VANUATU FINANCIAL SERVICES COMMISSION

GUIDANCE NOTES

ON

CUSTODY OF DIGITAL ASSETS

SUPERVISION DEPARTMENT

1. INTRODUCTION

The Commission is issuing this guideline in accordance with Section 19A of the Financial Dealers Licensing Act No. 9 of 2021.

The Commission does not envisages that the Financial Dealers licensed under the Financial Dealers Licensing Act to perform the full set of dealers and securities functions with respect to digital assets including maintaining custody of these assets unless they fully understand the inherent risks and have established mechanisms in a manner that addresses the unique risks attributes of digital assets and minimizes risk to investors and other market participants.

For purposes of this guideline, the term “digital asset” refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology (“distributed ledger technology”), including, but not limited to, “virtual currencies,” “coins,” and “tokens.”

The focus of this guideline is digital assets that rely on cryptographic protocols. A digital asset meets the definition of a “security” as a new asset class under the Financial Dealers Licensing Act.

2. BACKGROUND

Customers who deal in digital assets through the Financial Dealers licensed by the Commission to trade or custody of their digital assets are not protected by any statutory compensation in Vanuatu. Investors who trade in digital assets with these licensees or use them as custodian of their digital assets, do so at their own risk.

Financial Dealers acting as custodian of traditional securities is an integral part of their service, however, custody of digital assets raises certain compliance questions with respect to the Customer Protection requirements, as it may not be possible for a financial dealer to establish control over a digital asset with the same control mechanisms used in connection with traditional securities. Moreover, there have been instances of fraud, theft, and loss with respect to the custodianship of digital assets. Therefore VFSC would not accept a financial dealer licensed under the Financial Dealers Licensing Act to provide custodian services for Digital Assets unless they can provide evidence that they understand the risks and have established mitigating factors to manage the risks.

The risks associated with digital assets, are due in part to differences in the clearance and settlement of traditional securities and digital assets. Traditional securities transactions generally are processed and settled through clearing agencies, depositories, clearing banks, transfer agents, and issuers. A Financial Dealer’s employees, regulators, and external auditors can contact these third parties to confirm that the financial dealer is in fact holding the traditional securities reflected on its books

and records and financial statements, thereby providing objective processes for examining the broker's compliance with the Customer Protection. Also, the traditional securities infrastructure has established processes to reverse or cancel mistaken or unauthorized transactions. Thus, the traditional securities infrastructure contains checks and controls that can be used to verify proprietary and is designed "to give more specific protection to customer funds and securities, in effect forbidding brokers and dealers from using customer assets to finance any part of their businesses unrelated to servicing securities customers; *e.g.*, a firm is virtually precluded from using customer funds to buy securities for its own account").

3. RISK - DISTRIBUTED LEDGER TECHNLOGY

Digital assets that are issued or transferred using distributed ledger technology may not be subject to the same established clearance and settlement process familiar to traditional securities market participants. The manner in which digital assets are issued, held, or transferred may create greater risk for financial dealers who are maintaining custody of this type of asset. For example, a Financial Dealer could be victimized by fraud or theft, could lose a **"private key"** necessary to transfer a client's digital assets, or could transfer a client's digital assets to an unintended address without the ability to reverse a fraudulent or mistaken transaction.
In addition, malicious activity attributed to actors taking advantage of potential vulnerabilities that may be associated with distributed ledger technology and its associated networks could render the Financial Dealers unable to transfer a customer's digital asset.

The potential liabilities caused by the theft or loss of property from a custodian, including digital assets, could cause the Financial Dealer to incur substantial losses or even fail, impacting customers and other creditors.

A custodian that maintains custody of a fully paid or excess margin digital asset for a customer must hold it in a manner that is safe and secure, including that the digital asset must be in the exclusive physical possession or control of the custodian. A digital asset that is not in the exclusive physical possession or control of the custodian because, for example, an unauthorized person knows or has access to the associated private key (and therefore has the ability to transfer it without the authorization of the custodian) would not be considered as being held in a manner that is safe and secure.

As noted above, the loss or theft of digital asset may cause the firm and its digital asset customers to incur substantial financial losses. This, in turn, could cause the firm to fail, imperilling its traditional securities customers as well as the financial dealer's counterparties and other market participants.

