

SFC's guidance for firms engaging in tokenised securities

Nov 2023

Introduction

On 2 November 2023, the Securities and Futures Commission ('SFC') released 2 circulars in relation to the tokenisation of securities and other investment products, namely (1) Circular on intermediaries engaging in tokenised securities-related activities ('1st Circular') and (2) Circular on tokenisation of SFC-authorized investment products ('2nd Circular' together with the 1st Circular, the 'Circulars').

These Circulars represent a bold move by the Hong Kong regulator to formally recognise tokenisation as a financial services tool, and importantly, to open up retail investor access to authorised tokenised securities and investment products in primary markets (subject to the authorisation¹ and prospectus² requirements). Previously the SFC's position was that all tokenised securities were 'complex products' that were only available to those meeting the definition of a 'professional investor' ('PI'). The SFC is now taking a more risk-based approach and placing more emphasis on the substance of the underlying assets that are being tokenised. For instance, the SFC has made clear that whether a tokenised security is a complex product or not is based on an assessment of the complexity of its underlying traditional security. Obviously, the tokenisation platform and mechanism need to be appropriate, but this change of approach means that some tokenised securities will be available to both PIs and retail clients.

In this news flash, we have summarised the 1st Circular, outlining our views on some of the SFC's expectations for Intermediaries engaging in tokenised securities-related activities and areas where external assistance could be helpful as appropriate.

Circular on intermediaries engaging in tokenised securities-related activities

The SFC has set out its expectations around entities licensed with the SFC/registered with the Hong Kong Monetary Authority ('Intermediaries') that are looking to get involved with tokenised securities.

Tokenised securities vs digital securities

At the outset, the SFC clarified that 'tokenised securities' are a sub-set of a broader category of 'digital securities'. 'Tokenised securities' are traditional financial instruments (such as bonds and funds) that are essentially 'wrapped' by a digital representation recorded onto a programmable platform and using distributed ledger technology ('DLT') (e.g. a blockchain) in their security lifecycle ('tokenised securities'), whereas 'digital securities' may encompass a wider range of instruments that may be structured in different forms. To explain the difference, the SFC referred to examples of digital securities which are not tokenised securities – fractionalised digital interests in underlying real-world assets (such as artwork or land that are also caught by the definition of a 'collective investment scheme'³), or a tokenised profit-sharing arrangement, both of which would fall under the definition of 'securities'⁴.

¹ See Part IV of the Securities and Futures Ordinance (Cap. 571) ('SFO').

² See Companies (Winding up and Miscellaneous Provisions) Ordinance (Cap. 32).

³ See Schedule 1 of the SFO.

⁴ See Schedule 1 of the SFO.

News Flash

Interestingly, the SFC also mentioned that digital securities may exist exclusively on a blockchain with no links to extrinsic rights or underlying assets – which does not seem to fit well with the definition of ‘securities’ under the SFO and the SFC’s own previous [circular](#). This distinction also appears arbitrary in that instead of directly tokenising artwork or real estate (which are considered digital securities), creating a fund structure to invest into and hold those assets and then tokenising the fund units would now render those tokenised securities – which have implications in terms of their treatment as ‘complex products’ under the SFO.

SFC’s expectation for Intermediaries engaging in tokenised securities-related activities

