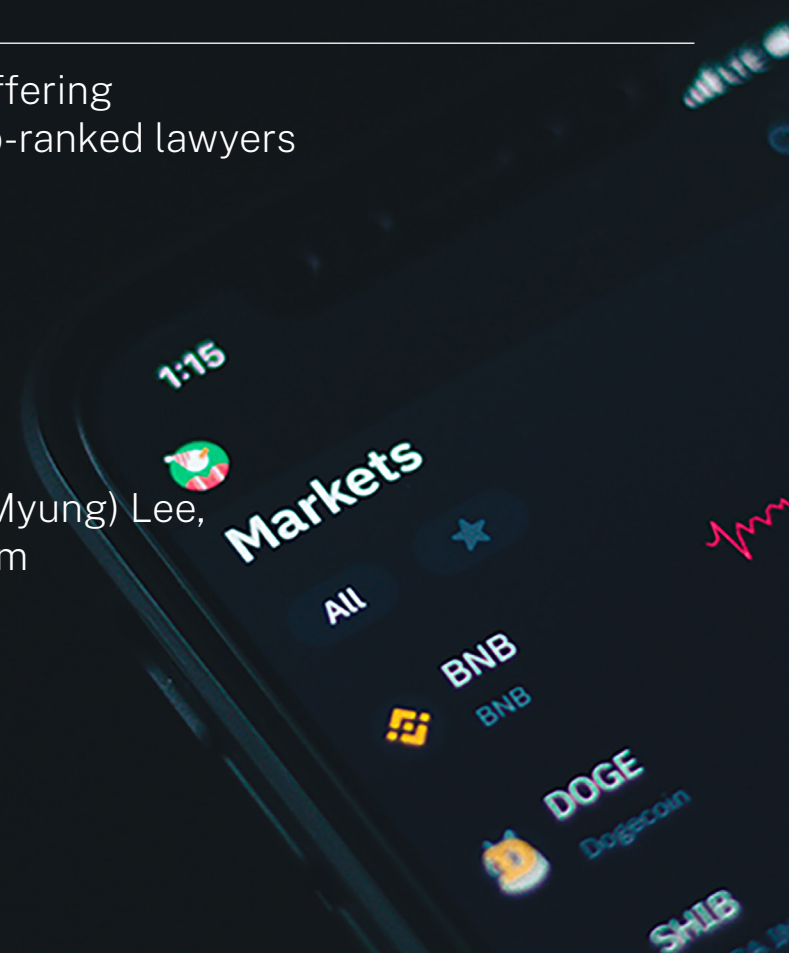
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Blockchain 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers



South Korea: Trends and Developments

Wooyoung Choi, Chloe (Jung Myung) Lee, Kun Hoon Lee and Yu Deok Kim
Lee & Ko

Trends and Developments

Contributed by:
Wooyoung Choi, Chloe (Jung Myung) Lee, Kun Hoon Lee and Yu Deok Kim
Lee & Ko

Lee & Ko has more than 50 experienced attorneys and industry specialists who have accumulated leading know-how and expertise on the full range of regulatory issues arising in the fintech space. Lee & Ko's digital finance team provides well-balanced, insightful and useful guidance to clients across all legal, policy-making and business aspects of the fintech industry. Such expertise and know-how are supplemented by the team's advanced understanding of the various technologies that underpin this sector, which enables the firm to focus on the issues that matter most to our clients. Lee & Ko's ability to provide one-stop legal services spanning the full spectrum of legal issues affecting the fintech sector stands out as the firm's greatest strength.

Authors

Wooyoung Choi is a partner at Lee & Ko, with expertise in virtual assets and IP. His practice primarily focuses on virtual asset service provider (VASP) regulatory issues, disputes, and IP disputes. In particular, Wooyoung is renowned for his excellence in matters related to crypto market entry in crypto-friendly jurisdictions, as well as cross-border IP disputes. Since 2017, he has continuously worked on virtual assets matters and is considered one of the first generation of digital assets lawyers, with a market-leading practice in relation to regulatory matters concerning virtual assets, VASPs, real-world assets and play-to-earn tokens.

Chloe (Jung Myung) Lee is a partner at Lee & Ko and the co-head of the firm's digital finance team. During the past 20 years, Chloe has been noted for her extensive experience and expertise in the areas of digital finance, fintech, blockchain, NFTs and financial regulatory and compliance. In these areas, she represents prominent onshore and offshore clients. She is a member of various academic law societies and associations, such as the Blockchain Law Society, the Capital Markets Law Society and the Korea Securities Law Association, and regularly gives presentations on legal issues and topics.

