欧科云链控股有限公司
OKG Technology Holdings Limited

31 March 2023
By Email

Securities and Futures Commission (**"SFC"**)
54/F, One Island East,
18 Westlands Road, Quarry Bay
Hong Kong
Consultations | Securities & Futures Commission of Hong Kong

To Whom It May Concern,

Re: Consultation on the Proposed Requirements for Operators of Virtual Asset Trading Platforms

As the virtual asset (VA) market evolves, regulatory and compliance challenges are increasing. In order to effectively regulate the VA market, Hong Kong needs to adopt Regulatory Technology (RegTech) and Supervisory Technology(SupTech) to create a supportive business environment for the VA market. RegTech can improve regulatory efficiency by analysing on-chain and off-chain data of virtual asset service providers (VASPs) and using AI and other technologies to identify potential risks in VA transactions quickly. SupTech, on the other hand, can enhance the transparency and credibility of regulation and compliance, improve compliance efficiency, and reduce risks through blockchain and other technical means.

As the first blockchain data company listed on the Hong Kong Stock Exchange, OKG Technology Holdings Ltd.(01499.HK) has accumulated years of experience in on-chain data analysis and cooperation with law enforcement agencies of China Mainland through technology solutions. By identifying, evaluating, and tracking potential risks of VA in transactions, we help institutions and investors ensure the legality, compliance, and security of their transactions and use of VAs. We hope to use the years of practical experience in investigating VA-related financial crimes in the industry to become Hong Kong's on-chain "Independent Commission Against

Corruption". Now I am responding on behalf of OKG Technology Holdings Ltd. (OKG Technology) to the second, third, sixth, and ninth questions in the Consultation on the Proposed Requirements for Operators of Virtual Asset Trading Platforms (VATPs) issued by the Securities and Futures Commission. Please find below the written submissions for your consideration.

Question 2: Do you have any comments on the proposals regarding the general token admission criteria and specific token admission criteria?

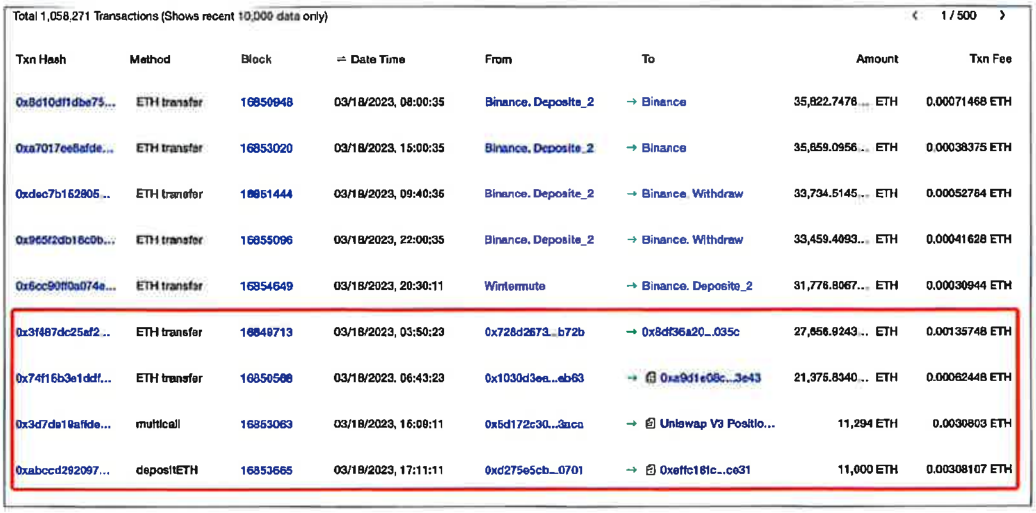
While the consultation paper already contains very detailed criteria, we would suggest SFC supplement some real-time on-chain data metrics such as real-time monitoring of wallets of founders/key stakeholders, introducing real-time monitoring of VAs and alerts for large transfers, alerting the security attacks on the VA ecosystem, etc. These on-chain data metrics can be incorporated into monitoring to beware of market risks, thus enhancing transparency and accountability for token issuers and trading platforms and better-protecting investors.

There are three reasons:

1. When trading stocks, all funds flow through bank custody accounts, but in contrast, VA transactions can happen on some blockchains and centralised trading platforms. Transactions on blockchain often have anonymity and anti-censorship features.

