllable shareholder register	Public chains need to support whitelist and update functions
② On chain profit distribution	Smart contracts need to support regular dividends and tax retention
③ Data Protection and Privacy	Support privacy layer or off chain data storage mechanism
Source: Relevant regulatory documents from the Hong Kong Securities and Futures Commission and the Hong Kong Monetary Authority	

06 Conclusion

The decision logic of traditional securities firms' public chain layout is not a purely technical choice, but a comprehensive framework of policy compliance, business demands, cost constraints, and future profit expectations. The weight of factors differs for domestic and foreign securities firms. Comprehensively analyzing domestic and foreign policy frameworks, securities firms' public chain layout decision logic, and referencing various cases and specific technical practice details, we emphasize the following conclusions:

First, current Mainland regulation remains relatively cautious about securities firms deploying blockchain business, highly emphasizing the ability of blockchain technology to solve actual business problems for securities firms. Self-research of public chains and external selection are basically impossible to achieve in the short term. If wishing to conduct securities firm blockchain-related business in the Mainland, it is recommended to focus on the two consortium chain business directions of electronic deposit and transaction traceability.

Second, Hong Kong regulation is relatively inclusive regarding securities firms' layout of blockchain, and there is a possibility of certain relaxation as relevant regulatory policies and industrial layouts in the US and Singapore advance. In the short term, constrained by relatively cumbersome compliance requirements and high public chain development costs, the volume of innovative business is not yet sufficient to support Hong Kong securities firms in vigorously developing self-researched public chains. The subsequent public chain layout logic for most Hong Kong securities firms should be primarily external selection. If wishing to conduct relevant business in Hong Kong, it is recommended to conduct targeted design based on the actual business needs of the securities firm, or combine the advantages of one's own public chain to specifically match corresponding businesses.

Third, it is recommended to actively pay attention to the public chain self-research situation of international leading securities firms like JPMorgan and Goldman Sachs, as well as leading fintech securities firms like Robinhood. Their subsequent actions will have a significant impact on the business standards of global securities firms' public chain layout.

Due to space limitations, this paper still has certain research deficiencies, such as specific judgments on the trend of subsequent Hong Kong financial regulatory policy changes based on changes in financial regulatory policies and crypto-asset industry development in countries like the US and Singapore, as well as detailed comparisons of technical indicators and advantages in various business scenarios of Solana, Pharos, HashKey Chain, and various public chains. Corrections from practitioners and research experts are welcome to continuously improve it together.

References

[1] Securities Association of China. Specification for Blockchain Electronic Data Deposit Application in the Securities Industry (T/SAC 004—2024) [S]. Beijing: Securities Association of China, 2024-07-29.

[2] 21st Century Business Herald. GF Securities: Actively Exploring Digital Application Innovation, Enhancing Digital Compliance and Risk Management Capabilities [EB/OL].

[3] China Banking Association. Bank Confirmation Blockchain Service Platform Business Scale Grows Steadily, Effectiveness of Empowering Industry Digital Transformation Initially Shown [EB/OL].

[4] People's Bank of China. Personal Financial Information Protection Technical Specification (JR/T 0171—2020) [S]. Beijing: People's Bank of China, 2020-02-13.

[5] China Fortune Network. Ant Digital Technologies Joins Hands with GCL Energy Technology to Establish Ant Xinneng, Promoting Energy Intelligence [EB/OL]. (2025-06-12).

[6] Onyx DAO. An Introduction to the Onyx Protocol [R/OL].

[7] China Securities Regulatory Commission. 14th Five-Year Plan for Scientific and Technological Development of the Securities and Futures Industry [EB/OL]. (2021-10-21).

[8] Standing Committee of the National People's Congress of the People's Republic of China. Data Security Law of the People's Republic of China [EB/OL]. (2021-06-10).

[9] Standing Committee of the National People's Congress of the People's Republic of China. Personal Information Protection Law of the People's Republic of China [EB/OL]. (2021-08-20).

[10] State Council. "14th Five-Year" Digital Economy Development Plan: Chapter 4 Section 1 [EB/OL]. (2021-12-12).

[11] Ministry of Industry and Information Technology of the People's Republic of China. Blockchain Technology Architecture Security Requirements: YD/T 3747-2020 [S]. Beijing: China Communications Standards Association, 2020-10-01.

