CANADIAN BLOCKCHAIN CONSORTIUM

Centre of Excellence

Canadian Blockchain Consortium Corp

Centre of Excellence

Conceptual Framework for Value-Referenced Cryptoassets (Stablecoins)

VERSION 2

November 1, 2023

1. Introduction to Value-Referenced Crypto Assets (Stablecoins)

1.1 Overview

This regulatory framework outlines the principles, guidelines, and requirements that should govern value-referenced crypto assets (VRCAs) in the Canadian financial landscape. VRCAs, a form of digital assets, aim to address the inherent volatility of cryptocurrencies while retaining the advantages of blockchain technology. The purpose of this framework is to establish a comprehensive and harmonized approach to the regulation of VRCAs, ensuring consumer protection, financial stability, and fostering innovation.

In recent years, there was little regulatory attention given to stablecoins (as VRCAs are widely referred to) in Canada. They were often grouped under the umbrella of crypto assets without specific guidance. However, in February 2023 and again in October 2023, the Canadian Securities Administrators (CSA) addressed VRCAs via staff notices, referring to them as value-referenced crypto assets (the term adopted herein). Staff expressed concerns about trading, borrowing, and lending related to VRCAs, highlighting various consumer protection and governance issues, such as insufficient information for users and significant risk. In their October, 2023 staff notice, the CSA proposed an interim set of terms and conditions applicable to both crypto trading platforms and VRCA issuers, in an attempt to address the aforementioned disclosure and governance-related issues.

The CSA asserted jurisdiction over VRCAs as CSA staff noted that most VRCAs meet the very broad definition of “security” (for example, depending on how the sale of a VRCA is structured, a VRCA may represent an evidence of indebtedness owed by the VRCA issuer to the VRCA holder, where “evidence of indebtedness” is included in the definition of “security” in virtually all provincial securities legislation). However, recent case law from several provinces, including British Columbia and Alberta, appears to challenge this interpretation. Particularly, for an "evidence of indebtedness" to be categorized as a security, there needs to be funds raised from the public for an investment purpose. A predominant portion of VRCAs are not acquired with the anticipation of appreciation in value, thereby, in most instances, lacking the necessary investment purpose.

Since the value of a VRCA is derived or based upon the value of the underlying asset backing or anchored to the VRCA, VRCAs may also fall within the expansive definition of “derivative” found in Canadian securities law. Despite being commonly used for payment purposes, VRCAs might meet the definition of a security and a derivative but might not necessarily be used for investment purposes or with investment intent. The CSA emphasized the need for reserves and required issuers to provide disclaimers about the stability of VRCAs. The CSA appears to be more comfortable with fiat-backed VRCAs and expressed discomfort with algorithm-backed VRCAs in trading.

In connection with a confidential consultation, which proposed draft terms and conditions governing the trading of VRCAs, the CSA asked for examples of VRCAs that maintained their peg in certain market conditions. However, the Canadian regulatory landscape for trading VRCAs remains uncertain, and there is no conclusive, comprehensive regulatory framework in place governing the trading of VRCAs in Canada. The lack of communication between provincial and federal governments, both of which are represented in the process (given that VRCAs have characteristics of payment instruments, which is governed by the federal government, and securities, governed by the provinces), creates a conflict regarding the regulation of VRCAs. There are already carve outs for banks issuing or guaranteeing debt, exempting them from prospectus and registration requirements, but no clear control asserted by the federal government over VRCAs used for payments.

The CSA staff notice from October 2023 requires VRCA issuers to publicly file an undertaking which includes a condition that VRCA issuers obtain a monthly assurance report, prepared by a public accountant. But the governing body of auditors, such as Canadian Public Accounting Board (CPAB) and Public Company Accounting Oversight Board (PCAOB), or Chartered Professional Accounting bodies, such as CPA Canada, have not provided guidance on the attestation standards and associated procedures. In the absence of such guidance, the procedures covered in existing monthly attestations provided in accordance with the Agreed Upon Procedures (AUP) standards lack consistency and robustness to ensure that the risks of material misstatement of management's assertion on VRCAs issuance, redemption and reserve assets, whether due to fraud or error, are appropriately addressed. In most cases, "big 4" accounting firms are unwilling to accept such regular attestation engagements due to lack of clear guidance. It is important to note that although the PCAOB has issued some guidance on issues related to previously completed attestations, it has not specifically addressed VRCAs.

CSA shall push the likes of CPAB and CPA Canada to provide clear guidelines on scope, independence, engagement acceptance or continuance, and deliverable requirements for such monthly attestations providing a pathway for VRCA issuers and accounting professionals to meet the enhanced transparency requirements.

Given the importance of VRCAs in Canada's digital currency economy, the need for a well-defined regulatory framework is of paramount importance to Canadian participants. Such guidance would set a clear stage for the trading of VRCA's, enabling dealers in digital currency to align their operations and comply with regulatory requirements. It is crucial for the CSA to collaborate with the accounting industry and other relevant stakeholders to establish a practical and effective approach to monthly attestations.

The potential conflict between federal law (payments) and provincial law (securities/derivatives) as it pertains to the regulation of VRCAs further complicates matters. A unified and cohesive stance is needed to ensure non-duplicative, unambiguous and consistent regulation, and in order to foster investor confidence in VRCAs offerings. The Canadian digital asset industry would greatly benefit from a collaborative approach between both levels of government.

Overall, VRCAs have emerged as a very significant asset class in the cryptocurrency landscape, offering various potential benefits, including but not limited to enhanced digital payments, offered domestically or on a cross-border basis. Financial institutions are expressing interest in offering VRCAs or dealing in them, and large multinational corporations, such as PayPal, are starting to offer them to consumers as a fast and easy way to send funds without the involvement of banks. We do not want Canadians to be excluded from VRCA service offerings, nor is it in the best interest of any level of the Canadian government to lose a talented workforce and economic incentives to other countries. As per above, there is regulatory uncertainty surrounding the regulation of VRCAs in Canada. The CSA's recent staff notice and consultation efforts are positive steps towards addressing this concern, but more concrete and detailed guidance from the federal government and the CSA is essential. By providing clearer guidance on gray areas which include, but are not limited to, monthly reserve asset attestations, the nature and composition of reserve assets held by VRCA issuers, the public messaging around VRCAs used by crypto asset trading platforms, and the use of VRCAs as payment instruments, the CSA can help stabilize the Canadian VRCA market and foster responsible innovation in the digital payment space. Collaboration between regulatory authorities, accounting firms, and other stakeholders is crucial to develop a robust and effective regulatory framework that promotes growth while safeguarding investor interests.

Current Challenge:

Regulatory safeguards for all types of VRCAs are vital to ensure integrity and stability within the market. This includes a systematic approach such as implementing issuer registration requirements to validate and track all participants. A clearly defined taxonomy is essential for distinguishing and clarifying the various VRCA forms, setting standards for industry comprehension. Prudential rules provide the governing principles to ensure financial soundness and ethical behavior among issuers. Collateral custodial safeguards need to be established to protect and manage the underlying assets, reinforcing confidence in the stability of VRCAs. Transparency in reporting is pivotal for accurate oversight, while comprehensive risk disclosure provides potential investors and users with necessary information to make informed decisions. Lastly, containment measures must be in place to mitigate potential adverse effects, establishing clear guidelines for intervention in times of market stress or other unusual circumstances. Together, these elements form a robust regulatory structure, promoting transparency, security, and trust within the rapidly evolving landscape of VRCAs.

We have identified various practical uses for VRCAs that go beyond the CSA’s assertion, as contained for example in CSA Staff Notice 21-332 *Crypto Asset Trading Platforms: Pre-Registration Undertakings - Changes to Enhance Canadian Investor Protection*, that VRCAs serve solely for buying securities. Participants in the workshop referenced below which occurred on July 26, 2023, highlighted different ways they have seen VRCAs being used across various sectors and situations. This includes embedding VRCAs in private blockchain applications for equipment leasing, using them as an intermediate currency for settling transactions, and converting them into any fiat currency, as demonstrated in Ukraine during wartime.

In the course of identifying those uses we determined that while some uses and structures created VRCAs that are a security and should be regulated as such, many were not related to use as a security and rather were used for trade transactions, payment systems, and providing transaction assurance among others. The use and structure of the VRCA, particularly its linked assets, affects how and by whom the VRCA and its use should be regulated. The different regulatory regimes have different aims, policies and processes and these differences need to be taken into account in recommending a regulatory approach to an asset that can be many things and function in many different roles. The Consortium has tried to take these aspects of regulation into account in making recommendations in this paper.

The following is a summary of the various VRCA use-cases that many crypto asset trading platforms, lawyers, consultants and payment processors are witnessing in the market today:

1. **Equipment Leasing**: Utilizing VRCA as a fiat-embedded currency within private blockchain applications for equipment leasing.