2. Large transactions tend to be executed via on-chain wallets rather than centralised exchanges. For instance, in our Ethereum Explorer data (*https://www.OKLink.com/eth/tx-list?type=large*), the ranking page for large transactions shows nine large transactions. Except for the flow of funds between exchange accounts and Market Maker Service accounts, all large transactions by personal accounts were made on-chain rather than on some centralised exchanges. The clients behind these on-chain addresses can not be identified unless regulators use an address labelling system accumulated through technology and industry experience.

Figure 1 OKLink ETH Explorer Large Transactions Ranking on March 18, 2023



Total 1,058,271 Transactions (Shows recent 10,000 data only)

‹ 1 / 500 ›

Txn Hash	Method	Block	⇌ Date Time	From	To	Amount	Txn Fee
0x8d10df1dbe75...	ETH transfer	16850948	03/18/2023, 08:00:35	Binance. Deposite_2	→ Binance	35,822.7476... ETH	0.00071468 ETH
0xa7017ee8afde...	ETH transfer	16853020	03/18/2023, 15:00:35	Binance. Deposite_2	→ Binance	35,659.0956... ETH	0.00038375 ETH
0xdec7b152805...	ETH transfer	16851444	03/18/2023, 09:40:35	Binance. Deposite_2	→ Binance. Withdraw	33,734.5145... ETH	0.00052764 ETH
0x965f2db18c0b...	ETH transfer	16855096	03/18/2023, 22:00:35	Binance. Deposite_2	→ Binance. Withdraw	33,459.4093... ETH	0.00041628 ETH
0x6cc90f0a074e...	ETH transfer	16854649	03/18/2023, 20:30:11	Wintermute	→ Binance. Deposite_2	31,776.8067... ETH	0.00030944 ETH
0x3f487dc25af2...	ETH transfer	16849713	03/18/2023, 03:50:23	0x728d2673...b72b	→ 0x8df36a20...035c	27,856.9243... ETH	0.00135748 ETH
0x74f16b3e1ddf...	ETH transfer	16850568	03/18/2023, 06:43:23	0x1030d3ea...eb63	→ 0xa9d1e08c...3e43	21,375.8340... ETH	0.00062448 ETH
0x3d7da19afide...	multicall	16853063	03/18/2023, 16:09:11	0x5d172c30...3aca	→ Uniswap V3 Positio...	11,294 ETH	0.0030803 ETH
0xabccd292097...	depositETH	16853665	03/18/2023, 17:11:11	0xd275e5cb...0701	→ 0xeffc181c...ce31	11,000 ETH	0.00308107 ETH

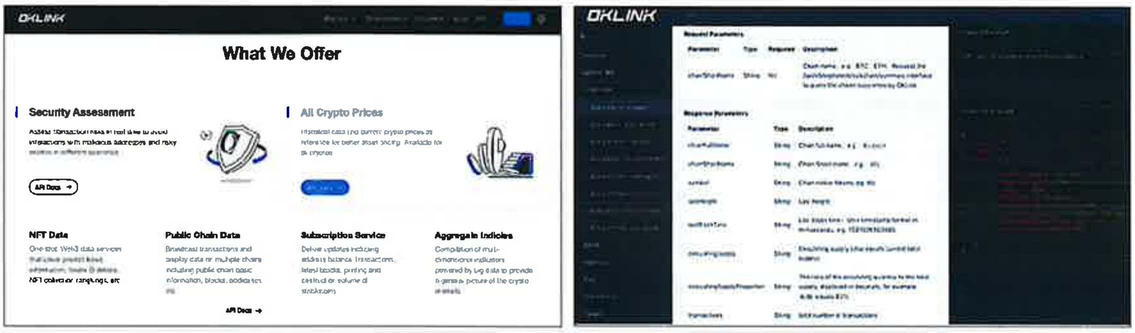
3. Securities are issued based on companies, while VA is community- or ecosystem-based. Therefore, the company information required for securities issuance may not apply to the examination of VAs. To truly evaluate the development level of a public chain and its ecosystem, deep analysis and sorting of its blockchain data are required to measure its development status in various dimensions and indicators comprehensively.

Suggested Solutions from OKG Technology:

1. Unlike native blockchain explorers, our product OKLink's multi-chain explorer has the database to clean and analyze on-chain data. We have developed various data tools and technology solutions for VA-related issues.