Contributed by: Wooyoung Choi, Chloe (Jung Myung) Lee, Kun Hoon Lee and Yu Deok Kim, **Lee & Ko**

Kun Hoon Lee is a partner at Lee & Ko, where he represents clients as a member of the firm's tax practice and corporate practice groups. Kun Hoon advises on a broad range of matters, including taxation on corporate restructuring, financial and other corporate transactions, as well as tax issues arising from fintech, blockchain and digital assets. Recently, Kun Hoon has devoted a significant portion of his practice to tax issues related to the issuance and offering of digital assets and non-fungible tokens, and he has counselled fintech companies and coin issuers in connection with their effort to establish foreign subsidiaries.

Yu Deok Kim is a criminal defence attorney at Lee & Ko. Based on his experiences from his prior position as a police investigator, Yu Deok provides practical and effective counsel to clients. He is also renowned for his excellent advisory track record across a broad spectrum of criminal cases, from specialised criminal cases involving financial markets and digital assets to general criminal cases at a corporate level.

Lee & Ko

Hanjin Building
63 Namdaemun-ro
Jung-gu
Seoul 04532
South Korea

Tel: +82 2 772 4000
Fax: +82 2 772 4001
Email: mail@leeko.com
Web: www.leeko.com

Overall Legislative and Regulatory Landscape for Blockchain in 2023

Previously, the only regulation applicable to digital assets in South Korea was the Act on Reporting and Using Specified Financial Transaction Information (the "AML Act"). The AML Act broadly defines virtual assets as "electronic certificates that have economic value and that can be traded or transferred electronically" and defines a Virtual Asset Service Provider (VASP) as an entity that engages in certain activities related to virtual assets, and VASPs are required to report to the financial authorities and comply with AML regulations. However, although it was commonly believed that digital assets would be subject to the same regulations as securities under the Financial Investment Services and Capital Markets Act (FISCMA) if such digital assets could be classified as securities, uncertainties persisted owing to the lack of clear guidance or interpretation by financial authorities on this issue.

Against such a backdrop, in February 2023, the financial authorities clarified that "security tokens" – ie, digital assets that can be classified as securities – are distinct from virtual assets under the AML Act and are subject to the same regulations as securities under the FISCMA, according to the "Measures to Overhaul Regulations to Permit Issuance and Circulation of Security Tokens" (the "ST Guidelines"). This ST Guidelines define "security tokens" as digitalised securities (referring to securities under the FISCMA) utilising distributed ledger technology and proposes the following:

- principles for determining whether digital assets can be classified as security tokens; and
- a plan to set up the regulatory framework for the issuance and distribution of security tokens.

Regarding virtual assets, which are digital assets that do not have the characteristics of securities, the Act on Protection of Virtual Asset Users (the "Virtual Asset User Protection Act") – designed to regulate the virtual asset industry – was enacted on 18 July 2023 and is scheduled to take effect on 19 July 2024.

As discussed earlier, 2023 can be considered as the year that established the regulatory framework for the regulation of digital assets by:

- dividing the blockchain-based digital assets into two broad categories (general virtual assets and security tokens); and
- clarifying that general virtual assets are subject to the AML Act and the Virtual Asset User Protection Act, whereas security tokens are subject to the FISCMA.

Enactment of the Virtual Asset User Protection Act

As previously mentioned, the Virtual Asset User Protection Act, which is the first South Korean regulation on virtual asset services designed for the protection of users in the virtual asset market and the regulation of unfair trade practices, was enacted on 18 July 2023 and is scheduled to take effect on 19 July 2024.

Matters concerning the protection of virtual asset users

According to the Virtual Asset User Protection Act, VASPs are required to deposit or entrust users' deposits with a financial institution (bank) separate from their own assets. Except in certain cases, these deposited or entrusted funds cannot be subject to set-off, seizure or provisional

seizure, nor can they be transferred, assigned or provided as security. In the event of bankruptcy of a VASP, these deposited funds must be prioritised to be paid to the user.

In addition, VASPs must segregate their own virtual assets from users' virtual assets and are obligated to ensure that they in effect hold the same types and quantities of virtual assets entrusted by users. Furthermore, at least 80% of the economic value (based on the average of the immediately preceding year) of the users' virtual assets must be stored in cold wallets. Moreover, VASPs are required either to subscribe to insurance policies or mutual aid programmes or to establish reserves in anticipation of incidents such as hacking and computer failures.