2. **Currency Exchange**: Utilization of a VRCA like USDT for easier currency exchange in transactions, both in everyday use and in specific contexts such as war zones where wire transfers may not be possible.

3. **Cross-Border Transactions**: VRCAs facilitate efficient money transfer across borders, for purposes ranging from sending remittances to paying international vendors and employees.

4. **Reducing Business Costs**: Technologies using VRCAs, such as USDT, have cut down on back-end business costs, with examples like grain sales in Ukraine.

5. **Paying Contractors**: VRCAs are used to quickly and easily pay contractors all over the world, demonstrating its versatility.

6. **Royalties and Ecommerce**: An entertainment lawyer confirmed that VRCAs have been used for automatic royalty payments, and there is anticipation that ecommerce for both vendors and clients may shift towards VRCAs.

7. **Smart Contracts**: VRCAs are becoming essential in smart contracts, maintaining stability during extended shipping or development times.

8. **Legal and Government Use**: Law firms and governmental entities are also seeing value in VRCAs for collecting fees or retainers, offering instant cross-border payment mechanisms.

9. **Micro and Macro Transactions**: For both small and large transactions, VRCAs are seen as an efficient alternative to traditional solutions, devoid of complex layers.

10. **Trade Payment and Finance:** A substantial market has emerged for VRCAs as a seamless and efficient solution for global transactions, catering to diverse needs from cross-border trade settlements to supply chain financing.

The flexibility of VRCAs has proven valuable in international money remittances, as in sending money from Canada to the Philippines and Cameroon.

The conceptual framework (the **Framework**) presented herein offers a comprehensive guide to VRCAs and outlines recommendations which can be used as a basis for building future regulation governing VRCAs, amending existing regulation and for the development of policies. The Framework delves into detailed categorizations of VRCAs and for each type, encompasses guidelines on authorization and licensing, reserve and collateral requirements, governance and risk management, consumer protection and disclosure, market conduct, anti-money laundering measures, financial stability and stress testing. By addressing both the general landscape and specific challenges, this Framework seeks to ensure a responsible, transparent, and efficient regulatory environment for VRCAs, reflecting the evolving nature of the digital economy. The Framework is based in part on feedback gathered from a workshop which occurred on the afternoon of July 26, 2023, which was attended by approximately 25 digital asset industry experts, ranging from principals of crypto asset trading platforms, to lawyers, consultants, accountants and other industry professionals from Canada, the United States, the Caribbean and Europe.

1.2 Definition

For the purposes of this Framework, VRCAs are defined as digital assets designed to maintain a stable value by anchoring to a stable fiat currency, cryptocurrency or commodity which are held in reserve, or alternatively by an algorithmic mechanism or a combination of the above.

1.3 Scope

A VRCA arrangement typically provides three core functions with associated activities:

1) issuance, redemption and stabilization of the value of the VRCA;
    a) Issuing, creating and destroying VRCA
    b) Managing reserve assets
    c) Providing custody/trust services for reserve assets

2) transfer of VRCA;
    a) Operating the infrastructure
    b) Validating transactions

3) interaction with users for storing and exchanging VRCA
    a) Storing the private keys providing access to VRCA (wallets)

b) Exchanging, trading, reselling and market making of VRCA

Given these functionalities, VRCA might exhibit functional resemblances to payment systems or financial services or products, like deposit obligations or securities (comprising pooled investment strategies), which could consequently expose them to identical risks. Nevertheless, they might also introduce novel risks contingent upon the structure of the VRCA arrangement.

This Framework may apply to VRCA dealers, VRCA issuers and custodians who hold custody of a VRCA reserve asset.

1.4 Regulatory Objectives

The key objectives of this framework are as follows:

1. **Consumer Protection:** To safeguard the interests of VRCA users by ensuring transparency, disclosure of risks, and promoting fair practices.

2. **Financial Stability:** To mitigate potential systemic risks and ensure the stability of the financial system arising from VRCA operations.

3. **Market Integrity:** To prevent market abuse, fraudulent activities, and money laundering related to VRCA transactions.

4. **Innovation and Market Development:** To foster a conducive regulatory environment that encourages responsible innovation and growth in the VRCA market.

1.5 Regulatory Principles

This regulatory approach is guided by the following principles and is grounded in the foundational principle of “same business, same risk, same rules”:

1. **Technology-Neutrality:** To accommodate advancements in technology while ensuring regulatory efficacy.

2. **Proportionality:** To calibrate regulations based on the size, complexity, and systemic importance of VRCA activities.

3. **Risk-Based Approach:** To identify and address potential risks associated with VRCA operations.

4. **International Cooperation:** To collaborate with international counterparts on matters of common interest and cross-border stability.

5. **Regulation to Recognize Use and Structure:** To categorize the VRCAs as to structure, linked asset and use to identify the correct regulatory regime and approach for the functionality and user exposure.

1.6 Framework Structure

This regulatory framework is divided into distinct sections, each addressing specific aspects of VRCA operations:

a. **Authorization and Licensing:** Procedures and requirements for VRCA dealers, VRCA issuers and custodians seeking regulatory approval.

b. **Reserve and Collateral Requirements:** Guidelines for the composition, management and custody of VRCA reserves.

c. **Governance and Risk Management:** Standards for governance structures, risk management frameworks, and internal controls.

d. **Consumer Protection and Disclosure:** Measures to protect VRCA users and ensure adequate disclosure of risks.

e. **Market Conduct and Anti-Money Laundering (AML) Measures:** Rules to maintain market integrity and prevent illicit activities.

f. **Financial Stability and Stress Testing:** Methods to assess and address systemic risks arising from VRCA operations.

1.7 Compliance and Enforcement

This framework includes provisions for monitoring compliance, conducting audits, and imposing penalties for non-compliance. Regulatory authorities shall have the power to investigate, intervene, and take appropriate enforcement actions to maintain regulatory compliance and uphold the objectives of this framework.

d. Consumer Protection and Disclosure

User Rights and Obligations: Provide clear information to users about their rights and obligations. This could include information about the nature and enforceability of any redemption rights, the process for redemption, and the user's responsibilities in relation to the use of the stablecoin.

A FBCA issuer must specify and disclose that all the holders of its FBCA would have a direct legal right to redeem the SCS for the pegged currency at par value (or any other currencies of equivalent value), and that redemption requests can be made at any time with the FBCA issuer.

Any conditions that the FBCA issuer wishes to impose for redemptions, such as fees and minimum redemption amount, must be reasonable and clearly disclosed on its corporate website and any other communication channels with the public regarding the FBCA.

An FBCA issuer should return the par value of the B to the B holder expediently, and in any case, no later than five business days from the date when a legitimate redemption request is received. A redemption request is generally deemed as legitimate if the B holder can meet the B issuer's onboarding requirements, including the applicable customer onboarding rules to mitigate ML/TF risks. During times of stress, a short redemption period requirement may exacerbate the risk of a run on the B and the B issuer.

Whitepaper: A whitepaper is a comprehensive and structured document that delineates the foundational principles, technical architecture, economic mechanisms, and operational intricacies of a VRCA project. It serves as the primary informational source for stakeholders, investors, regulators, and the broader public, offering an authoritative elucidation of the VRCA's design, purpose, and envisaged impact on the financial ecosystem. The whitepaper outlines the VRCA's value proposition, underlying algorithmic or collateral mechanisms, governance structure, security protocols, and risk mitigation strategies. In doing so, it establishes a transparent framework that guides informed decision-making and regulatory considerations while promoting transparency, accountability, and responsible innovation in the domain of VRCAs.

An B issuer must publish a white paper on its corporate website, to disclose information such as the description of the B , rights and obligations of the B issuer and B holders, risks that can affect the stability of the B value and ability of the B issuer to fulfill its obligations etc, and update such information as needed.

Terms and Conditions: Make the terms and conditions of the B arrangement clear and easily accessible. These should cover all aspects of the user's relationship with the FBCA arrangement, including the use of the FBCA, the handling of user data, and the resolution of disputes.

Legal Compliance: Ensure that all information provided to users and stakeholders complies with all applicable laws and regulations. This could include laws and regulations related to consumer protection, data protection, and financial services.

e. Market Conduct and Anti-Money Laundering Measures

Compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations is essential for FBCA issuers to prevent illicit activities and enhance user protection.

FBCA issuers should have mechanisms in place to freeze assets in compliance with relevant regulations and policies. The challenges and limitations associated with these procedures should be carefully addressed.

Anti-Money Laundering (AML) and Financial Crime:

AML Compliance: Implement robust AML procedures to prevent, detect, and report potential money laundering activities. This could include customer due diligence (CDD) procedures, transaction monitoring systems, and suspicious activity reporting mechanisms.