   - In accordance with specific regulatory requirements, our product OKLink can provide professional API functions for licensed VATPs and for the SFC to monitor on-chain anomalies of VAs and analyse on-chain address behaviour. Based on OKLink's accumulated data from more than 20 mainstream public chains on the market and over 2.7 billion address-label data, we provide KYT (Know Your Transaction), KYA (Know Your Address), and other API services for third-party real-time risk detection. API details can be found at: *https://www.OKLink.com/OKLink-api*

Figure 1 OKLink ETH Explorer Large Transactions Ranking on March 18, 2023



OKLINK

What We Offer

Security Assessment

Assess transaction risks in real time to avoid interactions with malicious addresses and risky assets in different scenarios

API Docs →

All Crypto Prices

Historical data and current crypto prices as reference for better asset pricing. Available for [illegible] cryptos

NFT Data

One-stop Web3 data services that [illegible] NFT collection rankings, etc

Public Chain Data

Broadcast transactions and display data on multiple chains including public chain basic information, blocks, addresses, etc

Subscription Service

Deliver updates including address balance, transactions, latest blocks, pricing and contract or volume of stablecoins

Aggregate Indicies

Compilation of multi-dimensional indicators powered by big data to provide a general picture of the crypto markets

API Docs →

OKLINK

Request Parameters

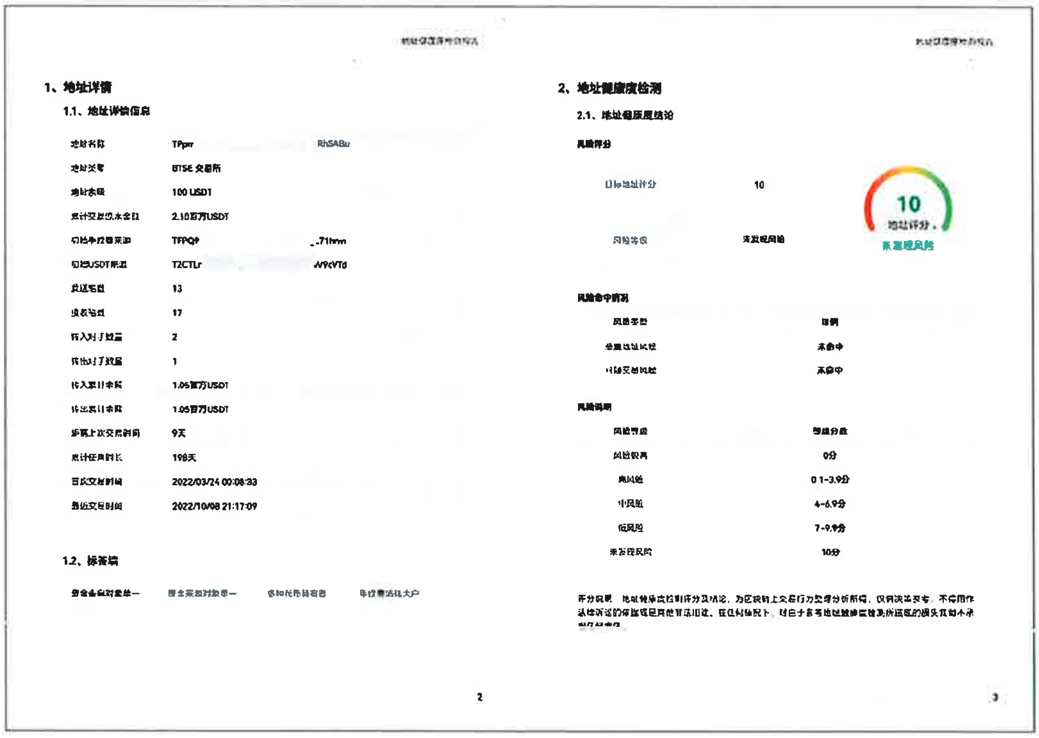
Parameter	Type	Required	Description
chainShortName	String	Yes	Chain name, e.g. BTC, ETH

Response Parameters

Parameter	Type	Description
chainFullName	String	Chain full name, e.g. Bitcoin
chainShortName	String	Chain short name, e.g. BTC
symbol	String	[illegible]
lastHeight	String	Last height
lastBlockTime	String	[illegible]
circulatingSupply	String	[illegible]
circulatingSupplyProportion	String	[illegible]
transactions	String	Total number of transactions

- Our on-chain address labelling system (with approximately 700 million entity label addresses) can identify specific target-related addresses, and deeply and accurately monitor the wallet address anomalies of major stakeholders in VAs. We provide 24/7 real-time monitoring of designated addresses, allowing users to set alert parameters flexibly. OKLink can also generate reports on relevant addresses for regulatory authorities on a regular basis.