Regulation of unfair trade practices

Similar to the FISCMA, the Virtual Asset User Protection Act stipulates that unfair acts in the virtual asset market are prohibited. Specifically, it prohibits:

- the use of material non-public information;
- market manipulation through matched orders, wash trading, etc;
- trading virtual assets issued by the VASPs themselves or their related parties; and
- fraudulent trade practices such as:
  - (a) employing improper means, schemes or tricks;
  - (b) making false statements of material facts; and
  - (c) using false market prices.

It is important to note that severe criminal penalties and financial penalties may be imposed for engaging in unfair trade practices. Criminal penalties include imprisonment for a minimum of one year (up to ten years in cases of violation of restrictions on trading in self-issued virtual assets) and financial penalties equivalent to at least three times (but not more than five times) the profit gained or loss avoided through the violation. For financial penalties, the amount can be up to twice the profit gained or loss avoided through the violation.

Moreover, VASPs that establish and operate virtual asset markets must monitor abnormal transactions at all times, immediately notify the financial authorities when suspicious behaviour is detected, and immediately report to the investigative agency if the offence is sufficiently substantiated. In addition, VASPs are prohibited from blocking users' deposits and withdrawals of virtual assets without just cause.

ST Guidelines

On 6 February 2023, the Financial Services Commission (FSC) announced the "Measures to Overhaul Regulations to Permit Issuance and Circulation of Security Tokens" and the "Guideline on Security Tokens". The ST Guidelines outline the basic principles for determining whether a digital asset utilising distributed ledger technology qualifies as a security. They clarify that such "security tokens", which correspond to securities, are subject to securities regulations under the FISCMA. Additionally, they unveil plans to improve the relevant system to ensure that security tokens are issued and distributed in accordance with the FISCMA and the Act on Electronic Registration of Stocks and Bonds by amending those laws.

Under the FISCMA, various types of securities (eg, debt securities, equity securities, beneficiary certificates, derivatives-linked securities, and depositary receipts) are standardised, with established application cases. However, investment contract securities may be widely recognised and subject to interpretation due to their

broad definition and the negative regulatory system of the FISCMA. Consequently, they are applied complementally in cases where they do not fall under the other types of securities. Digital asset business operators must closely examine whether the digital assets they issue, distribute, and/or handle may fall under each category of securities under the FISCMA (in particular, investment contract securities) by meeting the following requirements:

- common enterprise;
- investment of money and others;
- mainly carried out by others;
- contractual rights in which gains and losses resulting from the common enterprise vest; and
- purpose of profit acquisition.

The FSC explicitly stated in the ST Guidelines its intention to test the distribution plan of investment contract securities and the issuance and distribution plan of beneficiary certificates as an innovative financial service (referred to as a "financial regulatory sandbox") under the Special Act on Support for Financial Innovation to the extent that innovation is recognised. In this regard, it may also be an option for a business operator to consider applying for designation as an innovative financial service in accordance with the ST Guidelines.

Strengthened Regulation of Deposits and Management of Virtual Assets Due to the Haru Investment Case

Haru Investment advertised for guaranteed principal through risk-free management and highest returns in the industry for crypto deposits on its platform from 2020 to 2023, and abruptly suspended withdrawals in June 2023 after receiving approximately KRW1.4 trillion worth of cryptocurrencies. Around the same time, another virtual asset deposit service provider, Delio, also abruptly suspended withdrawals.

Haru Investment was incorporated in Singapore by a South Korean blockchain accelerator, but it was actually operated by Haru Investment Korea, a South Korean subsidiary of Haru Investment. However, Haru Investment Korea did not report itself as a VASP in accordance with the AML Act despite continuing to provide virtual asset management services in South Korea, owing to uncertainties concerning whether depositing and managing virtual assets fell within the activities that needed to be reported under the AML Act. Because Haru Investment Korea did not report itself as a VASP, it was not under the supervision of financial authorities and was essentially in the regulatory blind spot.

The Haru Investment case led to the need to strengthen the regulation of virtual asset deposit and management services and, subsequently, as shown in Potential Expansion of the Scope of VASPs, a number of interpretations by the FSC were published in order to expand the scope of VASPs from various perspectives.

In addition, the Virtual Asset User Protection Act does not provide for specific regulations on the deposit and management of virtual assets. However, it stipulates that VASPs are obligated to ensure that they in effect hold the same types and quantities of virtual assets entrusted by users, which made deposit and management services by VASPs impossible in fact.

