

THE CANADIAN LAW REVIEW

QUARTERLY

ISSUE III

GENESIS

EMERGING AREAS OF LAW



ACKNOWLEDGEMENTS

This volume would not have been possible without the dedication and determination of our editorial team: Annika Pavlin-Jamal, Alysha Ahmad, Deeba Mehr, Chiara Puglielli, Anjalique Raghunauth, Mila Shull, Katie Timms, and Melani Vevečka.

A special thanks goes out to Nikhil Trehan for bringing life to this wonderful first volume of *Canadian Law Review Quarterly*.

MASTHEAD

EDITORS-IN-CHIEF

Damai Siallagan

Rachel Brouwer

COPYEDITOR

Annika Pavlin-Jamal

EDITORS

Alysha Ahmad

Deeba Mehr

Annika Pavlin-Jamal

Chiara Puglielli

Anjalique Raghunauth

Mila Shull

Katie Timms

Melani Vevečka

EDITOR'S NOTE

Dear readers,

We extend to you a sincere welcome to the third and concluding issue of the *Canadian Law Review Quarterly*, volume 1. Over the past year, the *Canadian Law Review Quarterly* has had the privilege to host ten authors and twelve editors animating a breadth of voices in diverse areas of legal advocacy. As we prepare to transition to our second volume, we would like to express our deepest gratitude for you, our readers, for your investment of interest in the future voices of Canadian law.

The theme of this issue is “Emerging Areas of Law.” Our editorial board curated two papers that demonstrated an awareness of the mutually-transformative relationship between law, society, and technology. Each paper venture beyond the well-established borders of legal precedent to boldly traverse uncertain and amorphous legal grounds. Both authors demonstrate a firm, global conception of legal transformations, illustrating with comparative examples how Canadian jurisprudence can benefit from a more international outlook. Though diverging in subject matter, the two papers present contrapuntal lines that, taken together, convey an insightful look into the legal issues that occupy tomorrow’s agenda.

Vic S. Maan inaugurates the issue with a review of the *Artificial Intelligence and Data Act* (AIDA), initially proposed under Bill C-27. Through a probing survey of legal literature and comparative legislative frameworks, Maan presents a bipartite proposal to render AIDA a more responsive and accountable mechanism for the governance of artificial intelligence systems.

Thomas Tudor-Doonan furnishes a thematic contrast expositing the legal underpinnings of Canada’s weak cryptocurrency climate. Tudor-Doonan extends his analytical reach into financial market prospects and economic behaviours, underscoring the importance of interdisciplinary approaches in legal analysis. He concludes with concise recommendations on regulatory amendments to improve Canada’s prospects in cryptocurrency markets.

It has been a pleasure to lead the first issue of the *Canadian Law Review Quarterly*. To our editors, authors, and all involved in making this volume a success: thank you. We are indebted to each and every one of you for showing the world what the next generation of legal advocates and activists offers.

Sincerely,

Damai Siallagan & Rachel Brouwer

Editors-in-Chief, *Canadian Law Review Quarterly*, 2024–2025

POSITIONALITY STATEMENT

Canadian Law Review Quarterly is a journal that primarily operates across Canada. Canadian law has historically been and continues to operate as a vehicle of oppression, violence, and dispossession toward those underrepresented in arenas of legislation and jurisprudence.

Our conviction is that law may also be an avenue toward an equitable future. We hope the *Canadian Law Review Quarterly* will help transform law by providing opportunities for emerging voices in legal advocacy to engage meaningfully with the issues of today. We see the diverse experiences and positionalities of our authors and editors as vital to our success as a journal.

TABLE OF CONTENTS

MAAN, Vic S

Amending AIDA: A Fight for Independence and Action	1
----------------------------------------------------	---

TUDOR-DOONAN, Thomas

Canada's Crypto Regulatory Crossroads: The Need for Legal Evolution in a Globalized Economy	18
---------------------------------------------------------------------------------------------	----

This page is intentionally left blank.