Figure 3 OKG Technology Product - Address Risk Screening Report by OKLink



地址健康度检测报告

1、地址详情

1.1、地址详情信息

地址名称	TPpr	RhSABu
地址关联	BTSE 交易所	
地址余额	100 USDT	
累计交易总流水金额	2.10百万USDT	
初始手续费来源	TFPQP	_71hnn
初始USDT来源	T2CTLr	W9cVTd
发送笔数	13	
接收笔数	17	
转入对手数量	2	
转出对手数量	1	
转入累计金额	1.05百万USDT	
转出累计金额	1.05百万USDT	
距离上次交易时间	9天	
累计活跃时长	198天	
首次交易时间	2022/03/24 00:08:33	
最近交易时间	2022/10/08 21:17:09	

1.2、标签墙

资金来源对象单一　资金去向对象单一　参与代币持有者　[illegible]大户

2

地址健康度检测报告

2、地址健康度检测

2.1、地址健康度结论

风险评分

目标地址评分	10
风险等级	未发现风险

10 地址评分，未发现风险

风险命中情况

风险类型	结果
恶意地址风险	未命中
可疑交易风险	未命中

风险说明

风险等级	评级分数
风险极高	0分
高风险	0.1-3.9分
中风险	4-6.9分
低风险	7-9.9分
未发现风险	10分

评分说明：地址健康度检测评分及结论，为区块链上交易行为数据分析所得，仅供决策参考，不得用作法律诉讼的依据或其他非法用途。在任何情况下，对由于参考地址健康度检测所造成的损失我司不承担任何责任。

3

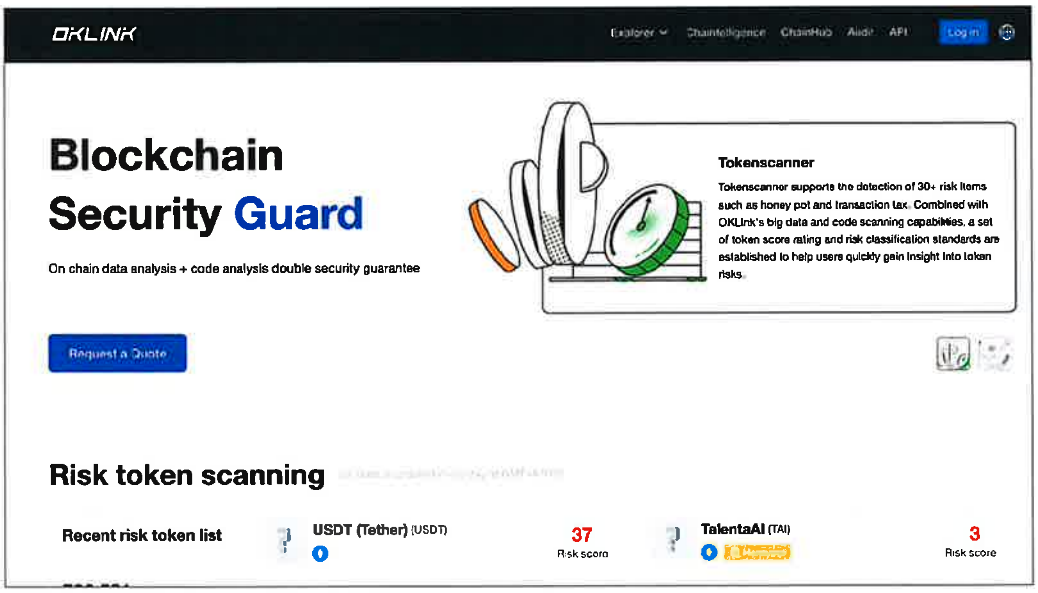
2. In addition, OKG Technology also suggests SFC consider the following two points related to token admission criteria :

   - Increase the on-chain activity assessment of the VA ecosystem, such as the number of active addresses on the chain, on-chain interactions, and social media updates of the project, to ensure that there are trading scenarios for tokens after they are listed. When investors choose VAs for trading, they will pay more attention to VA's ecosystem/community to evaluate the development status of a project.