Furthermore, the amended Act on the Regulation of Conducting Fundraising Business Without Permission – scheduled to take effect on 28 May 2024 – includes the act of raising funds using virtual assets within its scope of regulation. In other words, the previous Act on the

Regulation of Conducting Fundraising Business Without Permission prohibited the act of raising "funds" from unspecified individuals by guaranteeing principal without obtaining authorisation or permission in accordance with other acts and regulations, but the amended act explicitly stipulates that the scope of "funds" includes virtual assets. The primary reason behind such amendment was the lack of a legal basis to punish Anchor Protocol's promise to provide interest on deposits in the Terra-Luna case. In light of such background, it is likely that virtual asset deposit and management services that guarantee the return of the principal amount will also be prohibited under the aforementioned amended act.

Potential Expansion of the Scope of VASPs

Currently, the AML Act defines a VASP as an entity or person engaged in any of the following activities:

- selling or buying virtual assets;
- exchanging virtual assets for other virtual assets;
- transferring virtual assets, as prescribed by the Presidential Decree of the Act;
- safekeeping or managing virtual assets; and
- brokering, arranging, or acting as an agent for the sale and purchase of virtual assets or the exchange of virtual assets for other virtual assets.

Initially, the financial authorities interpreted the scope of VASPs subject to the requirement for reporting to the financial authorities to be limited to "major" VASPs (such as virtual asset exchanges, custodians, and wallet service providers). To date, these major VASPs appear to be the main targets of the financial authorities' watchful eyes.

However, in light of a number of interpretations in the second half of 2023, the authors' take is that the financial authorities are now leaning towards a broader definition of a VASP than before, and that reporting to the financial authorities is required if a business falls under the definition. By way of example, the financial authorities hinted that the development and supply of "software programs that automatically trade virtual assets according to algorithms" and the provision of services through applications by securities companies, which allows customers to connect to virtual asset exchanges to buy and sell virtual assets without separate customer verification, may be included in the act of brokering, arranging, or acting as an agent for the sale and purchase of virtual assets under the Specified Finance Act.

In addition, the financial authorities provided their official interpretation that – even if a company distributes virtual assets to an unspecified number of people for free (eg, via airdrop) – it may be difficult to consider treating such a distribution of virtual assets alone as running a business. However, they cautioned that each case may be individually reviewed on potential profit-seeking and repetition/continuation aspects of such behaviours to determine whether an entity falls under the scope of a VASP.

Nonetheless, for now, it is unlikely that the financial authorities will take active measures – such as notifying law enforcement agencies against unreported VASPs that are currently not under the scope of major VASPs – unless there is a large number of victims or it becomes a social issue. In the long term, it is possible that the financial authorities will refer to overseas regulations such as the Markets in Crypto Assets Regulation (MiCA) to set forth the types of business

activities of VASPs in a more specific manner in the form of legislation or guidelines.

In addition, as the financial authorities are expected to actively supervise the virtual asset market in 2024 under the Virtual Asset User Protection Act that will go into effect in the summer, it is possible that the financial authorities will clarify their stance or change their stance in step with the trends of the virtual asset market. It is thus necessary to monitor the regulatory and legislative trends of the financial authorities especially carefully with regard to the scope of VASPs.

Accounting and Disclosure Guidelines for Virtual Assets

The Guidelines for the Supervision of Accounting for Virtual Assets (the "Accounting Guidelines") include considerations for:

- accounting for token issuers;
- accounting for token holders;
- accounting for VASPs (exchanges); and
- fair value measurement for virtual assets.

The Accounting Guidelines can be summarised as follows.

First, the Accounting Guidelines clarify the revenue recognition criteria for the transfer of virtual assets after the virtual asset issuer has "fulfilled all of the performance obligations described in the White Paper". Virtual asset issuers are also required to clearly identify whether they have fulfilled their performance obligations at the time of token sale and, if they change their performance obligations after the sale without any significant reason (eg, a significant change in the White Paper), the related accounting treatment will be considered erroneous.

Second, the Accounting Guidelines clarify that reserved tokens that are kept internally by an issuer without transferring them to others after issuance (creation) cannot be recognised as assets. In addition, if the reserved tokens are transferred to a third party in the future, it may affect the value of the virtual assets already in circulation – hence the quantity of reserved tokens and future utilisation plans should be disclosed as annotations. The information that must be disclosed in the annotations includes:

- the size and obligations of issuing virtual assets, which are the main contents of the White Paper;
- the status of internal reserves and free distribution;
- the contents of the contract for entrusting virtual assets to customers; and
- the risk of custody.