Canadian Law Review Quarterly
Volume 1 Issue 3
December 2025

AMENDING AIDA: A FIGHT FOR INDEPENDENCE AND ACTION

Vic S. Maan

ABSTRACT

The proliferation of artificial intelligence (AI) technologies has prompted significant legislative responses in jurisdictions such as the European Union and the United States. By contrast, Canada’s regulatory framework remains in a nascent stage. Central to Canada’s proposed AI governance regime is the *Artificial Intelligence and Data Act* (AIDA), initially contained within the federal Bill C-27. Although the introduction of AIDA marks a commendable first step toward statutory oversight of AI, it requires amendments to adequately address the complexities of contemporary AI use. This article proposes two amendments necessary to improve AIDA’s efficacy as a regulatory instrument. First, this article recommends the formation of an executive oversight board composed of lawyers, jurists, and tech experts rather than allocating sole regulatory authority to a single AI and Data Commissioner. Second, this article advocates for the inclusion of an explicit private right of action similar to the provision in AIDA’s supplementary statute to enable individuals to seek redress for harms resulting from AI-generated errors or malfunctions. Without such a mechanism, AIDA risks limiting recourse to administrative fines and regulatory sanctions, which may serve punitive or deterrent purposes, but fail to compensate affected individuals or rectify systemic harms. Taken together, decentralized governance and enforceable private remedies are essential to ensuring that AIDA develops into a responsive, accountable, and rights-protective framework capable of regulating the present and future impacts of AI in Canada.

Maan, Vic S, “Amending AIDA: A Fight for Independence and Action” (2025)
1:3 Can L Rev Q 1.

I. INTRODUCTION

In 2014, Elon Musk stated: “[I] think that there should be some regulatory oversight [of artificial intelligence], maybe at the national and international level, just to make sure that we don’t do something very foolish ... with artificial intelligence we’re summoning the demon.”¹ Nevertheless, Canada has enacted minimal legislation—federally or provincially—to address the proliferation of artificial intelligence (AI) across industries such as commerce, healthcare, education, finance, and daily life. The evolving use and potential misuse of AI in these sectors poses significant risks including threats to data privacy, cybersecurity, and information integrity. The development of Canadian common law has been equally slow with little reference to AI in current jurisprudence.²

This article examines Canada’s present framework for AI oversight, reviews legislative and policy proposals currently under consideration, and offers recommendations for future regulatory action. This article begins by discussing what steps Canada has taken toward regulating AI. It then presents a review of the *Artificial Intelligence and Data Act* (hereafter, “AIDA” or “the *Act*”) focusing on the powers it affords the Governor-in-Council (GIC), the Minister of Innovation, Science, and Industry (“the Minister”), and risk regulation.³ Lastly, this article proposes two amendments to AIDA: (1) forming an executive oversight board to ensure sufficient regulatory independence and accountability; and (2) enshrining an individual’s private right of action. These amendments will offer stronger protections for Canadians—individually and collectively—by limiting concentrated authority, empowering a coalition of experts, and codifying redress mechanisms.

¹ Samuel Gibbs, “Elon Musk: Artificial Intelligence Is Our Biggest Existential Threat” (27 Oct 2014) online: <[theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat](https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat)>.

² Florian Martin-Bariteau & Teresa Scassa, *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2023) at 6; see also Mike Zajko, “Canada Is Failing to Regulate AI Amid Fear and Hype” (13 Jan 2023), online: <policyoptions.irpp.org/2023/06/canada-failing-ai-regulation-fear-hype/>; Channarong Intahchomphoo et al, “References to Artificial Intelligence in Canada’s Court Cases” (2020) 20:1 Leg Info Mgmt 39 at 4, DOI: <10.1017/S1472669620000080>.

³ Bill C-27, *An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts*, 1st Sess, 44th Parl, 2021, online: <parl.ca/legisinfo/en/bill/44-1/c-27> [AIDA].