Sanctions Compliance: Establish procedures to ensure compliance with economic and trade sanctions. This could include sanctions screening systems, sanctions risk assessments, and procedures for handling potential sanctions hits.

Fraud Prevention: Implement measures to prevent and detect fraudulent activities. This could include fraud detection systems, fraud risk assessments, and procedures for investigating and reporting suspected fraud.

Financial Crime Training: Provide regular training for staff on AML and financial crime risks and compliance. This could include training on recognizing and reporting suspicious activities, understanding sanctions requirements, and preventing and detecting fraud.

Financial Crime Risk Management: Develop a comprehensive financial crime risk management framework. This should include policies and procedures for managing AML, sanctions, and fraud risks, a designated officer responsible for financial crime risk management, and regular reviews and audits of the financial crime risk management framework.

f. Financial Stability and Stress Testing

Prudential Requirements:

Base capital: Higher of C$1 million or 50% of annual operating expenses of the FBCA issuer.

Solvency: To hold at all times, liquid assets which are valued at higher of 50% of annual operating expenses or an amount assessed by the FBCA issuer to be needed to achieve recovery or an orderly wind-down.

Business restrictions: An FBCA issuer is not allowed to undertake other activities that introduce additional risks to itself. This includes investing in and extending loans to other companies, lending or staking of FBCA and other deposit taking institutions, and trading.

2.2 VRCA Type: **Commodity-Referenced Crypto Assets (Commodity-Backed Stablecoins or CRCA)**

Definition:

Commodity-referenced crypto assets are a category of digital or virtual assets that are pegged to the value of physical commodities such as precious metals, agricultural products, or energy resources. These crypto assets derive their value and stability from underlying commodities that act as collateral or references.

In a typical structure, each unit of the commodity-referenced crypto asset is supported by a defined quantity or value of a specific commodity or basket of commodities, held and managed by the issuer or a third-party custodian. The backing commodities may be held in physical form, or through derivatives, contracts, or other financial instruments tied to the commodities' market prices.

Commodity-referenced crypto assets constitute a negotiable claim against the issuer. When these crypto assets change hands, the issuer's obligation shifts from one holder to the next, without requiring an adjustment to the issuer’s commodity holdings. it is only where a holder wishes to redeem a commodity-referenced crypto asset, that the issuer’s commodity/asset balances are updated. The transfer of a commodity-referenced crypto asset is executed solely at the discretion of the holder, and does not necessitate the consent or participation of the issuer. Upon receipt of a commodity-referenced crypto asset, an individual assumes ownership and, in turn, the corresponding liability from the issuer.

It is noteworthy that fluctuations from the nominal value, or par value, of commodity-referenced crypto asset can occur, despite concerted efforts by issuers to maintain stability. Although such variations may be minimal under ordinary circumstances, they have the potential to escalate significantly during times of market turmoil.

Utility

Asset Tokenization and Investment Opportunity: Commodity-referenced crypto assets can represent a fraction of ownership in a physical commodity. By tokenizing the asset, they can be easily traded and invested in, offering a new avenue for investment and portfolio diversification.

Payment Facilitation and Settlement: These assets offer a stable medium of exchange, particularly in regions with volatile fiat currencies. Businesses and individuals can utilize them for seamless cross-border transactions, reducing conversion fees and time delays often associated with traditional banking systems.

Supply Chain Management: In industries that depend on commodities, these crypto assets can be used to streamline and automate transactions throughout the supply chain. By

embedding them into smart contracts, parties can set predetermined rules for the automatic transfer of assets upon the fulfillment of specific conditions, such as the delivery of goods.

Hedge Against Volatility: For individuals and businesses concerned with the volatility of traditional cryptocurrencies, commodity-referenced crypto assets offer a safer alternative. Since they are pegged to tangible commodities, they are less prone to wild price fluctuations, providing a more stable store of value.

Enhanced Liquidity: By representing ownership in a commodity, these crypto assets can increase market liquidity. They allow smaller investors to participate in the commodities market, and fractional ownership ensures that these assets can be bought and sold in more manageable increments.

Insurance and Risk Management: Some organizations are using commodity-referenced crypto assets to mitigate risks associated with commodity price fluctuations. By holding these assets, they can create a natural hedge against potential adverse price movements in the underlying commodity.

a. Authorization and Licensing

Specific Regulatory Context:

Securities Law

Although it depends heavily on the specific facts and circumstances, an offering of a commodity-referenced crypto asset may meet the definition of a “security” contained in the *Securities Act (Ontario)* R.S.O. 1990, Chapter S.5 (OSA) because it involves an “evidence of indebtedness” that is otherwise not specifically excluded from subparagraph (e) of the definition in the OSA (e.g., an evidence of deposit issued or guaranteed by a financial institution). This interpretation may seem overly broad, but it aligns with the OSA's language and regulatory structure, as stated by the Ontario Court of Appeal (ONCA) in the 2018 *Ontario Securities Commission v. Tiffin* decision.[1] Tiffin has held that this interpretation is consistent with the plain text of the OSA and the logic of the regulatory scheme which contains broad definitions with equally broad exemptions to otherwise exclude transactions that should not be captured under the OSA.

However, this classification is only applicable in the usage context of investment and not in other uses such as immediate payment, trade facilitation, financial services delivery, among others. The usage most easily characterized as being a payment and not a security is where the acquisition of the CRCA is accompanied by essentially immediate (or at least short term) use for payment to another third party. Another is purchase facilitation where again on a short term

[1] 142 OR (3d) 223 (Tiffin). The ONCA ruled that the trial judge erred in finding that promissory notes did not fall within definition of "security" under s.1 of the OSA and that the trial judge improperly imported the American "family resemblance" test into Ontario securities law to determine whether promissory notes were excluded from statutory definition of "security".

basis the CRCA is paid to a seller and the right to ownership of another asset, potentially also in digital form, is given to the user of the CRCA. Another is to facilitate a series of payments within a transaction chain on a short term basis against payment requirements that are not based on value or value change for the CRCA. None of these uses have the characteristics of a security and should not be regulated as such. Where the acquisition and holding of the CRCA has the characteristics of a security, including a longer term holding without a designated use, an arbitrage intention and similar, regulation of that as a security is accepted as the appropriate action. Where the use of the CRCA does not have such characteristics the CRCA should be regulated for the use and its characteristics by the appropriate regulatory body.

Commodity-referenced crypto assets may meet the definition of an investment contract and a “document constituting evidence of title to or interest in the capital, assets, property, profits, earnings or royalties of any person or company”, which corresponds with subparagraph (b) in the definition of security contained in the OSA. In addition, these assets will likely meet the very broad definition of a “derivative” under the OSA, because commodity-referenced crypto assets are typically tied to the price of a specific commodity, such as gold, oil, or other tangible goods. The value of the asset is derived from, referenced to, or based on the underlying commodity's value, price, or rate. This connection to an underlying interest fits the definition of “derivative” provided in the OSA. In most provinces in Canada, derivatives are regulated as securities and subject to legislation, national instruments and staff notices promulgated by members of the Canadian Securities Administrators.

The exception to this characterization will be the use of the CRCA to immediately upon payment receive the evidence of entitlement to ownership attributes of a commodity to be acquired. This is different than a backing of the CRCA by a commodity as the stabilizing factor for the CRCA and will need to be clearly differentiated. The mere linkage to a commodity may not create a security or a derivative if the use is for the true purchase of the intended commodity. Whether this use is a derivative in nature will not arise from the digital nature of the CRCA but rather the contract arising from the payment for the commodity. Regulation should then be applied according to the transaction and the commodity linked to the CRCA. In order for the CRCA to be effectively and efficiently used to facilitate trade including in commodities this difference will need to be recognized in the application of the regulatory regime.

The distribution of securities to Canadian residents and trading in securities triggers prospectus and registration requirements under Canadian securities laws, unless an exemption can be relied upon. If the sale of a commodity-referenced crypto asset triggers the prospectus and registration requirements, provincial and territorial securities regulators will have jurisdiction over the issuer, dealer and custodian of these assets.

Depending on the unique facts and circumstances of a particular offering, it is possible that there may be instances where the sale of a commodity-referenced crypto asset does not trigger Canadian securities laws. In this case, the asset would likely be akin to a commodity and would be subject to the complex regulatory framework governing commodities in Canada.