Third, the Accounting Guidelines propose the principle for classifying virtual assets as inventory assets, intangible assets, or financial instruments depending on the purpose for which the virtual assets were acquired by an entity and whether the virtual assets are considered financial instruments. In other words, as the International Financial Reporting Standards (IFRS) Interpretations Committee (June 2019) had previously suggested only classifying virtual asset holders as intangible assets or inventory assets depending on whether they are intended for sale, there have been conflicting views on whether it is permissible to classify virtual assets as financial assets or liabilities if they are token securities under the FISCMA.

However, according to the Accounting Guidelines, if token securities meet the definition of financial instruments under the Financial Instruments Standard (K-IFRS No 1032), they can be

classified as financial assets or liabilities and the related standards can be applied. However, companies applying the general corporate accounting standards are required to designate an account category (eg, miscellaneous assets) that can represent the characteristics of virtual assets and present it in the financial statements.

Fourth, the Accounting Guidelines stipulate that VASPs (such as exchanges) should determine who has control over the tokens between customers and the service providers, in order to decide whether the VASPs recognise them as assets or liabilities. In other words, if the VASP is viewed to have control over the virtual assets entrusted to it by the customer, the VASP should recognise the virtual assets and the liabilities to the customer as assets and liabilities respectively and, if not, the VASP should disclose it in the annotations.

Fifth, the Accounting Guidelines provide specific conditions for the concepts of active market, fair value and the like in virtual asset transactions – with detailed examples – so that companies and auditors can refer to them when preparing financial statements and performing audits.

Finally, the Accounting Guidelines set forth that the main contents of the White Paper – such as the size of virtual asset issuance and performance obligations, the status of internal reserve and free distribution, the contents of the contract for entrusting virtual assets to customers, and custodial risks – should be disclosed in the annotations.

Hacking of Virtual Assets by Hacker Groups Such as Those From North Korea

Current situation regarding damages

Hacking cases by groups such as those from North Korea have been observed frequently in the virtual asset market. The pattern of hacking has evolved in parallel with enhanced security policies, as they used to focus on attacking exchanges in 2016 but now focus on attacking weaknesses in the decentralised finance (DeFi) transaction structure, and hackers are using any means possible to exploit all possible vulnerabilities, whether on-chain or off-chain.

The biggest problem with these attacks involving virtual assets is not only the scale of the damage, but also the fact that it is very difficult to track and arrest the hackers, which is why hackers continue to try to hack without much fear. For the victims of the cyber-attack, it is not easy to even analyse the intrusion path of the hacker group, so there are cases where the service provider itself goes bankrupt after civil and criminal lawsuits from cryptocurrency investors.

Ultimately, when it comes to the hacking of virtual assets by hacker groups such as those from North Korea, it would be ideal to recover the stolen crypto assets or cure the damage. However, in reality, this is not easy and thus it becomes necessary to determine the appropriate "response strategy, response direction, and response speed" by referring to the practice guidelines of the counter-hacking investigation by organisations such as the Korea Internet and Security Agency (KISA) and the police.

Limitations of KISA and police investigation

In the cyber-attack incidents by hacker groups such as those from North Korea, generally the police (the Cyber Terrorism Investigation Unit of the National Police Agency) and analysts from the KISA Infringement Response Centre work together to analyse the intrusion path. The police usually conduct the investigation to track down the suspect by securing the damaged system and logs, analysing the intrusion path, tracking

coins, and international co-operation. On the other hand, KISA tends to operate a little faster owing to the practice's nature, and produces the analysis report and makes conclusion earlier than the police.

Due to the increased number of hacking cases recently, it has become difficult for the police to focus on one case for detailed analysis. Thus, if KISA's analysis report is generated first, it may be shared with the police and – if necessary – the police will analyse the intrusion path in more depth via the search-and-seizure process. However, in the case of the police investigation, even if the analysis of the intrusion path is completed quickly, the investigation to trace the suspect (eg, an international co-operation investigation) takes a very long time compared with a general police investigation. Therefore, it may take a long time for the police to analyse the intrusion path and trace the suspect – usually several months but sometimes up to two to three years.

In addition, even when the suspect is identified, it can be very difficult to apprehend the suspect because most of the attacks are carried out in North Korea, China, Eastern Europe, Russia, and other countries with which Korea cannot easily co-operate in judicial matters. For this reason, the focus of KISA investigations and police investigations – unlike general criminal cases – is not to apprehend the suspect but to "analyse the intrusion path" and additionally to "identify security vulnerabilities and request improvements to the industry to prevent recurrence". Also, given that the investigation usually takes such a long time, it is extremely difficult for victims to recover damages through the analysis and investigation process.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com