Area	SFC’s key expectations	PwC’s view
Additional risks to consider	The overarching principle of the SFC’s regulatory approach is ‘same business, same risks, same rules’. In addition to complying with existing legal and regulatory requirements applicable to traditional securities, Intermediaries should manage the new risks, which are not typically associated with traditional securities, especially ownership risks and technology risks in activities involving tokenisation.	The SFC clarified that Intermediaries are expected to manage risks on behalf of their clients. ‘Same business, same risks, same rules’ means that the SFC will treat tokenised assets in the same way as if the Intermediary were dealing in the underlying asset itself as well as being comfortable that additional risks that apply to tokenised assets are being appropriately managed by the token issuer. ⁵
Risk assessment and due diligence (‘DD’)	Intermediaries should act with due skill, care and diligence, and perform DD on the tokenised securities based on all the available information to identify the key features and risks of the tokenised Securities, including Intermediaries’ existing obligation to conduct DD on the product itself and also on the technology aspects.	Token issuer DD is a key focus area for the SFC and Intermediaries should be assured that they are dealing with robust counterparties. Although token DD can fit within existing processes, Intermediaries will require the necessary manpower and expertise to undertake such tasks.
Issuance of tokenised securities - Responsibility over 3rd-party vendors	Where Intermediaries issue or are substantially involved in the issuance of the tokenised securities which they intend to deal in or advise on, they remain responsible for the overall operation of the tokenisation arrangement notwithstanding any outsourcing to 3rd-party vendors/service providers.	Intermediaries involved in issuance need to take full responsibility over the overall operations of the tokenised securities, and such responsibility cannot be outsourced to a 3 rd party even if it is engaged to perform a particular service. This requires Intermediaries to understand the risks associated with the tasks outsourced and develop controls and governance over the oversight of the arrangement.
Appendix - Part A - Factors for intermediaries to consider in assessing risks related to technical and other aspects	In assessing the risks related to the technical and other aspects of tokenised securities, an Intermediary should take into account the list of non-exhaustive factors set out in Part A of the Appendix to the 1st Circular: <ul style="list-style-type: none"> (a) the experience and track record of the 3rd-party vendor(s)/service provider(s) used in the tokenisation arrangement of the tokenised securities; (b) the technical aspects of the tokenised securities, <ul style="list-style-type: none"> (i) smart contract deployed (if any) <p>For example, an Intermediary should consider whether appropriate technology audits have been conducted in respect of the technical aspects of the tokenised securities. In particular, if a smart contract is deployed in the tokenised securities’ operation, the Intermediary may need to ensure a smart contract audit has been conducted on the smart contract.⁶ The</p> 	As there is a myriad of risks associated with tokenising securities and the list provided by the SFC is non-exhaustive, Intermediaries should make a detailed risk assessment on each type of tokenisation to ensure that all relevant risks are understood and that appropriate controls and governance are in place to mitigate those risks to avoid operational incidents, etc. <p><u>Experience and track record</u></p> <p>Intermediaries should conduct DD and put in place appropriate controls and governance before engaging 3rd-party vendors/service providers as the digital assets industry is relatively immature and they have not had a significant amount of time to build up experience and track record.</p> <p><u>Smart contracts</u></p> <p>Not all audits are created equal and the framework for conducting audits is often not fit-for-purpose to identify any vulnerabilities and flaws. Where smart contracts are deployed, this is best approached in a</p>

⁵ See appendix A to the 1st Circular.

⁶ If the Intermediary relies on a smart contract audit conducted by a 3rd party, it should be able to demonstrate that it is reasonable to rely on such smart contract audit.

	<p>smart contract audit should focus on reviewing whether the smart contract is not subject to any contract vulnerabilities or security flaws with a high level of confidence;</p> <ul style="list-style-type: none"> (ii) robustness of the DLT network⁷; (iii) inter-operability issues between DLT networks and the back-end systems of the product issuer and other parties throughout the security lifecycle;⁸ and (iv) robust and properly maintained policies and procedures, systems and controls underpinning the operation of the tokenised securities to manage.⁹ <p>Note: For example, adequate administrative controls in the form of transfer restrictions, mint-and-burn mechanism, transaction reversals or redemption.</p>	<p>staged manner, factoring in additional risk associated when making product decisions.</p> <p><u>Robustness of DLT networks</u></p> <p>Understanding the vulnerability and security infrastructure are important steps in determining the right DLT to use, prior to determining the most appropriate one for the tokenisation project based on the speed, size, scaling solutions and interoperability that the DLT may offer.</p> <p><u>Interoperability</u></p> <p>The interoperability considerations from a vulnerability and security lifecycle perspective are also key in mitigating risks associated with their use. As an example, some of the biggest hacks seen across the digital asset world have been as a result of weaknesses in 'bridges' which were implemented to allow for interoperability between different systems. When setting up the DLT, the objectives across the full end-to-end lifecycle of the product must be considered.</p> <p><u>Policies, procedures, systems and controls ('PPSC')</u></p> <p>The PPSC all depend on the risks associated with the tokenised securities. Understanding the underlying risks is therefore vital to the design of appropriate controls. Taking into consideration the operational set-up, product, size and scale of the company, it is clear that Intermediaries should conduct a risk assessment that is broader and more holistic than the highlighted risks in the Circulars to determine PPSC that are fit-for-purpose.</p>
<p>Disclosure requirements</p>	<p>Intermediaries should:</p> <ul style="list-style-type: none"> (a) make adequate disclosure of and communicate relevant material information specific to tokenised securities in a clear and easily comprehensible manner; and (b) provide clients with material information on the tokenisation arrangement. 	<p>Transparency and adequate disclosure to highlight the risks is key. Ensuring that this can be done in a clear and easily comprehensible manner given the complexity and technical nature of the subject matter will be key to ensuring it achieves its purpose.</p>

⁷ For example, the security infrastructure of its blockchain protocol, the size of the blockchain and network, and especially how resistant it is to common attacks, including a 51% attack or similar attacks which would have an impact on transaction finality, the type of consensus algorithm, and the risks relating to code defects, breaches, exploits and other threats relating to the tokenised securities and its supporting blockchain, the international/industry best practices and protocols that apply to them, and any adverse incidents relating to the DLT used and whether they have been resolved.