Commodities Laws

Regulation governing the sale of commodities in Canada exists at both the federal and provincial levels. Some provinces have specific acts that regulate commodity trading, such as Ontario's *Commodity Futures Act* RSO 1990, c C.20, which is governed by the Ontario Securities Commission. At the federal level, the *Competition Act* RSC 1985, c C-34 addresses anti-competitive practices within commodity markets, and is governed by the Competition Bureau. The *Canada Consumer Product Safety Act SC 2010, c 21* ensures that products, including commodities, are safe for use, and is governed by the Minister of Health (Health Canada). There is also agricultural marketing legislation, natural resources acts and environmental legislation which may apply to commodity-referenced crypto assets which do not meet the definitions of “security” and “derivative”.

b. Reserve and Collateral Requirements

Commodity-referenced crypto assets are typically backed by underlying commodities, and the integrity of this backing is crucial to maintain the value and stability of the crypto asset. Therefore, reserve and collateral requirements are essential components in the regulatory framework.

Reserve Requirements

Quantity and Quality of Reserves: Regulations must define the acceptable types and quantities of commodities that can be used as reserves, ensuring that they are of a standard quality and that the quantity is proportionate to the number of crypto assets in circulation.

Valuation Methodology: Standardized methods for valuing the underlying commodities must be established to prevent inconsistencies and manipulation.

Rebalancing Mechanisms: Provisions must be in place to periodically assess and rebalance the reserves to maintain alignment with the crypto asset's value.

Collateral Management

Custody and Storage: Regulations must dictate secure custody and storage requirements, particularly if the commodities are physical (e.g., gold, oil). This includes security protocols, insurance coverage, and third-party audits.

The comments as to the structure and use of reserve techniques using trust-based legal concepts are equally applicable to CRCAs as to FBCAs. The use of the well recognized legal techniques used to ring fence and protect assets held as reserve from the creditors of the issuer should be considered. These techniques have stood the test of court assessment in bankruptcy and insolvency matters and can be implemented by required asset segregation and trust language that complies with true trust requirements. The beneficiaries of this are the holders of the CRCA. This does not require the use of professional trustees or financial institutions and

need not add cost or complexity if done in a manner consistent with the legal requirements for a true trust.

Liquidity Management: Guidelines should be provided on how issuers can manage the liquidity of the underlying commodities, including rules for liquidation to ensure that investors can redeem their assets if needed.

Third-Party Oversight: Regulations may require third-party entities to oversee collateral management to ensure unbiased and consistent practices.

Transparency: Issuers should provide regular disclosures on the composition and valuation of the reserves, giving investors insights into the backing of their assets.

c. Governance and Risk Management

Strong governance and risk management are essential to maintain the integrity, stability, and confidence in commodity-referenced crypto assets. Regulations and best practices in these areas may include:

Governance Structure

Roles and Responsibilities: Clearly defined roles, responsibilities, and accountabilities within the issuing organization must be established to prevent conflicts of interest and ensure alignment with the best interests of holders.

Board Oversight: The governance structure may require oversight by a board or governance committee with the expertise to evaluate the risks and strategies associated with commodity-referenced crypto assets.

Ethical Standards: Implementing a code of conduct or ethical standards that guide decision-making and operations.

Risk Management Framework

Commodity Market Risk

Price Volatility: The underlying commodities' prices may fluctuate due to changes in supply, demand, geopolitical events, or economic conditions. These fluctuations can affect the value of the commodity-referenced crypto asset. **Mitigation:** Implementing hedging strategies using derivatives and constantly monitoring market trends can help stabilize the asset. Transparency in reporting the commodity's underlying metrics can also aid in investor understanding and risk management.

Liquidity Risk: Some commodities might have less liquid markets, making them difficult to buy or sell without significantly impacting their price, potentially affecting the stability of the asset. ·

Mitigation: Diversifying commodity backing, setting minimum liquidity thresholds, and engaging multiple market makers can enhance liquidity. Regulatory oversight of market practices might also minimize manipulation and ease liquidity concerns.

Operational Risk

Custodial Risk: If the commodities are held in physical form, there is a risk related to the storage, security, and integrity of the commodities. **Mitigation:** Ensuring proper storage facilities, conducting regular audits, and implementing insurance protections can mitigate physical commodity risks.

Technology Risk: Failures, vulnerabilities, or inefficiencies in the technology used to issue or manage the crypto assets can lead to disruptions, fraud, or loss. **Mitigation:** Regular security audits, using established and vetted technology platforms, and implementing redundancy measures can reduce technology-related risks.

Counterparty Risk

Issuer Risk: The failure or fraudulent activity of the issuer could lead to a loss of value or confidence in the crypto asset. **Mitigation:** Regulatory oversight, transparency in operations, and regular audits can provide safeguards against issuer-related risks.

Third-party Risk: Involvement of third-party custodians or other entities introduces additional risk if those parties fail to meet their obligations. **Mitigation:** Due diligence on third parties, contractual agreements with clear obligations, and ongoing monitoring of third-party performance can reduce this risk.

Redemption Risk

Redemption Constraints: Limitations or restrictions on redeeming the crypto asset for the underlying commodity or fiat currency can create liquidity problems for investors. **Mitigation:** Clear and transparent redemption policies, with adequate liquidity provisions, can minimize constraints on redemption.

Settlement Risk: Delays or failures in the settlement process can affect investors' ability to realize value from their holdings. **Mitigation:** Using reliable settlement systems, monitoring settlement processes, and implementing automated reconciliation can alleviate settlement risk.

Concentration Risk

Single Commodity Exposure: If the crypto asset is linked to a single commodity, it may be more susceptible to specific market conditions affecting that commodity. **Mitigation:** Encouraging or mandating diversification of underlying commodities can limit exposure to any single commodity's market conditions.

Over-Concentration in Portfolio: Holders with a high concentration of commodity-referenced crypto assets might face increased risk if the market for those specific commodities faces sudden changes. **Mitigation:** Educating investors on diversification benefits and providing clear guidelines on portfolio construction can mitigate concentration risks.

Consumer Protection and Disclosure Risk

Information Asymmetry: Lack of transparency or misleading information regarding the backing commodities can lead to misinformed investment decisions.**Mitigation:** Enforcing transparency requirements, regularly updating disclosures, and ensuring that information is clear and understandable can promote informed decision-making.

Fraud Risk: Scams or fraudulent schemes related to these assets can result in financial loss. · **Mitigation:** Regulatory oversight, robust legal enforcement, and public awareness campaigns can help in detecting and preventing fraud related to commodity-referenced crypto assets.

Risk Assessment: Regular risk assessments should be conducted to identify, evaluate, and prioritize risks specific to commodity-referenced crypto assets, such as market risk, operational risk, and regulatory risk.

Risk Mitigation Strategies: Tailored strategies should be developed to mitigate identified risks, including hedging strategies for commodity price risks and cybersecurity measures for technological risks.

Monitoring and Reporting: Continuous monitoring and reporting mechanisms should be in place to track risk exposure and the effectiveness of mitigation strategies.

Disaster Recovery and Business Continuity Planning: Robust plans should be established to ensure that operations can continue in the event of unforeseen disruptions.

Regulatory Compliance

Alignment with Existing Regulations: Compliance with existing laws and regulations applicable to financial instruments, commodities, and technology should be expected.

Adherence to Specific Guidelines: Compliance with specific regulatory requirements related to commodity-referenced crypto assets, including licensing, reporting, and consumer protection.

Stakeholder Engagement

Transparency with Investors: Regular communication with investors about governance practices, risk management strategies, and the status of the underlying commodities should be expected.

Engagement with Regulators and Industry Bodies: Collaboration with regulatory authorities and industry organizations to align with standards and contribute to the development of best practices should be encouraged.

Market Volatility

Stabilization Mechanisms: Regulations should require issuers to implement mechanisms that minimize the impact of market volatility. Guidelines should be established on the use of stabilization tools and automated algorithms to maintain the peg with the underlying commodity.

Reserve Requirements: Stringent requirements regarding the composition and value of reserves are required. Periodic stress-testing of reserves should be conducted to ensure that they can withstand extreme market conditions.

Transparency and Reporting: Real-time reporting of reserve status, market orders, and significant price movements should be mandated with a requirement for third-party audits to verify the adherence to volatility control measures.

Investor Education and Communication: Guidelines should be established for issuers to provide clear explanations about market volatility risks and the measures taken to mitigate those risks.

Counterparty Risk

Due Diligence Requirements: Regulations should compel issuers, exchanges, and custodians to perform due diligence on counterparties and a framework for assessing and categorizing the risk profile of counterparties should be developed.

Risk Management and Mitigation Policies: Issuers should be required to have detailed risk management and mitigation strategies in place, and an obligation to diversify counterparties and to have contingency plans for potential defaults.

Monitoring and Reporting: Issuers should be required to conduct continuous monitoring of counterparty behavior and risk exposure. They should be subject to regular reporting to regulatory authorities and disclosure to investors.