II. CANADA: SOFT LAWS & LITIGATION

a. Killing Laws Softly

Canada has been slow to respond to the expansion of AI innovation and commercial use through either legislation or litigation. Both federal and provincial regulation on AI design, development, and deployment has been limited to non-binding frameworks issued by powerless governmental, quasi-governmental, public, and private organizations. As Canadian Professors Florian Martin-Bariteau and Teresa Scassa describe, these “soft laws” are a series of codes, standards, statements, and programs, among other things, that are “rarely (if ever) operationalized or made mandatory.”⁴ Examples include the Federal Court of Canada’s (FCC) “Interim Principles and Guidelines on the Court’s Use of Artificial Intelligence” (PGCUAI) which governs the court’s use of AI technology as well as its “Notice to the Parties and Profession” issued in May 2024 (the “FCC Notice”).⁵ In brief, the PGCUAI suggests that the FCC is committed to refraining from AI use, namely automated decision-making tools, in its judgments and orders without first conducting public consultations. It has also pledged to adhere to established principles in any internal application of AI and to engage relevant stakeholders before deploying AI for specific purposes.⁶ Likewise, the FCC Notice requires that counsel or parties appearing before the FCC declare when “content [is] created or generated directly by AI” and the “role AI plays in the preparation of materials for the purpose of litigation [when it] resembles that of a co-author.”⁷ In other words, the FCC has implemented loose rules restricting AI use within the Court except in specific circumstances and requiring counsel, among others, to disclose when it is used to prepare submissions. The specific circumstances referred to by the FCC and to what extent disclosure is required remains undetermined and undefined. These principles, guidelines, and requirements are restrictive in scope as they apply solely to the FCC. Furthermore, it is yet to be

⁴ Martin-Bariteau & Scassa, *supra* note 2 at 7–8. For a list of initiatives taken by independent organizations or federal government institutions, see Blair Attard-Frost, Ana Brandusescu & Kelly Lyons, “The Governance of AI in Canada: Findings and Opportunities From a Review of 84 AI Governance Initiatives” (2024) 41:2 Government Information Q 101929 at 5, DOI: <10.1016/j.giq.2024.101929>.

⁵ Federal Court of Canada, *Interim Principles and Guidelines on the Court’s Use of Artificial Intelligence* (Ottawa: Federal Court of Canada, 2023), online: <fct-cf.ca/en/pages/law-and-practice/artificial-intelligence>; see also Paul S Crampton, *Notice to the Parties and Profession: The Use of Artificial Intelligence in Court Proceedings* (Ottawa: Federal Court of Canada, 2024), online: <fct-cf.ca/Content/assets/pdf/base/FC-Updated-AI-Notice-EN.pdf>.

⁶ Federal Court of Canada, *supra* note 5 at 1.

⁷ Crampton, *supra* note 5.

seen whether violating these rules will result in any form of discipline or recompense by the FCC.

Despite these limitations, government-funded programs are the favoured approach by regulatory bodies towards federal and provincial AI policy, while comprehensive legislation and overarching regulation take a back seat.⁸ Although the government has introduced statute—such as Canada’s Privacy Commissioner making recommendations to amend the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Bill C-11, and Bill C-27—none of these policy initiatives have come into effect.⁹ As Martin-Bariteau and Scassa argue, Canada requires “hard laws [such as] regulation and clear legal principles” to ensure effective oversight and enforcement of AI technologies.¹⁰ Until such legislation is enacted, Canada’s AI policy framework will continue to rely on soft and meretricious policies or ill-equipped legislation such as PIPEDA and the *Charter*.¹¹

b. A Time to Litigate

Canadian common law has yet to meaningfully engage with the legal complexities of AI. Although the courts have issued decisions involving AI, the jurisprudence is narrow and restrictive. Notable examples include legal research and lawyer billings, monitoring remote university examinations, and access to ministry records.¹² With few cases reaching the courts, the pace of incremental legal development has been relatively stagnant. However, AI litigation has recently gained some traction with lawsuits filed across various Canadian jurisdictions in 2024.¹³ Two such cases involve “data scraping,” a process in which a computer

⁸ Attard-Frostt, Brandusescu & Lyons, *supra* note 4 at 6–7.