   - As proposed by the SFC in 48. b) "The licensed platform operator is expected to conduct a smart contract audit for virtual assets based on blockchains with a smart contract layer unless the platform operator demonstrates that it would be reasonable to rely on a smart contract audit conducted by an independent auditor".

     We suggest that SFC should pay attention to the fact that even if the code of VAs has been audited by different independent institutions, it can not guarantee that the code is 100% free of risks. Other security technical solutions should also be used, such as risk alerts and risk token scanning, to improve security protection.

Figure 4 OKG Technology Product OKLink's Risk Token Scanning



Blockchain Security Guard

On chain data analysis + code analysis double security guarantee

Tokenscanner

Tokenscanner supports the detection of 30+ risk items such as honey pot and transaction tax. Combined with OKLink's big data and code scanning capabilities, a set of token score rating and risk classification standards are established to help users quickly gain insight into token risks.

Risk token scanning

Recent risk token list

USDT (Tether) (USDT) 37 Risk score

TalentaAI (TAI) 3 Risk score

Question 3: What other requirements do you think should be implemented from an investor protection perspective if the SFC is minded to allow retail access to licensed VA trading platforms?

In addition to the recommended regulations on insurance/compensation arrangements disclosed in the paper, we suggest that SFC can guide licensed institutions to strengthen risk management technology solutions for VATPs. This can be done by building their on-chain firewall that operates in parallel with passive and active safety solutions to prevent investor losses caused by hacker attacks.

1. We propose the following three solutions for VATPs:

   - Use the situational awareness system: make risk alerts to achieve around-the-clock, all-around cyber security monitoring. In particular, the situational awareness system analyses historical risk events such as lightning loan attacks, NFT phishing, and ad token airdrops, determines risk patterns, and establishes corresponding detection models. The system can achieve real-time discovery, tracking, analysis, and response to suspicious addresses and risky transactions across multiple chains and scenarios.

     As of the end of last year, OKG Technology's product - OKLink's on-chain situational awareness system had identified 243 risk events. Regarding mixers in money laundering, it identified 1.9374 million risky transactions, and in cross-chain bridges, it identified 20,400 risky transactions. With timely warning and OKLink's on-chain tracking capabilities after identifying risk events, risks can be effectively managed.

   - In terms of compliance with VASPs, with the situational awareness system, when it warns of the flow of risky funds, centralised VATPs can refuse these funds to ensure compliance with AML/CFT standards.

   - VATPs should also set up an investor protection fund to compensate investors for losses due to platform failures, security attacks, etc. They can also improve their complaint handling and dispute settlement procedure to address investor complaints and disputes arising from technical failures promptly.

2. The SFC should join the force with leading industry enterprises to conduct more market-oriented cyber security training on a regular basis to deal with the losses caused by VA crimes.

   According to the "Global Virtual Currency Crime Situation and Security Governance White Paper (2022-2023)", jointly released by OKG Research and the Key Laboratory of the Third Research Institute of Information cyber security of the Ministry of Public Security, private key leaks and losses were the primary causes of security attacks in the ecosystem in 2022, resulting in losses of up to $930 million, accounting for about 40% of the total losses. Phishing attacks (27%) were the most common attack method in the blockchain ecosystem in 2022.

   Raising investors' cyber security awareness is the key to addressing private key leaks and phishing attacks on non-custodial wallets and VA exchanges. OKG Technology has conducted over 20 training sessions on cracking VA cases and VA crime technology for law enforcement and the public in Greater China. OKG Technology is willing to work with the SFC to provide investors with cyber security and related knowledge training.

Question 6: Do you have any suggestions for technical solutions that could help reduce the risks associated with the custody of client virtual assets, particularly in hot storage?

Although the importance of cold wallets has been emphasised in the paper, based on experience in tracking and analysing security incidents, we provide recommendations for the SFC from three aspects: cold wallet solutions, hot wallet solutions, and cloud service security.