Regulatory Collaboration: Cooperation between regulatory bodies across jurisdictions should be encouraged to share information and monitor global counterparty risks.

d. Consumer Protection and Disclosure

Transparency and Full Disclosure Regulations: Detailed requirements should exist for issuers to disclose all aspects of the commodity-referenced crypto assets, including potential risks, fee structures, and rights. Mandatory real-time reporting of relevant operational metrics and the use of third-party verification should be required.

Consumer Education and Awareness Programs: There should be an expectation to implement educational campaigns to increase public awareness and understanding of commodity-referenced crypto assets. Guidelines should be established for providing clear, concise, and understandable educational materials.

Complaint Handling and Redress Mechanisms: Clear and accessible channels for consumer complaints and disputes should be established, and requirements for timely and fair resolution of disputes, possibly through an independent ombudsman service should be established.

Cybersecurity and Fraud Prevention: Rigorous standards for cybersecurity to protect consumer data and assets should exist and a framework for monitoring, detecting, and combating fraudulent activities should be developed.

Accessibility and Non-discriminatory Practices: VRCA projects should ensure equitable access to services related to commodity-referenced crypto assets, prohibit discriminatory practices and foster inclusion.

Whitepaper: A whitepaper is a comprehensive and structured document that delineates the foundational principles, technical architecture, economic mechanisms, and operational intricacies of a VRCA project. It serves as the primary informational source for stakeholders, investors, regulators, and the broader public, offering an authoritative elucidation of the VRCA's design, purpose, and envisaged impact on the financial ecosystem. The whitepaper outlines the VRCA's value proposition, underlying algorithmic or collateral mechanisms, governance structure, security protocols, and risk mitigation strategies. In doing so, it establishes a transparent framework that guides informed decision-making and regulatory considerations while promoting transparency, accountability, and responsible innovation in the domain of VRCAs.

A VRCA issuer must publish a white paper on its corporate website, to disclose information such as the description of the VRCA, rights and obligations of the VRCA issuer and VRCA holders, risks that can affect the stability of the VRCA value and ability of the VRCA issuer to fulfill its obligations etc, and update such information as needed.

e. Market Conduct and Anti-Money Laundering Measures

Market Conduct Guidelines

Fair Trading Practices: VRCA issuers should be prohibited from manipulative and deceptive practices, such as front-running, wash trading, or insider trading. Requirements should exist for transparent pricing, clear terms of service, and non-discriminatory access to services.

Investor Protection: Rules should be implemented for transparent disclosure of fees, risks, terms and conditions, and other vital information. A redress mechanism should be established to handle customer complaints and disputes.

Reporting Requirements: Regular reporting of trading volumes, open interest, margin balances, etc. should be reported to the relevant regulatory authorities. Requirements for immediate disclosure of significant events that could impact market stability or investor interests should be determined.

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Measures

Customer Due Diligence (CDD): Know Your Customer (KYC) procedures should be implemented to verify and maintain records of customers' identities. Enhanced Due Diligence (EDD) for customers who may pose higher risks, such as foreign Politically Exposed Persons (PEPs) or those connected to high-risk jurisdictions should be required.

Transaction Monitoring: Continuous monitoring of transactions to detect suspicious patterns should be required and thresholds for automatic reporting or blocking of unusually large or rapid transactions should be implemented.

Record-Keeping and Reporting: Detailed records of all transactions should be maintained for a prescribed period, usually 5-7 years. There should exist an obligation to report suspicious activities to the relevant Financial Intelligence Unit (FIU) or other regulatory body.

Compliance Program: VRCA issues should be required to implement an AML/CTF compliance program, including policies, procedures, controls, and a designated Compliance Officer. Regular independent audits should be conducted to ensure the effectiveness of the program.

Cooperation with Law Enforcement: Issuers should be required to comply with lawful requests from law enforcement agencies, and a provision for international cooperation and information sharing with other jurisdictions to combat cross-border crime should exist.

Sanctions Compliance: Processes should exist to ensure adherence to international sanctions regimes, including screening customers and transactions against sanctions lists.

f. Financial Stability and Stress Testing

Financial Stability Measures

Capital Requirements: Minimum capital thresholds should be established that issuers must maintain to ensure solvency and absorb losses. Risk-weighted assets to align capital requirements with the specific risks of different commodity-referenced crypto assets should be incorporated.

Liquidity Management: Rules should be implemented to maintain sufficient liquidity to meet redemption requests and other obligations. Requirements for regular reporting on liquidity ratios, stress tests, and holding high-quality liquid assets should be adhered to.

Concentration Risk Controls: Over-exposure to single asset classes, counterparties, or geographic regions should be limited, and regularly monitoring and reporting concentration risks to prevent systemic vulnerabilities should be required.

Systemic Risk Oversight: Coordination with other regulators and central banks to monitor and address potential systemic risks from commodity-referenced crypto assets should be encouraged. Macroprudential measures should be adhered to when necessary to mitigate widespread threats to financial stability.

Stress Testing

Stress Testing Framework: VRCAs should develop and implement periodic comprehensive stress tests to evaluate the resilience of commodity-referenced crypto assets under various adverse scenarios. These scenarios may include extreme but plausible market conditions, significant changes in commodity prices, sudden liquidity shocks, regulatory changes, and more.

Disclosure of Stress Testing Results: Transparency in sharing stress testing methodologies, assumptions, results, and remedial actions with regulators should be required. Selective public disclosure to promote market confidence without revealing sensitive information should also be explored.

Remedial Actions and Contingency Planning: Clear guidelines and timelines for taking corrective actions in response to stress test results, including capital replenishment, risk reduction, or other operational adjustments should be established. Robust contingency plans should be developed to ensure continued operation during extreme stress conditions, including predefined triggers, responses, and communication strategies.

Ongoing Review and Improvement: VRCA issuers should be subject to regular review and updating of stress testing methodologies and scenarios to keep them relevant and effective. They should be expected to incorporate lessons learned from actual stress events, regulatory feedback, and industry best practices.

2.3 VRCA Type: **Algorithmic Value-Referenced Crypto Assets (Algorithmic Stablecoins)**

Definition:

Algorithmic-referenced crypto assets are a subset of VRCAs that use programmable rules and self-executing protocols to maintain a stable value. There tend to be no assets held in reserve and instead algorithmic-referenced crypto assets rely on a price stabilizing algorithm to maintain their peg to the external reference asset. This typically involves a smart contract that expands or contracts the VRCA supply in response to changes in demand, aiming to realign the price with the intended value. These types of VRCAs may be further classified into:

Cryptocurrency-collateralized algorithmic-referenced cryptoassets, also known as crypto collateralized algorithmic VRCAs and include MakerDAO (DAI), Liquity (LUSD), RAI Reflex Index (RAI), Celo Dollar (cUSD), TerraUSD (UST) and others.

These VRCAs are designed to maintain a relatively stable value through a combination of algorithmic mechanisms and collateralization using other cryptocurrencies. Unlike traditional VRCAs which are typically backed by external assets like fiat currency, cryptocurrency-collateralized algorithmic-referenced cryptoassets derive their stability from the interplay between algorithmic protocols and cryptocurrency holdings.

The term "cryptocurrency-collateralized" highlights the reliance on underlying cryptocurrencies held as collateral, forming a reserve that supports the value stability of the VRCA. Algorithmic mechanisms embedded within VRCA determine the supply of tokens in response to market demand, dynamically adjusting to fluctuations to ensure adherence to a target value.

These types of VRCAs present a unique fusion of algorithmic innovation and cryptocurrency collateralization, offering potential benefits such as reduced volatility, increased transaction efficiency, and broader accessibility to decentralized financial networks. The combination of these elements contributes to the stability of cryptocurrency-collateralized algorithmic-referenced crypto assets and their potential to serve as a reliable medium of exchange and store of value in the evolving digital financial ecosystem.

Rebasing algorithmic-referenced cryptoassets, also known as rebase style algorithmic VRCAs and include Ampleforth (AMPL) and others.

Rebasing algorithmic-referenced crypto assets utilize a unique mechanism called "rebasing" to adjust their total supply periodically based on predetermined conditions, aiming to achieve and maintain a stable value in relation to a specific reference, such as a fiat currency or a cryptocurrency.

The term "rebasing" refers to the process of altering the token supply by proportionally increasing or decreasing the balances held by token holders. This adjustment is typically triggered when the token's value deviates from its target reference value. For instance, if the token's price rises above the target, a rebase might reduce each holder's balance, effectively lowering the token's value. Conversely, if the token's price falls below the target, a rebase could increase each holder's balance, thereby raising the token's value.