⁹ See Teresa Scassa, “Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act” (2023) 101:1 Can Bar Rev 1 at 3; Martin-Bariteau & Scassa, *supra* note 2 at 10; Attard-Frostt, Brandusescu & Lyons, *supra* note 4 at 7; see also Bill C-11, *An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to Make Consequential and Related Amendments to Other Acts*, 2nd Sess, 43rd Parl, 2020 (first reading 17 November 2020), online: <parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading> [perma.cc/5N3E-UWGW].

¹⁰ Martin-Bariteau & Scassa, *supra* note 2 at 10.

¹¹ *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11; see also Martin-Bariteau & Scassa, *supra* note 2 at 372.

¹² Intahchomphoo et al, *supra* note 2; *Drummond v The Cadillac Fairview Corp Ltd*, 2018 ONSC 5350; *McMaster University (Re)*, 2024 CanLII 17583 (ON IPC); *Ontario (Finance) (Re)*, 2017 CanLII 143361.

¹³ Matina Stevis-Gridneff, “Major Canadian News Outlets Sue OpenAI in New Copyright Case” *New York Times* (29 November 2024), online: <bbc.com/news/articles/cm27247j6gno>; Jessica

program extracts information from content designed for human users. In these matters, AI-powered tools are alleged to have extracted data from third-party sources, including local and national news outlets as well as CanLII, and repurposed the information for commercial use and profit.¹⁴ In the CanLII case, a technology company developed AI software intended to transform legal practice by streamlining research and drafting. At present, these cases are framed under copyright law, in part due to relevance and in part because Canada lacks comprehensive legislation addressing civil liability for AI-related governance, protection, and/or infringements. Legislation is therefore imperative to clarify legal responsibilities and improve access to justice for both corporations and consumers.

III. THE *ARTIFICIAL INTELLIGENCE AND DATA ACT*

a. Artificial Intelligence

AIDA represents the federal government's first comprehensive attempt to regulate "high-impact"¹⁵ AI systems, i.e., technologies that have a significant effect on individuals' rights, safety, or socio-economic well-being, focusing on design, development, and deployment. Its objective is to mitigate the risk of harmful outcomes, such as algorithmic bias, that may adversely affect Canadians.¹⁶ AIDA is designed to prevent or reduce harm rather than to provide redress or compensation, grounded in what academics describe as "risk regulation."¹⁷ It is framed as an "agile" legislative instrument, intended to adapt to ever-evolving provincial and federal frameworks as well as ongoing technological developments.¹⁸ Rather than an independent commissioner or regulatory body, the

Mach, "CanLII Sues AI Legal Assistant CasewayAI for Copyright Infringement" *Canadian Lawyer Mag* (7 Nov 2024), online: <canadianlawyermag.com/resources/legal-technology/canlii-sues-ai-legal-assistant-caseway-ai-for-copyright-infringement>; Anja Karadeglija, "Can AI Be an Author? Federal Court Asked to Decide New Copyright Case" *CTV News* (13 Jul 2024), online: <ctvnews.ca/sci-tech/article/can-ai-be-an-author-federal-court-asked-to-decide-in-new-copyright-case>.

¹⁴ Stevis-Gridneff, *supra* note 13; Mach, *supra* note 13.

¹⁵ "High-impact" remains undefined by the *Act*.

¹⁶ Maggie Arai, "Five Things to Know About Bill C-27" (18 October 2022), online: <srinstitute.utoronto.ca/news/five-things-to-know-about-bill-c-27>; Amaya Arancibia-Albornoz, "Concerns in the Age of Intelligence: Shaping Regulatory Frameworks for AI in Canada" (2023/24) 14 *Queen's Pol'y Rev* 147 at 175; AIDA, *supra* note 3, ss 4–5, 7–9, 11–12, 14, 17.

¹⁷ Scassa, *supra* note 9 at 4, 15; Arai, *supra* note 16.