1. Cold wallet management: In the paper "10.6 (c) The Platform Operator and its Associated Entity should store 98% of client virtual assets in cold storage except under limited circumstances permitted by the SFC on a case-by-case basis to minimise exposure to losses arising from a compromise or hacking of the platform; " and other details about VA storage, we also suggest that VAs can be stored in different cold wallets which are located in different areas of Hong Kong. Managing private key encryption documents and AES passwords should be handled by different personnel, with one private key being authorised for storage in a bank safe. Once a private key is used for an online transaction, it should be invalidated and never used again.

2. Hot wallet management: Private keys for hot wallets can be stored and backed up using a multi-point decentralised approach, with a technical solution that utilises semi-offline signature services to store the private key in memory without accessing the internet. This approach isolates online hacker attacks from physical attacks offline. In addition to using multi-signature technology, Multi-Party Computation (MPC) is one of the latest techniques for securing private keys. Backup plans for private key activation should be established for multiple scenarios. Multiple risk control detection solutions should be implemented in the risk management process to prevent suspicious token inflows or outflows.

3. Cloud security management: A high-performance distributed intelligent computing network architecture (HPCS) and BTOK bi-directional authentication technology should be adopted to protect VA data from internal and external access. Existing HSM solutions may violate the zero-trust principle.

Question 9: Do you have any comments on the requirements for virtual asset transfers or any other conditions in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs? Please explain your views.

Regarding the "Blockchain analytic tools" mentioned in Chapter 12 of the paper, the SFC has provided detailed regulations on using technology solutions for compliance. We strongly support the use of Blockchain analytic tools to help VASPs identify suspicious activities, understand the risk profile of their clients, and provide support for AML/CFT.

Here, we propose more detailed suggestions:

1. Blockchain analytic tools must be able to analyse on-chain addresses, monitor on-chain risks, and track on-chain cases. Only by achieving the three-in-one closed-loop risk control can we better grasp the characteristics of address and transaction behaviour and vividly depict the user profile of the ultimate controller behind the address.

    - To achieve the capability of analysing on-chain data, it is necessary to present the full lifecycle behaviour and characteristics of a specific on-chain address from multiple dimensions and perspectives, enabling users to grasp the address and transaction behaviour characteristics quickly, present conclusive analysis results, and depict the user profile of the actual controller behind the address. By deeply analysing data, combined with the overall VA flow of the platform, second matching can be performed on non-labelled addresses with high secrecy, identifying potential specific associated addresses on the suspected person's platform and opening up analysis ideas.

- To achieve the capability of on-chain risk monitoring, based on the accumulated historical security events, analysing data and classifying them from related dimensions such as projects, transactions, and addresses, to extract and decompose the indicators that can be developed and establish a model for risk monitoring.

- To achieve the capability of on-chain risk monitoring, combined with the analysis and judgment experience accumulated from hundreds of cases such as gambling platforms, fake exchanges, and phishing websites, professional modelling of technical methods was carried out, achieving automated analysis of the VA flow and platform addresses. This helps to quickly identify the flow of platform VAs and the location of hidden funds. Based on the deposit and withdrawal addresses after data mining and the platform's wallet addresses with large amounts of VA, we can quickly understand the number of people involved and the scale of the case's funds involved in the corresponding platform.

2. Blockchain analytic tools must undergo time verification and have practical experience before the SFC can recommend them to licensed VATPs. Otherwise, the lack of analytical capabilities will affect AML/CFT compliance support.

3. Blockchain analytic tools can also exist with direct API to the SFC, making automatic reports that include major attack alerts and on the compliance status of licensed VATPs for regulatory authorities to review on a regular basis.

OKG Technology can provide technological solutions regarding blockchain analytic tools:

1. Address labelling technological solution:

   By adopting AML standards for identification rules and models, we conduct a comprehensive "physical examination" of addresses and have established the address labelling system. Currently, OKG has labelled nearly 2.7 billion addresses, of which over 4 million are malicious addresses, and the accuracy rate of the system is as high as 99.7%.

Figure 5 OKG Technology Address Labelling System

2. Situational awareness system technological solution:

   Identify different types of security events and provide timely risk alerts. Based on risk event scenarios such as flash loan attacks, NFT phishing, and advertising token airdrops, OKLink establishes detection models, and combines with OKLink's on-chain real-time data analysis capabilities to achieve real-time discovery, tracking analysis, and response handling of suspicious addresses and risk transactions in multiple chains and scenarios.