Rebasing algorithmic-referenced cryptoassets aim to maintain a stable purchasing power over time by adjusting the supply dynamically. This approach offers potential advantages such as reduced volatility, enhanced price stability, and adaptability to changing market conditions. However, it also introduces complexities in understanding and managing the token's value, as the rebasing mechanism influences the number of tokens each holder possesses.

Seigniorage algorithmic-referenced cryptoassets, also known as seigniorage style algorithmic stablecoins and include Basis Cash (BAC) and others.

These VRCAs commonly involve a dual-token structure: the VRCA itself and an accompanying free-floating cryptocurrency. The latter serves to counterbalance price volatility associated with the VRCA, enabling users to capitalize on arbitrage opportunities. Consequently, users retain the ability to consistently purchase or sell the VRCA at its intended value, transacting through the intermediary of the second token.

Fractional algorithmic-referenced crypto assets, also known as fractional style algorithmic stablecoins and include Frax Finance (FRAX) and others.

Fractional algorithmic-referenced crypto assets are designed to maintain a stable value through algorithmic mechanisms while also incorporating a fractional reserve system. Unlike fully collateralized VRCAs, which are backed by a 1:1 ratio of reserves, fractional algorithmic-referenced crypto assets maintain a reserve that is a fraction of the total token supply.

In this context, "fractional" signifies that only a portion of the total supply is backed by collateral or reserves, while the remainder is generated algorithmically. The algorithmic mechanisms are responsible for expanding or contracting the token supply to maintain a stable value based on market demand.

Fractional algorithmic-referenced crypto assets aim to strike a balance between collateralization and algorithmic control, offering potential advantages such as scalability, reduced risk exposure, and efficient utilization of resources. This hybrid approach combines the benefits of both collateralized and algorithmic stability mechanisms, contributing to the broader spectrum of VRCAs in the digital financial ecosystem.

Utility:

Algorithmic-referenced crypto assets represent a disruptive innovation within the VRCA landscape, offering several compelling efficiency gains that distinguish them from traditional VRCAs and other forms of digital assets. These efficiency gains stem from their unique design and reliance on algorithmic mechanisms for maintaining value stability.

Real-Time Value Adjustment

The real-time adjustment mechanism of algorithmic-referenced crypto assets reduces the need for constant intervention by central authorities, ensuring that the VRCA's value remains close to its intended peg without manual interventions.

Reduced Volatility

Algorithmic-referenced cryptoassets aim to minimize price volatility, making them attractive for users seeking a stable store of value or medium of exchange. If successful, this stability can encourage increased adoption by merchants, businesses, and consumers for everyday transactions, fostering broader acceptance of digital currencies and modernization of financial infrastructure.

Lower Counterparty Risk

Traditional VRCAs may carry counterparty risk due to reliance on external reserves held by custodians or banks. Algorithmic-referenced cryptoassets mitigate this risk by relying on programmable mechanisms that don't require direct backing by external assets. This can enhance user confidence and reduce concerns about the stability of the issuer.

Innovation Potential

Algorithmic-referenced cryptoassets encourage innovation in financial technology by exploring new ways to achieve value stability. This innovation extends beyond VRCA technology itself and can influence the broader blockchain and cryptocurrency ecosystem, fostering novel use cases and applications. The efficiency gains offered by algorithmic-referenced cryptoassets are multifaceted, transforming the way we perceive and engage with digital financial instruments.

Illustrative Innovation Use Case: DAI by MakerDAO

In illustrating an innovation use case within the algorithmic-referenced cryptoasset landscape, we analyze DAI, an algorithmic-referenced cryptoasset issued by MakerDAO. This instance serves to provide regulators with a tangible example to contemplate when discussing the sandbox approach for algorithmic-referenced cryptoassets and stands as a prominent example that warrants a nuanced regulatory approach.

Understanding the Issuer: DAI is generated through an intricate decentralized smart contract system overseen by the MakerDAO community. The issuance of DAI relies on an algorithmic process and maintains itself through collateralization, predominantly utilizing Ether (ETH) locked within the system. It is paramount to acknowledge that DAI's issuance is orchestrated by a network of autonomous smart contracts rather than a central issuing authority.

Ecosystem Participants and Trading Dynamics: DAI finds its trading ground across both decentralized and centralized exchanges. Ecosystem participants encompass independent users, traders, and investors, all forming part of an intricate web of activity. The DAI ecosystem is constituted by an array of stakeholders who interact with the VRCA to facilitate diversified functionalities such as value preservation, lending, borrowing, and trading.

Decentralized Governance: The decentralized issuance and management framework of DAI, under the MakerDAO community's consensus, signifies a departure from conventional security issuance models. Regulators are encouraged to acknowledge the decentralized nature of the issuance process in their considerations.

Participant Landscape: While the participants in DAI trading and utilization may not necessarily warrant a securities-focused lens, regulatory contemplation could gravitate towards transparency, user safeguarding, and adherence to regulatory norms within the ecosystem.

Smart Contract Integrity: Given the reliance on smart contracts for DAI operations, a spotlight on smart contract security audits and adherence to best practices becomes an imperative facet of regulatory discourse.

Innovation-Friendly Framework: The proposed regulatory framework should provide an environment that fosters innovation and responsible experimentation while remaining steadfast in its commitment to user protection, market integrity, and a resilient financial ecosystem.

The DAI case furnishes a pertinent vantage point into the evolution of VRCA issuance and trading through decentralized smart contracts. By acknowledging the unique attributes of algorithmic-referenced cryptoassets like DAI, regulators can adeptly distinguish between the inherent nature of the VRCA, the decentralized network framework, and the diverse participants involved. An equitable equilibrium between nurturing innovation and upholding the tenets of regulatory oversight is pivotal in shaping a framework that aptly addresses the intricate dimensions of algorithmic-referenced cryptoassets.

a. Authorization and Licensing

Specific Regulatory Context:

A sandbox approach provides a controlled environment where new and innovative financial technologies can be tested and refined under regulatory oversight. This approach is especially relevant when dealing with novel financial instruments like algorithmic VRCAs, as it allows for iterative development and congruent risk assessment without stifling innovation. The following key elements outline the proposed sandbox framework for algorithmic VRCAs:

1. **Voluntary Participation:** Participation in the sandbox would be entirely voluntary for algorithmic VRCA projects. Interested projects would need to apply for entry and meet certain eligibility criteria, including clear documentation of their algorithmic mechanisms, cybersecurity measures, and commitment to compliance.

2. **Limited Duration:** The sandbox program would have a predetermined limited duration with clear exit guidelines, determined by the relevant regulatory body on a case-by-case basis. Following the expiry of the specified sandbox period, it would be generally expected that the licensee would either have to apply for the next tier of licensing or cease carrying on business, although the relevant regulatory body would have the discretion to extend the specified period.

3. **Phased Launch:** Projects in the sandbox would be launched over a phased period, allowing for gradual testing and adjustment of their algorithmic mechanisms. This measured approach would help to detect and address issues before full-scale deployment.

4. **Tiered Regulatory Oversight:** The sandbox framework would establish multiple tiers of regulatory oversight based on the project's stage of development, scale, and potential risks. Less mature projects with limited user bases would operate under lighter regulatory constraints, while more mature projects with significant user adoption would be subject to stricter rules. This approach would enable issuers to proactively engage with regulatory authorities as well as academics to communicate their intentions, share details about their mechanisms and seek feedback. Collaboration would promote mutual understanding and responsible innovation.

5. **Consumer Protection:** Robust consumer protection measures would be a central component of the sandbox. Algorithmic VRCA projects would be required to provide clear and understandable disclosures to users, outlining the risks associated with the volatility of the VRCA's value and the underlying algorithmic mechanisms.

6. **Regular Reporting and Audits:** Participants in the sandbox would be required to provide regular reports on their operations, financial health, and algorithmic stability.

Independent audits would also be mandated to verify the stability mechanisms and ensure compliance with the disclosed algorithms.

7. **Collaboration and Information Sharing:** Regulatory authorities, participants, and stakeholders would engage in ongoing dialogue to share insights, address challenges, and identify potential regulatory gaps or issues that might arise during the sandbox period.

The proposed sandbox approach for algorithmic VRCAs strikes a balance between encouraging innovation and safeguarding financial stability and consumer protection. By offering a controlled testing environment under regulatory supervision, this framework allows for the exploration and development of algorithmic VRCAs while minimizing potential risks to the Canadian financial system. As the cryptocurrency landscape evolves, it is imperative that regulatory authorities remain adaptable and open to new technological paradigms, fostering an environment where responsible innovation can flourish.