4. VFSC POSITION

VFSC therefore requires that a firm providing custodian services of digital assets, must be a licensed custodian, well capitalized and well regulated by a reputable regulator in another jurisdiction.

A firm providing custody over digital assets must ensure that:

a) It take appropriate measures to shield traditional securities customers, counterparties, and market participants from the risks and consequences of digital asset fraud, theft, or loss;

b) Must be professional custodian operating in well regulated jurisdiction;

c) Must be sufficiently capitalised;

d) operate in a manner consistent with the Commission's position, that it could not deal in, effect transactions in, maintain custody of, or operate an alternative trading system for traditional securities;

e) by limiting its activities exclusively to digital asset, the custodian would shield its customers from the risks that could arise if the firm engaged in activities involving non-digital assets;

f) a custodian must establish, maintain, and enforce reasonably designed written policies and procedures to conduct and document the safe keeping of digital asset. Such policies and procedures should provide a reasonable level of assurance that any digital assets held in custody by the firm are in fact digital asset and not other types of securities.

5. POLICIES, PROCEDURES AND ASSESSMENT OF DISTRIBUTED LEDGER TECHNILOGY

A firm providing custody services must establish, maintain, and enforce reasonably designed written policies and procedures to conduct and document an assessment of the characteristics of a digital asset's distributed ledger technology and associated network prior to undertaking to maintain custody of the digital asset and at reasonable intervals thereafter. The assessment should examine at least the following aspects of the distributed ledger technology and its associated network, among others:

a) performance (*i.e.*, does it work and will it continue to work as intended);

b) transaction speed and throughput (*i.e.*, can it process transactions quickly enough for the intended application(s));

c) scalability (*i.e.*, can it handle a potential increase in network activity);

d) resiliency (*i.e.*, can it absorb the impact of a problem in one or more parts of its system and continue processing transactions without data loss or corruption);

e) security and the relevant consensus mechanism (*i.e.*, can it detect and defend against malicious attacks, such as 51% attacks or Denial-of-Service attacks, without data loss or corruption);

f) complexity (*i.e.*, can it be understood, maintained, and improved);

g) extensibility *(i.e.*, can it have new functionality added, and continue processing transactions without data loss or corruption); and

h) visibility (*i.e.*, are its associated code, standards, applications, and data publicly available and well documented).

The assessment also should examine the governance of the distributed ledger technology and associated network and how protocol updates and changes are agreed to and implemented. This would include an assessment of impacts to the digital asset of events such as protocol upgrades, hard forks, airdrops, exchanges of one digital asset for another, or staking. Such assessments would allow a firm to be able to identify significant weaknesses or other operational issues with the distributed ledger technology and associated network utilized by the digital asset, or other risks posed to the firm's business by the digital asset. That would allow the firm to take appropriate action to identify and reduce its exposure to such risks. Accordingly, if there are significant weaknesses or other operational issues with the distributed ledger technology and associated network, the firm would be able to determine whether it could or could not maintain custody of the digital asset.

6. POLICIES, PROCEDURES AND SAFEKEEPING OF DIGITAL ASSETS

A firm providing custody services must establish, maintain, and enforce reasonably designed written policies, procedures, and controls for safekeeping and demonstrating that the firm has exclusive possession or control over the digital assets that are consistent with industry best practices to protect against the theft, loss, and unauthorized and accidental use of the private keys necessary to access and transfer the digital assets the firm holds in custody. These policies, procedures, and controls should address, among other matters:

a) the on-boarding of a digital assets such that the firm can associate the digital asset security to a private key over which it can reasonably demonstrate exclusive physical possession or control;

b) the processes, software and hardware systems, and any other formats or systems utilized to create, store, or use private keys and any security or operational vulnerabilities of those systems and formats;

c) the establishment of private key generation processes that are secure and produce a cryptographically strong private key that is compatible with the distributed ledger technology and associated network and that is not susceptible to being discovered by unauthorized persons during the generation process or thereafter;

d) measures to protect private keys from being used to make an unauthorized or accidental transfer of a digital asset held in custody by the firm; and

e) measures that protect private keys from being corrupted, lost or destroyed, that back-up the private key in a manner that does not compromise the security of the private key, and that otherwise preserve the ability of the firm to access and transfer a digital asset security it holds in the event a facility, software, or hardware system, or other format or system on which the private keys are

stored and/or used is disrupted or destroyed. These policies, procedures, and controls for safekeeping and demonstrating the firm has exclusive possession or control over digital assets should serve to protect against the theft, loss, and unauthorized and accidental use of the private keys and therefore the customers' digital assets.