¹⁸ The Preamble to Bill C-27 states: "Whereas organizations of all sizes operate in the digital and data-driven economy and an agile regulatory framework is necessary to facilitate compliance with

Act grants broad regulatory powers to the GIC and the Minister.¹⁹ These powers extend to governing high-impact systems and establishing notice requirements, disclosure requirements, and defining what may constitute “material harm” resulting from high-impact AI systems.²⁰ Finally, the proposed statute imposes legal obligations regarding “the use of anonymized data in AI systems; the design, development and making available for use of AI systems; and the design, development and making available for use of high-impact AI systems.”²¹

b. Risky Business (Regulation, Accountability & Enforceability)

American jurist Margaret Kaminski argues that any AI policy ought to include risk regulation akin to that in effect in the EU and the US. Kaminski observes that risk regulation is typically administered by specialized regulatory bodies rather than through judicial processes. Risk regulation focuses on promoting societal benefits while minimizing collective harms rather than offering remedies to individual claimants. This approach is forward-looking, aiming to guide the development and application of technology in real time.²² Put simply, risk regulation supports innovation by anticipating and mitigating harm through continuous, expert oversight administered by independent bodies equipped to respond to emerging risks. In reviewing the provisions of the *Act*, AIDA adopts this normative approach emphasizing proactive safeguards over reactive remedies.²³ For example, AIDA mandates a minimum degree of accountability for parties using AI for commercial purposes and places sanctions on clandestine cooperation therein.²⁴ Section 5 of the *Act* states that, “a person is responsible for an [AI] system, including a high-impact system, if, in the course of ... trade and commerce, they design, develop or make available for use the [AI] system or manage its operation.”²⁵ Under this statute, a “person” includes “a trust, a joint venture, a partnership, an unincorporated association and any other legal entity.”²⁶

rules by, and promote innovation within, those organizations.” See Scassa, *supra* note 9 at 5–11; see also Arai, *supra* note 16.

¹⁹ Scassa, *supra* note 9 at 5–7, 11.

²⁰ *Ibid* at 8; *Canadian Charter of Rights and Freedoms*, *supra* note 11.

²¹ Scassa, *supra* note 9 at 4.

²² Kaminski, Margaret E, “The Developing Law of AI: A Turn to Risk Regulation” (2023) Digital Soc Contract: Lawfare Paper Series 24 at 2, DOI: <10.2139/ssrn.4692562>.

²³ Scassa, *supra* note 9 at 20.

²⁴ Arancibia-Albornoz, *supra* note 16 at 156.

²⁵ AIDA, *supra* note 3, s 5(2).

²⁶ *Ibid* at s 2.

On this basis, a person or alternative legal entity may be held accountable for the actions taken by AI systems under their oversight. Once accountability is established, AIDA's enforcement mechanisms outline possible administrative monetary penalties as well as offences whether regulatory or criminal.²⁷ As Arancibia-Albornoz writes:

[A] regulatory order would be that of an independent audit or cessation of the use of a system. In contrast, a regulatory offence would occur in more serious circumstances of non-compliance with the obligations set out in the document and carry certain penalties, such as monetary fines. A criminal offence, as outlined in the *Criminal Code* occurs when the accused knowingly or intentionally engages in the design, development, or deployment of a harmful AI system and does not take reasonable measures to prevent it.²⁸

The penalties under AIDA are substantial, ranging from “not more than \$50,000 in the case of an individual” to “not more than the greater of \$10,000,000 and 3% of the person's gross global revenues in its financial year [for corporations]” as well as the potential of criminal prosecution.²⁹ Serious concerns remain, however, chief among them, who will be held accountable for AI-related harms and which authority will enforce such consequences.

IV. AMENDING AIDA

a. AIDA

Rather than attempting to provide an exhaustive list of limitations, this section focuses on the most pressing deficiencies of AIDA. Journalists have criticized AIDA as undemocratic, overly individualistic, failing to account for harms to the collective or the environment, and a work in progress with relatively little enforceable language.³⁰ These concerns stem from the fact that AIDA was drafted with minimal public consultation, effectively bypassing democratic input. It lacks

²⁷ *Ibid* at ss 29, 30, 38; see also Arancibia-Albornoz, *supra* note 16 at 156.

²⁸ Arancibia-Albornoz, *supra* note 16 at 156.

²⁹ AIDA, *supra* note 3, ss 30(3)(a)(i), 30(3)(b)(ii), 38.