Supervision:

Continuous supervision is vital to ensure the ongoing compliance and stability of VRCA arrangements. Regulatory authorities should have the power to impose corrective measures when necessary to address any potential risks or breaches. An enforced cooperative environment between entities and supervisory authorities fosters information exchange and understanding, enhancing the overall regulatory effectiveness.

b. Reserve and Collateral Requirements

Algorithmic-referenced crypto assets are distinguished from other types of value-referenced crypto assets by the fact that they are not backed by reserves of tangible assets such as fiat currency or commodities. Instead, they utilize algorithms, smart contracts, and sometimes other crypto assets to maintain their value and stability. This structure eliminates the need for custodial management of physical or fiat reserves but introduces different risks and regulatory considerations.

Algorithmic Management

These crypto assets rely on algorithms and smart contracts to automatically adjust the supply and demand to maintain its peg to a specific value. Regulatory frameworks may require that the algorithms and smart contracts undergo rigorous testing, audits, and continuous monitoring to ensure that they function as intended without manipulation or vulnerabilities.

Collateral in Other Crypto Assets

Some algorithmic-referenced crypto assets may use other crypto assets as collateral, holding them in a decentralized manner. If other volatile crypto assets are used as collateral, regulators

may require additional risk management practices to account for potential price volatility, including diversified collateral portfolios, margin requirements, and regular stress testing.

Transparency and Disclosure

Given the non-traditional nature of reserves in algorithmic-referenced crypto assets, regulators may emphasize the need for transparent disclosure of the algorithms, smart contracts, and any collateral assets. Regulatory frameworks could require standardized reporting and public disclosure to enable users to understand the underlying mechanisms maintaining the value of the crypto asset.

c. Governance and Risk Management

Stability Risk

Principles for algorithmic mechanisms and stability

1. Algorithm Transparency: Algorithmic-referenced cryptoassets should provide comprehensive documentation detailing the operation of their algorithms. This transparency allows users and regulators to understand how the VRCA's value stability is achieved and maintained.

2. Predictability and Consistency: Algorithmic mechanisms should be designed to ensure predictability and consistency in maintaining the algorithmic-referenced crypto assets value over time. Users should have confidence that the VRCA will remain close to its intended value under varying market conditions.

3. Market Responsiveness: Algorithmic-referenced crypto assets should include mechanisms that respond effectively to changes in demand. These mechanisms should be designed to expand or contract the algorithmic-referenced cryptoassets supply in a timely manner to mitigate price volatility.

4. Public Accountability: Algorithmic-referenced crypto assets projects should provide regular public updates on the performance of their algorithms, adherence to principles, and any changes made to their mechanisms.

Governance Models

The governance of algorithmic-referenced crypto assets plays a critical role in ensuring their stability, security, and long-term viability. Given the diverse nature of algorithmic-referenced crypto assets and the various governance models they may adopt, it is essential to establish a framework that addresses the unique challenges and opportunities associated with each model. All algorithmic-referenced crypto asset projects must provide a detailed description of the governance arrangements

Approaches to Different Governance Models:

Transparent Governance Structures: algorithmic-referenced crypto asset projects should define and communicate their governance structures transparently. This includes outlining decision-making processes, roles, responsibilities, and the mechanisms through which stakeholders can participate.

Multi-Signature Approvals: For algorithmic-referenced crypto assets governed by a small group of entities or individuals, multi-signature approvals can enhance security and prevent unilateral decision-making. This approach involves requiring a predefined number of signatures for decisions to be executed.

Dynamic Parameter Adjustments: Algorithmic-referenced cryptoassets often involve adjustable parameters to fine-tune their algorithms. Governance mechanisms should allow for gradual parameter adjustments based on consensus, avoiding sudden or disruptive changes that could impact stability.

Community Feedback and Proposals: Algorithmic-referenced crypto assets projects should be encouraged to establish channels for community feedback and proposals. Transparent forums can foster open dialogue, allowing participants to share insights, concerns, and potential improvements.

Auditing and Reporting: Governance models should incorporate regular auditing of algorithms, mechanisms, and financial health. Transparent reporting enhances accountability and provides stakeholders with insights into the VRCA's performance.

Risk Assessment and Mitigation: Governance models should address risk assessment and mitigation strategies, especially in scenarios of extreme market conditions. Mechanisms to trigger emergency actions or parameter adjustments can help manage risks effectively.

Flexibility and Evolution: Algorithmic-referenced crypto asset projects should design governance models with flexibility to evolve as the project matures. Adaptability is critical for responsiveness to changing market dynamics, user needs and technological developments. New governance models should be tested in controlled environments before full implementation.

Data Risk Management

Data risk management is a crucial aspect of ensuring the stability, security, and trustworthiness of algorithmic-referenced crypto asset. As algorithmic-referenced crypto asset rely on real-time data feeds and computational processes, it is essential to address potential vulnerabilities related to data accuracy, integrity, and privacy to maintain the stability of the VRCA and protect

users' interests. A description of the systems, processes and procedures in place to safeguard the availability, authenticity, integrity and confidentiality of data.

Data Source Verification: algorithmic-referenced crypto asset projects should establish robust procedures to verify the accuracy and reliability of the data sources used to inform algorithmic mechanisms. Collaborating with reputable data providers and implementing data validation mechanisms can minimize the risk of erroneous data impacting the stablecoin's stability.

Data Integrity Measures: Cryptographic techniques, such as digital signatures and hash functions should be employed at every stage of processing to ensure the integrity of data. This prevents unauthorized data tampering that could compromise the accurate functioning of the algorithmic mechanisms.

Oracles and Feeds: Algorithmic-referenced crypto assets rely on oracles to fetch external data for decision-making. Projects should implement a decentralized oracle infrastructure, ensure transparency in oracle selection, and utilize multiple trusted oracles to mitigate the impact of potentially compromised data sources.

Real-time Monitoring: Data sources and algorithmic processes should be continuously monitored in real time to detect any anomalies or discrepancies. Swift responses to data irregularities will prevent disruptions in stablecoin stability.

Privacy and Security Measures: Stringent security protocols must be implemented to protect sensitive data from unauthorized access. Encryption and access controls must be used to safeguard data throughout its lifecycle.

Data Transparency: Users and stakeholders must be provided with visibility into the data sources, calculation methodologies, and parameters used in the algorithmic-referenced cryptoasset's operation.

Redundancy and Fail-Safe Mechanisms: Redundancy must be designed into the data feeds and algorithmic mechanisms to ensure stability even if certain data sources fail or are compromised.

External Auditing: Issues must engage third-party auditors to conduct regular reviews of data sourcing, processing, and risk mitigation strategies.

Data Governance Framework: A comprehensive data governance framework that outlines responsibilities, protocols, and procedures for managing data-related risks must be established. This framework should ensure compliance with relevant regulations and standards.

Counterparty Risk

While algorithmic-referenced crypto assets rely on algorithms and smart contracts to maintain their value, unique counterparty risks may arise from the dependence on various actors within

the ecosystem, including developers, users, and possibly other crypto assets. Theses risk may include:

Smart Contract and Developer Risk

Risk Profile: The failure or malicious actions of developers in designing or maintaining the smart contracts could lead to significant loss of value.

Mitigation: Regulatory oversight, code audits, and developer due diligence may mitigate these risks. Transparency regarding the development team's expertise, experience, and intentions can also provide users with insights into potential risks.

Network and Liquidity Risk: Dependence on liquidity providers and network participants may expose users to counterparty risk if these entities fail to meet obligations. Implementing robust liquidity provisions, closely monitoring participant behavior, and setting clear standards for network participation may address these risks.

User and Community Governance Risk Management

Nature: Some algorithmic-referenced crypto assets may rely on decentralized governance where users vote on key parameters. Incorrect or manipulative decision-making could impact stability.

Mitigation Strategies: Establishing clear governance guidelines, monitoring voting patterns, and implementing safeguards against manipulation could minimize these risks.

Dependency on Other Crypto Assets (if applicable): If the algorithm relies on other crypto assets as collateral or reference points, the failure or volatility of these assets may affect the stability of the algorithmic-referenced asset.

Mitigation Measures: Diversifying dependencies, setting limits on exposure, and closely monitoring the performance of related crypto assets can help manage this risk.

Risk Mitigation

Issuers of algorithmic-referenced crypto assets should conduct thorough risk assessments to identify potential vulnerabilities in their mechanisms. and provide a description of the internal control mechanisms and risk management procedures.

Regular Audits

Regular audits are essential to ensure transparency and accountability in VRCA arrangements. VRCA issuers should subject their operations, reserve management (if applicable), and financial reports to regular audits by independent auditors. These audits provide stakeholders with confidence in the VRCA's financial health and its adherence to regulatory requirements.

Smart Contract Vulnerabilities

Smart contracts are the cornerstone of algorithmic-referenced crypto assets, responsible for executing the complex instructions that maintain value stability. Ensuring the security of these smart contracts is paramount, as vulnerabilities can have far-reaching consequences that compromise the stability and user trust in the VRCA ecosystem.