7. POLICIESS AND PROCEDURES TO ADDRESS FUTURE EVENTS

A firm providing custody services must establish, maintain, and enforce reasonably designed written policies, procedures, and arrangements to:

a) specifically identify, in advance, the steps it intends to take in the wake of certain events that could affect the firm's custody of the digital assets, including blockchain malfunctions, 51% attacks, hard forks, or airdrops;

b) allow the firm to comply with a court-ordered freeze or seizure; and

c) allow the transfer of the digital asset held by the firm to another special purpose broker-dealer, a trustee, receiver, liquidator, a person performing a similar function, or another appropriate person, in the event the custodian can no longer continue as a going concern and self-liquidates or is subject to a formal bankruptcy, receivership, liquidation, or similar proceeding. These policies and procedures should include measures for ensuring continued safekeeping and accessibility of the digital assets, even if the firm is wound down or liquidated, and thus would provide a reasonable level of assurance that a firm has developed plans to address unexpected disruptions to its control over the digital asset.

8. POLICIES AND PROCEDURES ON INVESTMENT RISK IN DIGITAL ASSETS

A firm providing custody services must have written disclosures to prospective customers about the risks of investing in or holding digital assets. The disclosures could include, among other matters:

a) prominent disclosure explaining that digital asset may not be "securities" as defined in the Financial Dealers Licensing Act, in particular, digital asset that are "investment contracts" but are not registered with the Commission or are excluded from definition of "securities" in the Financial Dealers Licensing Act and thus the protections under the laws of Vanuatu may not apply with respect to those securities;

b) a description of the risks of fraud, manipulation, theft, and loss associated with digital asset;

c) a description of the risks relating to valuation, price volatility, and liquidity associated with digital assets; and

d) a description of the processes, software and hardware systems, and any other formats or systems utilized by the firm to create, store, or use the firm's private

keys and protect them from loss, theft, or unauthorized or accidental use (including, but not limited to, cold storage, key sharding, multiple factor identification, and biometric authentication).

The purpose of such disclosures is to provide the prospective customers with sufficient and easily understandable information about the risks to enable them to make informed decisions about whether to invest in or hold digital assets through the Class D Licensee.

9. CUSTOMER WRITTEN AGREEMENT

A firm providing custody services must enter into a written agreement with each customer that sets forth the terms and conditions with respect to receiving, purchasing, holding, safekeeping, selling, transferring, exchanging, custodying, liquidating, and otherwise transacting in digital assets on behalf of the customer. This step would ensure documentation of the terms of agreement between the customer and the custodian providing custody of the customer's digital asset, which would provide greater clarity and certainty to customers regarding their rights and responsibilities under the agreement with the custodian.

10. AML/CFT PROCEDURE

A firm providing custody services must establish AML/CTF procedures to ensure compliance with the Anti-Money Laundering and Terrorist Financial Act of Vanuatu.

11. DEFINITIONS

For the purposes of this guidance notes, the following definition shall apply:

a "51% attack" is an attack on a blockchain or distributed ledger in which an attacker or group of attackers controls a majority of the network's hash rate, mining or computing power, allowing the attacker or group of attackers to prevent new transactions from being confirmed.

"**Hard forks**" refer to backward-incompatible protocol changes to a distributed ledger that create additional versions of the distributed ledger, potentially creating new digital assets.

"**Airdrop**s" refer to the distribution of digital assets to numerous addresses, usually at no monetary cost to the recipient or in exchange for certain promotional services.

"Staking" refers to the use of a digital asset in a consensus mechanism.

"Sharding" is a method for distributing data across multiple machines

Please contact the following person should you have any questions:

Mr. Joshua Tari

Manager, Supervision Department

Email: tjoshua@vfsc.vu

Phone: (678) 22247

Fax: (678) 22242

Dated this 28 day of September 2021