Figure 6 OKG Technology Situational Awareness System

OKG Technology has cooperated with many institutions in mainland China, including:

1. Cooperated with Nanjing Institute of Public Security Technology to establish OKG Chaintelligence Nanjing Laboratory.

2. Established the "Criminal Intelligence Blockchain Technology Analysis Center" with Nanjing Forest Police College.

3. In cooperation with the Beijing Computer Federation, the first "National Blockchain Police Training" was held in Jinan, Shandong Province.

4. Organised over 20 online and offline VA crime-related training programs for public security bureaus nationwide and jointly signed contracts with multiple cyber security cooperation agencies to combat cyber security crimes.

In addition to providing advice on Blockchain analytic tools and training programs, we also suggest that the SFC:

1. Increase domain name detection, contract authorisation detection, and similar address phishing detection for "unhosted wallets" mentioned in the paper to protect the interests of investors. OKG Technology intercepts and reminds users in a timely manner by identifying suspicious phishing domain names, malicious addresses, malicious authorisation methods, and disguised commonly used transaction addresses to protect user assets and avoid VA losses.

2. With regard to the "Travel Rule" regulations, we recommend that the SFC must record and report key information involving the identities of both parties, including the names, addresses, account numbers, and identity proofs of the sender and recipient.

Figure 7 OKG Technology Product - Transaction monitoring screens out transactions that meet the required Travel Rule

3. VASPs have an obligation to provide relevant data to form a regulatory data dashboard, which can provide real-time, accurate, and comprehensive data on the VA market to regulators. OKG Technology is willing to customise a data dashboard for SFC to improve regulatory efficiency, reduce costs, and optimise regulatory decisions.

We suggest data elements in the data dashboard as follows:

VASP Basic Info	VASP name, registered address, registration number, contact person, contact information, etc.
User Data	VASP's user amount, user distribution, and user risk level distribution of VASPs, etc.
Transaction Data	VASP's transactions, transaction amount, transaction frequency, service fee source, risk level, transaction time, etc.
Malicious Address	Malicious addresses or associated addresses found by VASPs such as fraud, online gambling, and phishing.

4. To promote the development of VA-related businesses in Hong Kong by providing specific training and certification programs to prospective VATPs.

From the industrial era to the digital era, the value of VAs such as data and information has become increasingly prominent, and VAs are gradually being recognised globally. Due to its decentralisation, anonymity and borderless nature, the regulation has also become a new challenge. VAs require technology solutions to provide answers to regulatory challenges and risk management. Currently, the main paths for technological solutions are comprehensive regulation and cooperation between the two sides - regulatory and compliance sides. Data collection and data analysis to form risk identification, risk warning and then risk tracking is the optimal path and solution for RegTech of VAs and reducing the risk of VAs. An independent third-party technology solution is more conducive to developing cooperation between the regulatory and compliance sides, reducing compliance costs and optimising regulatory efficiency.

With its many years of experience as a case study, OKG Technology is willing to be the first model for the Hong Kong Securities and Futures Commission, acting as a bridge between VASPs, regulators and law enforcement agencies, using the accumulation and in-depth analysis of on-chain data to help law enforcement agencies investigate illegal transactions and combat financial crimes, and using RegTech to help VASPs comply. In addition, we are working with traditional Fiat AML institutions and cyber security companies to build a RegTech ecosystem through action and practice, thus promoting the healthy development of the industry.

Thank you for taking the time to look at our comments. Please get in touch with me at if you would like to discuss any of the suggestions or comments above.

Yours sincerely,

OKG Technology Holdings Ltd. (01499.HK)

About OK Group

As the parent company of OKG Technology Holdings Ltd. (01499.HK), OK Group (www.okg.com) is the world's leading blockchain group and one of the earliest blockchain enterprises in China. Since its establishment in 2013, OK Group is always dedicated to blockchain technology development and business application. Currently, OK Group has developed into a global large-scale blockchain technology service provider. Based in Beijing, China, it has branches or offices in first-tier cities such as Hong Kong, Shanghai, Shenzhen, Nanjing, and Jinan.

In recent years, with the development of the company's globalization strategy, OK Group now has branches or offices in multiple countries and regions, such as Singapore, Japan, Dubai, the United States, and Malta, covering over 180 countries and regions worldwide and serving over 50 million users all over the world.