³⁰ Zajko, *supra* note 2; see also Bianca Wylie, “ISED's Bill C-27 + AIDA” (22 April 2023), online: <[hbiancawylie.medium.com/iseds-bill-c-27-aida-part-9-my-remarks-to-indu-committee-re-aida-december-7-2023-38b06f3294be](https://biancawylie.medium.com/iseds-bill-c-27-aida-part-9-my-remarks-to-indu-committee-re-aida-december-7-2023-38b06f3294be)>; AIDA, *supra* note 3, s 5(1); Joe Castaldo, “How Will Canada Regulate AI? Ottawa Will Figure It Out Later” *Globe and Mail* (17 April 2023), online: <theglobeandmail.com/business/article-canada-ai-regulation-bill>.

provisions addressing the potential harm AI may pose to critical infrastructure or the environment. Because the *Act*'s language is designed to accommodate future technological developments, it provides insufficient safeguards to ensure present-day accountability.³¹ Scholars have expressed more pointed concerns with the legislation's governance structure. For instance, the *Act* centralizes authority over AI governance in the position of an "AI Czar" (the GIC or the Minister), thereby limiting the *Act*'s independence and insulating key decisions from broader institutional oversight.³² As such, this article contends that AIDA requires amendments to better protect individuals' rights, access to justice, and to establish a more robust and autonomous regulatory framework.

b. Independence Day (from Ministerial Oversight)

Scholarship suggests that AIDA requires reform to establish an autonomous and more comprehensive legal framework. Scassa argues that AIDA is not as agile as it claims to be, particularly due to its lack of independent oversight. As noted, the *Act* vests excessive authority in the hands of the GIC or Minister, raising concerns about the concentration of oversight and enforcement powers in a single office effectively creating an AI Czar. As Scassa explains:

[AIDA] sets up the Minister as the actor responsible for oversight and enforcement, but the Minister may delegate any or all of his or her oversight powers to a new Artificial Intelligence and Data Commissioner ... over which the Minister presides. ... [While] AIDA provides for the creation of an advisory committee that will offer the Minister advice ... [it] is the Minister who may choose to publish advice he or she receives from the committee on a publicly available website.³³

This arrangement raises fundamental concerns about the independence and effectiveness of AI governance in Canada. By concentrating authority in the hands of the Minister—and by extension, in the hands of any subordinate to whom the Minister delegates oversight powers—AIDA undermines its own risk regulation framework. The *Act* purports to adopt a risk-based approach to AI governance, which requires nuanced and expert oversight to assess and mitigate potential harms. However, vesting discretion in a political office undermines this goal by shifting oversight from technical and legal experts to political decision makers.

³¹ Zajko, *supra* note 2.

³² Scassa, *supra* note 9 at 7.

³³ *Ibid* at 11.

Scassa further highlights several troubling powers granted to the Minister under AIDA which underscore the dangers of consolidating authority in a single political actor. For instance, the Minister may compel AI developers to produce records based on broadly defined “reasonable grounds.” They may also order entities to stop using high-impact AI systems under similarly vague justifications, and disclose information about an AI system if they believe, whether correctly or incorrectly, that there is a serious imminent risk of harm and that publicizing it is essential to prevention.³⁴ While ostensibly designed to protect the public from AI-related harms, these powers become problematic when exercised without meaningful checks or balances. Under the current framework, an advisory committee functions merely as an extension of the Minister’s authority, rendering it ineffective as an independent safeguard. Their creation is therefore largely symbolic—adding layers of bureaucracy without establishing genuine autonomy or expertise in AI governance.

To remedy these deficiencies, AIDA must be amended to establish an independent regulatory body with statutory protections and powers modeled after institutions such as the Privacy Commissioner. AI, particularly generative AI, represents a novel and perpetually-evolving technological frontier. Its complexities and unpredictability necessitate specialized oversight by a multidisciplinary body capable of adapting regulatory approaches to match the pace of technological change. Entrusting oversight to a political office—or even a commissioner beholden to that office—jeopardizes the ability to develop a sophisticated, responsive, and impartial regulatory regime.