[12] Ministry of Industry and Information Technology of the People's Republic of China. Blockchain Technology Architecture Security Requirements: YD/T 3747-2020 [S]. Beijing: China Communications Standards Association, 2020-10-01: 6.2.

[13] Central Financial Commission. Opinions on Supporting the Acceleration of Shanghai as an International Financial Center [EB/OL]. (2025-06-18)

[14] Securities and Futures Commission. SFC Announces Regulatory Measures for Virtual Asset Trading Platforms, Balancing Innovation and Investor Protection [EB/OL]. (2023-06-16)

[15] Securities and Futures Ordinance, Cap. 571, Laws of Hong Kong [EB/OL]. (2002-03-08)

[16] Securities and Futures Commission (SFC). Guidelines for Virtual Asset Trading Platforms (HKEX-GL81-23): Chapter 3 "Eligibility Requirements", Chapter 4 "Conduct Standards", Chapter 5 "Internal Controls" [EB/OL]. (2023-06-16).

[17] Securities and Futures Commission (SFC). List of Licensed Virtual Asset Trading Platforms [EB/OL]. (2025-08-28).

[18] Securities and Futures Commission (SFC) & Financial Services and Treasury Bureau (FSTB). (2025, March 15). Consultation Paper: Regulatory Framework for Virtual Asset (VA) Dealers and VA Custodians.

[19] Financial Services and Treasury Bureau (FSTB) & Securities and Futures Commission (SFC). (2024, October 20). ASPIRe Virtual Asset Regulatory Roadmap: Dynamic Regulatory Framework for Diverse Scenarios.

[20] Financial Services and Treasury Bureau (FSTB). (2016, September 5). FinTech Supervisory Sandbox (FSS) Launch Announcement.

[21] Hong Kong Monetary Authority (HKMA). (2024, August 28). Launch Ceremony of the Ensemble Project Sandbox.

[22] GF Securities Hong Kong. GF Securities Hong Kong Selects HashKey Chain (Ethereum Layer 2) for Tokenized Securities Business [EB/OL]. (2024-10-18).

[23] HKbitEX. HKbitEX Secures SFC Licence (CE No. BPO721) After Sandbox Testing Focused on Cross-Chain Exchange and Institutional Custody [EB/OL]. (2024-12-18).

[24] J.P. Morgan Onyx. JPM Coin: A Digital Asset for Instant Cross-Border Payments and Settlements [EB/OL]. (2019-02-14).

[25] J.P. Morgan Institute. Evolving Blockchain Strategy: From Private/Consortium Chains to Layer 2 Scaling [R/OL]. (2024-10-20).

[26] Securities Association of China. SAC Launches Investment Banking Business Self-Regulatory Platform [EB/OL]. (2024-12-30).

[27] Securities Association of China. Notice on Issuing and Implementing "Guidelines for the Construction of Electronic Management Systems for Investment Banking Business Working Papers of Securities Companies" [EB/OL]. (2020-02-28).

[28] https://www.google.com/search?q=Caijing.com. SAC Plans to Build Investment Banking Business Self-Regulatory Platform, Optimizing Working Paper Directory Reporting Function [EB/OL].

[29] CMB International. CMB International Launches Tokenized USD Money Market Fund in Collaboration With DigiFT and OnChain [EB/OL]. (2025-08-08).

[30] Ministry of Industry and Information Technology and Three Other Departments. Guidelines for Construction of Blockchain and Distributed Ledger Technology Standard System [EB/OL]. (2023-12-29)

[31] People's Bank of China. Evaluation Rules for Financial Applications of Blockchain Technology (JR/T 0193-2020) [S]. Beijing: People's Bank of China, 2020.

[32] HSBC Holdings. (2024, September 19). HSBC pilots quantum-safe technology for tokenised gold.