⁸ For example, custodians/wallet service providers.

⁹ For example, the private key and risks of theft, fraud, errors and omissions, and cybersecurity risks.

Where you might want to seek external assistance

Whether you are a dealer, advisor or manager, there are a number of areas where external assistance may be helpful in your tokenisation journey, including support/advice on capital raising and go to market strategy, any specific or associated tax implications, performing an end-to-end risk assessments and issuance of assurance and attestation opinions over the underlying assets. In particular:

- performing feasibility assessment on the strategy and advise on tax structure, token design, tokenomics, and smart contract selection
- designing a target operating model of an end-to-end asset tokenisation structure, (e.g. vendor selection, and roles & responsibilities design)
- obtaining legal support in fund and entity formation, fund and tokenisation documentation and legal and regulatory compliance
- performing risk assessments (e.g. ownership and technology risk) and developing control frameworks in the areas of governance and oversight
- performing independent assessment on your control environment and provide remediation recommendations
- reviewing your existing policies, procedures, systems and controls or assist in developing these following an independent risk assessment
- advise on token issuer, blockchain and custody solution selection and DD (e.g. cybersecurity DD on vendors)
- assisting with the building or performing of vendor management processes and controls to satisfy ongoing vendor DD requirements
- conducting smart contract audits (or perform an assessment over the smart contract audit already conducted)

Final thoughts

The Circulars, while widely anticipated, are still very welcome developments in line with the overall theme of expanding Hong Kong's virtual asset ecosystem - opening up retail access to a small sub-set of virtual assets on SFC licensed exchanges, and now more generally, authorised tokenised securities. However, the opening up of retail access *only* to primary issuances at this stage may disappoint participants who were expecting to be able to tokenise assets and list them for secondary trading.

In any event, expectations around suddenly being able to tokenise anything in the real world and to allow a vast multitude of retail investors to purchase these tokens should be tempered – SFC authorisation is still needed and nothing about that process, including its rigour and compliance standards, has changed for tokenised securities. It will be interesting to see how the market reacts to this development, and what impact it will have on the energy and buzz around the tokenisation movement as a whole. What is clear is that Hong Kong's regulatory framework has kept pace with, and continues to accommodate, trends in the market - and that is great news for all of us working in this space!

Let's talk

For a deeper discussion of how this impacts your business, please contact us.

PwC Hong Kong



Duncan Fitzgerald
Financial Services
Risk and Crypto Leader,
Crypto and Web3 Co-Leader
+852 2289 1190
duncan.fitzgerald@hk.pwc.com



Peter Brewin
Tax Partner,
Crypto and Web3 Co-Leader
+852 2289 3650
p.brewin@hk.pwc.com



Michael Footman
Financial Services
Risk and Regulatory Leader
+852 2289 2747
michael.hc.footman@hk.pwc.com



Sagan Rajbhandary
Financial Services
Crypto and Web3 team
+852 2289 5089
sagan.a.rajbhandary@hk.pwc.com

Tiang & Partners



Gaven Cheong
Head of Investment Funds,
AWM Compliance Services Leader
+852 2833 4993
gaven.cheong@tiangandpartners.com



Esther Lee
Registered Foreign Lawyer (Counsel
equivalent)
+852 2833 4950
esther.yt.lee@tiangandpartners.com

www.pwchk.com

www.tiangandpartners.com

The information contained in this document is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of legal, tax or other professional advice or service by PricewaterhouseCoopers ('PwC') and Tiang & Partners. PwC and Tiang & Partners have no obligation to update the information as law and practices change. The application and impact of laws can vary widely based on the specific facts involved. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual PwC client service team, law firm contact or your other advisers.

The materials contained in this document were assembled in November 2023 and were based on the law enforceable and information available at that time.

© 2023 PwC. All rights reserved. PwC refers to the China member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2023 Tiang & Partners. All rights reserved. Tiang & Partners is an independent Hong Kong law firm.



Tiang & Partners
程偉賓律師事務所
An independent Hong Kong law firm and
a member of the PwC network