An independent regulatory body that is free from ministerial control would be better positioned to assess which areas of AI require intensive oversight and which can be governed with more flexibility. The composition of this body should be explicitly outlined in AIDA to ensure an appropriate balance of expertise. While the statute need not prescribe an exact number of representatives from each discipline, it should include language mandating the involvement of a diverse group of professionals, including: legal practitioners with expertise in technology law; jurists with experience in adjudicating matters involving emerging technologies; and AI experts, including software engineers, ethicists, and data scientists. This interdisciplinary approach would not only ensure that AIDA maintains the flexibility to adapt to evolving AI technologies but would also enhance its capacity to safeguard public interest through expert-driven oversight. By drawing on a range of perspectives, the regulatory body would be capable of identifying emerging risks, addressing unforeseen challenges, and ensuring that AI governance remains both agile and accountable.

³⁴ *Ibid* at 16.

An independent body composed of legal, technical, and academic experts would also preserve AIDA's intended agility by allowing for continuous regulatory adaptation to meet the demands of an ever-changing technological landscape. For example, generative AI systems introduce new challenges that may not be immediately apparent or predictable. A flexible and expert-led oversight regime would be able to dynamically update regulatory frameworks and guidelines as new threats emerge without being constrained by the slower pace of legislative reform or political decision-making.

Moreover, independent governance would enhance public trust in Canada's AI regulatory framework. Political oversight, however well-intentioned, risks introducing biases, conflicts of interest, and a lack of transparency into AI regulation. By contrast, an autonomous body insulated from political pressures would be better equipped to maintain public confidence in the integrity and impartiality of AI governance.

In sum, amending AIDA to establish an independent regulatory body with defined statutory powers is not merely a matter of improving regulatory efficiency—it is essential to ensuring that Canada's AI governance framework remains adaptive, accountable, and aligned with the public interest. Without meaningful reform, AIDA risks becoming a hollow instrument that offers only nominal accountability in oversight while entrusting critical AI governance decisions to political actors unqualified to confront the complexities of emerging technologies.

c. Saving a Private Right of Action

A more complex but essential reform involves the enactment of a private right of action within AIDA. While Bill C-27 included such a provision, it did so under a supplementary statute, the *Consumer Privacy Protection Act* (CPPA), which focuses primarily on privacy-related harms. Since the CPPA's provisions, particularly section 107, are narrowly tailored to privacy violations, it is unlikely that harms resulting from AI-related errors or malfunctions would fall within its ambit.³⁵ Instead, AIDA requires its own explicit private right of action to address the unique risks posed by AI technologies.

AI systems, particularly generative models, introduce novel and unpredictable challenges that presumably exceed the understanding of the layman, legal experts, and tech experts. The rapid pace of AI development makes it impossible to foresee the full range of potential harms or to rely solely on statutory penalties to regulate its risks. Given this inherent unpredictability, individuals must have access to legal recourse specific to the complexities of AI when harmed. A private right of action

³⁵ See AIDA, s 107.

would empower affected parties to hold corporations accountable and provide a necessary deterrent against negligent or reckless AI deployment. The need for a private right of action is not hypothetical as AI-related harms are already occurring with tangible consequences.³⁶ For instance, in a widely publicized case a British Columbia lawyer relied on ChatGPT to research case law for a family court hearing.³⁷ The AI, however, fabricated legal material—commonly referred to as an AI “hallucination”—resulting in the BCSC sanctioning the lawyer. Yet, the financial penalty imposed was only one of several consequences the lawyer faced. Her reputation and professional standing suffered damage and her name became the subject of national and international scrutiny. Given the acknowledged prevalence of AI hallucinations by the BC courts, among many others, a private right of action is necessary to ensure accountability and protect consumers.³⁸ Despite the lawyer’s professional responsibility, the incident highlights a more pressing concern: AI’s potential for error and its lack of safeguards to prevent such occurrences. While this example may be exceptional, it highlights the absence of clear legal recourse for parties injured by the misuse of AI.