Contributors

Authors: 猫咪佛陀 (𝕏@showtime9965)

Reviewers: Colin Su, Grace Gui, NingNing, Owen Chen
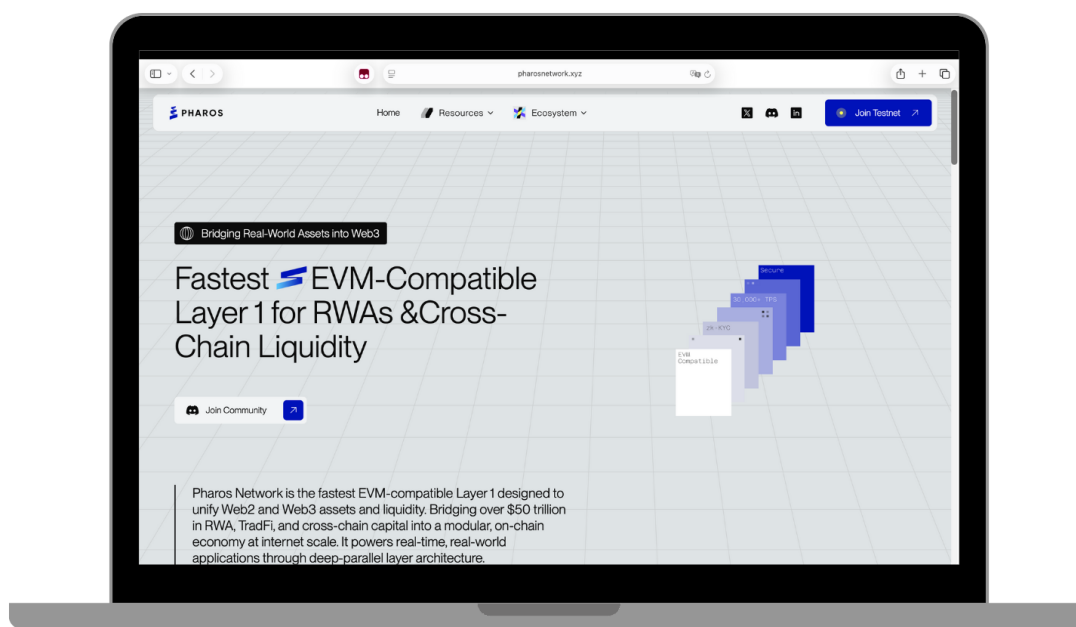
Design: Alita Li

Disclaimer

This material is prepared by Pharos Research for the purpose of providing general information. It does not constitute and should not be deemed as investment, legal, accounting, or tax advice, nor does it form an offer, solicitation, or recommendation with respect to any securities, cryptographic assets, or strategies. The information and opinions contained herein may be derived from internal or third-party sources. While efforts are made to ensure their reliability, their accuracy, completeness, or timeliness is not guaranteed. Any decisions made and risks arising therefrom shall be borne solely by the reader. Past performance is not indicative of future results. This material may contain forward-looking statements (including forecasts and scenarios), which are subject to uncertainties and not guaranteed to be achieved. Cryptographic assets are highly volatile, and total loss may occur. They are also exposed to risks such as liquidity, technology, smart contract, counterparty, and compliance risks. To the extent permitted by law, the Research Institute and/or its affiliates or researchers may hold positions in the relevant assets, have business relationships with relevant entities, or otherwise have interests that may affect the objectivity of opinions. This material is not intended for persons in restricted jurisdictions. Reading, following, or subscribing to this material does not constitute a client relationship. Without prior written permission, no institution or individual may reproduce, copy, modify, or distribute this material. Any quotation shall be objective and complete, with the source clearly credited as "Pharos Research".

Contact

Pharos Network is a next-generation public blockchain for Real-World Assets (RWA) and stablecoins, focused on asset tokenization and on-chain circulation. We connect traditional institutions with the Web3 ecosystem, enrich the types of on-chain assets, expand revenue sources, and meet the allocation needs of a broader range of investors. Meanwhile, we help traditional enterprises unlock sustainable value on-chain through customized solutions. Boasting profound professional expertise and top-tier technical capabilities, our team builds a secure, efficient, and scalable infrastructure, providing institutions with a comprehensive decentralized ecosystem for onboarding assets onto the blockchain. We welcome strategic partners with a long-term perspective to co-build an open, compliant, and sustainable RWA ecosystem. For industry exchanges with us, please contact: chris@pharoslabs.xyz
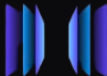
Pharos' Official Website: https://www.pharosnetwork.xyz/

WeChat Official Account: Pharos Research

From RWA to On-Chain Finance.
Mapping Real-World Value.