Code & Mechanism Design Transparency: Algorithmic-referenced crypto asset projects should openly share details about code deployments and updates, whether that code is open source, how code contributions are reviewed, approved and/or denied, how many different individuals or organizations contribute and underlying mechanisms to ensure that users, stakeholders and regulators have visibility into how value stability is achieved.

Code Review and Audits: Algorithmic-referenced cryptoassets projects should undergo thorough code reviews and independent security audits by reputable third-party firms. These reviews identify potential vulnerabilities and coding errors, allowing for preemptive fixes.

Formal Verification: Formal methods to mathematically prove the correctness of smart contract code should be implemented to enhance confidence in the code's behavior and to reduce the likelihood of critical vulnerabilities.

Secure Coding Practices: Secure coding practices, such as input validation, access controls, and proper error handling must be employed to prevent common vulnerabilities like reentrancy attacks and integer overflows.

Penetration Testing: Penetration testing must be conducted to simulate real-world attack scenarios and identify potential weak points in the smart contract infrastructure.

Timely Updates and Patches: Updates and patches must be promptly applied to address known vulnerabilities.

Emergency Shutdown and Upgradability

Emergency Shutdown Mechanism: An emergency shutdown mechanism must be designed that can be activated in the event of critical vulnerabilities or unexpected circumstances to protect user funds and stability.

Upgradability Safeguards: If the smart contracts are upgradable, strict safeguards must be implemented to prevent unauthorized changes and maintain transparency about the upgrade process.

d. Consumer Protection and Disclosure

Transparency and Full Disclosure Regulations: Detailed requirements should exist for issuers to disclose all aspects of the commodity-referenced crypto assets, including potential risks, fee structures, and rights. Mandatory real-time reporting of relevant operational metrics and the use of third-party verification should be required. Public dashboards that display real-time data could enable anyone to verify stability mechanisms.

Consumer Education and Awareness Programs: There should be an expectation to implement educational campaigns to increase public awareness and understanding of commodity-referenced crypto assets. Guidelines should be established for providing clear, concise, and understandable educational materials.

Complaint Handling and Redress Mechanisms: Clear and accessible channels for consumer complaints and disputes should be established, and requirements for timely and fair resolution of disputes, possibly through an independent ombudsman service should be established.

Cybersecurity and Fraud Prevention: Rigorous standards for cybersecurity to protect consumer data and assets should exist and a framework for monitoring, detecting, and combating fraudulent activities should be developed.

Accessibility and Non-discriminatory Practices: VRCA projects should ensure equitable access to services related to commodity-referenced crypto assets, prohibit discriminatory practices and foster inclusion.

Whitepaper: A whitepaper is a comprehensive and structured document that delineates the foundational principles, technical architecture, economic mechanisms, and operational intricacies of a VRCA project. It serves as the primary informational source for stakeholders, investors, regulators, and the broader public, offering an authoritative elucidation of the VRCA's design, purpose, and envisaged impact on the financial ecosystem. The whitepaper outlines the VRCA's value proposition, underlying algorithmic or collateral mechanisms, governance structure, security protocols, and risk mitigation strategies. In doing so, it establishes a transparent framework that guides informed decision-making and regulatory considerations while promoting transparency, accountability, and responsible innovation in the domain of VRCAs.

A VRCA issuer must publish a white paper on its corporate website, to disclose information such as the description of the VRCA, rights and obligations of the VRCA issuer and VRCA holders, risks that can affect the stability of the VRCA value and ability of the VRCA issuer to fulfill its obligations etc, and update such information as needed.

e. Market Conduct and Anti-Money Laundering Measures

Regulatory Compliance

Governance models should ensure alignment with regulatory requirements and engage in proactive communication with regulatory authorities. This helps build credibility and minimizes legal and regulatory risks.

Compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations is essential for VRCA issuers to prevent illicit activities and enhance user protection.

VRCA issuers should have mechanisms in place to freeze assets in compliance with relevant regulations and policies. The challenges and limitations associated with these procedures should be carefully addressed.

Anti-Money Laundering (AML) and Financial Crime:

AML Compliance: Implement robust AML procedures to prevent, detect, and report potential money laundering activities. This could include customer due diligence (CDD) procedures, transaction monitoring systems, and suspicious activity reporting mechanisms.

Sanctions Compliance: Establish procedures to ensure compliance with economic and trade sanctions. This could include sanctions screening systems, sanctions risk assessments, and procedures for handling potential sanctions hits.

Fraud Prevention: Implement measures to prevent and detect fraudulent activities. This could include fraud detection systems, fraud risk assessments, and procedures for investigating and reporting suspected fraud.

Financial Crime Training: Provide regular training for staff on AML and financial crime risks and compliance. This could include training on recognizing and reporting suspicious activities, understanding sanctions requirements, and preventing and detecting fraud.

Financial Crime Risk Management: Develop a comprehensive financial crime risk management framework. This should include policies and procedures for managing AML, sanctions, and fraud risks, a designated officer responsible for financial crime risk management, and regular reviews and audits of the financial crime risk management framework.

f. Financial Stability and Stress Testing

Stress Testing: Stress testing and scenario analysis can help identify potential failure points and guide the implementation of protective measures.

Market Integrity

Mechanisms should prevent malicious activities, such as price manipulation or algorithmic exploits, that could undermine the VRCA's value stability. Clear safeguards should be established to maintain market integrity.

Market Volatility & Market Dependence

Algorithmic-referenced cryptoassets operate within dynamic and interconnected markets, influencing their stability and value. Acknowledging the potential for market volatility and dependency is crucial in crafting a comprehensive regulatory framework.

Market Stability Assumptions: Regulators should be cognizant of the stability assumptions underlying these VRCAs. These VRCAs often rely on arbitrage and market dynamics to maintain their peg. Therefore, the regulatory approach should ensure that market participants understand the mechanisms at play and that any assumptions align with real-world market behavior.

Market Operations: Transparency in market operations is essential. Algorithmic-referenced cryptoassets interact with various trading platforms and exchanges, necessitating clear guidelines on data accuracy, market surveillance, and coordinated efforts among crypto trading platforms to prevent potential manipulation.

Liquidity: A well-functioning algorithmic-referenced cryptoassets requires sufficient liquidity across markets. Regulatory discussions should explore mechanisms to promote healthy liquidity, deter market abuse, and prevent liquidity concentration risks.

Stress Testing and Methodology: A progressive regulatory approach could involve the publication of stress testing methodologies. Regulators can collaborate with industry stakeholders to define stress scenarios, conduct comprehensive tests, and disclose the results. This proactive measure helps assess the VRCA's resilience against extreme market conditions.

Backstops for Volatility & Price Stabilization Mechanism: Algorithmic-referenced cryptoassets should incorporate robust mechanisms to address unexpected market volatility. Regulators should work alongside projects to define contingency protocols, emergency interventions, or mechanisms that enable the system to stabilize itself during turbulent periods.

Peg and Depeg Parameters: Clearly defining the parameters for pegging and depegging is pivotal. Regulators should collaborate with VRCA projects to establish unambiguous rules governing these transitions, ensuring transparency, predictability, and maintaining user trust.

Appendix: Stablecoin Working Group

Canadian Blockchain Consortium Stablecoin Working Group Members:

First Name	Surname	Organization	Role
Matt	Burgoyne	Osler	Partner and Co-Chair, Digital Assets and Blockchain Group
Kunal	Bhasin	KPMG Canada	Partner and Co-Lead, Cryptoassets & Blockchain CoE
Dina	Mainville	Collisionless	Founder & President
Koleya	Karringten	Canadian Blockchain Consortium	Executive Director
Simon	Chantry	Bitt	CIO & Co-Founder
Alex	McDougall	Stablecorp	President & CEO
Jacob	Robinson	McCarthy Tétrault	Associate
Eric	Kryski	Bidali	CEO & Co-Founder
Josh	Klayman	Linklaters	Head of Blockchain & Digital Assets
Justin	Newton	Netki	CEO
Sheereen	Khan	ARMS	Principal Consultant
Wayne	Logan	Miller Thompson	Partner
John-David	D'Souza	Miller Thompson	Associate
Joe	Tosti	Kraken	CCO
Brad	Yassar	EQIFI	Founder & CEO
Alison	Manzer	Cassels	Partner
Kevin	Zhang	DFX Finance	Co-Founder
Aaron	Unterman	xReg Consulting	Managing Director
Chris	Housser	Independent	Head of Strategy
Lucas	Matheson	Coinbase	Canada Country Director
Chris	Zuehlke	DRW Cumberland	Global Head
Nathalie	Ngo	DRW Cumberland	Digital Assets Trading Business Development