The potential for AI-related harm extends far beyond legal professionals. For instance, an employer conducting a background check on a prospective employee could be presented with false information, leading to wrongful termination or irreparable reputational harm. Alternatively, a spouse using AI to search for their partner’s social media presence may be shown fabricated profiles on platforms such as Ashley Madison or eHarmony, falsely suggesting infidelity. In both cases, AI hallucinations could upend lives, destroy relationships, and cause financial and emotional harm. Under AIDA as it is currently drafted, these individuals—like the BC lawyer—would have no legal remedy. The absence of a private right of action leaves those harmed by AI-generated errors without recourse, forcing them to bear the financial, emotional, and reputational costs of AI malfunctions.

³⁶ For examples of hallucinations and the response by US judiciaries, see Matthew Dahl et al, “Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models” (2024) 16:1 J Leg Analysis 64, DOI: <10.1093/jla/laae003>.

³⁷ Jason Proctor, “B.C. Lawyer Reprimanded for Citing Fake Cases Invented by ChatGPT” *CBC News* (26 February 2024), online: <cbc.ca/news/canada/british-columbia/lawyer-chatgpt-fake-precedent>; see also *Zhang v Chen*, 2024 BCSC 285 [Zhang]; *Hussein v Canada (Immigration, Refugees and Citizenship)*, 2025 FC 1060; Sara Merken, “AI ‘Hallucinations’ in Court Papers Spell Trouble for Lawyers” *Reuters* (18 February 2025), online: <reuters.com/technology/artificial-intelligence/ai-hallucinations-court-papers-spell-trouble-lawyers-2025-02-18>.

³⁸ *Zhang*, *supra* note 37 at paras 24–43; see also Cade Metz & Karen Weise, “A.I. Is Getting More Powerful, but Its Hallucinations Are Getting Worse” *New York Times* (5 May 2025), online: <nytimes.com/2025/05/05/technology/ai-hallucinations-chatgpt>.

Critics such as Kaminski and Scassa have expressed skepticism about introducing a private right of action within AIDA.³⁹ Their concerns stem from the belief that such a provision would undermine AIDA's framework of risk regulation. Kaminski's reasoning, for example, suggests that permitting individual lawsuits could risk deterring innovation and impeding the development of AI technologies. However, this perspective overlooks the growing dominance of AI in various sectors and the corresponding need for accountability. A purely regulatory approach, enforced through administrative penalties and government oversight, is insufficient to address the full spectrum of potential harms caused by AI. As AI systems become more embedded in critical infrastructure, healthcare, employment, and other high-stakes domains, the potential for widespread harm grows exponentially. Relying solely on regulatory fines and penalties does little to compensate victims or deter corporate negligence. By contrast, enabling private actors to pursue legal remedies through single lawsuits, mass torts, or class actions serves a dual purpose: it provides meaningful recourse to affected individuals and incentivizes corporations to adopt safer, more responsible AI practices.

V. CONCLUSION

This article supports the enactment of AIDA but emphasizes the need for two critical amendments to ensure that Canada's AI governance framework is both effective and accountable. First, AIDA must limit the centralized authority granted to the Minister, replacing it with an independent regulatory body composed of legal practitioners, AI experts, and ethicists. Such a body would ensure impartial, expert-driven oversight, free from political influence, and capable of adapting to the rapidly evolving nature of AI technology. Second, AIDA should enshrine a private right of action to allow individuals harmed by AI-related errors or misconduct to seek legal recourse. Regulatory fines and administrative penalties alone are insufficient to deter corporate negligence or compensate victims of AI harm. A private right of action would empower individuals, incentivize responsible AI deployment, and complement the risk regulation framework envisioned by AIDA. The establishment of expert oversight and a private right of action would ensure that the gaps left by regulatory frameworks are filled, offering both preventative safeguards and remedial mechanisms.

Canada is long overdue for comprehensive AI governance. While the EU and the US have made significant strides in regulating AI, Canada continues to rely on "soft laws" and unenforceable guidelines that do little to address the complex and unpredictable challenges posed by AI. A careful review of AIDA and related scholarship reveals that the legislation is not ready for enactment in its current

³⁹ Kaminski, *supra* note 22 at 16, 22; Scassa, *supra* note 9 at 13.

form. Without adequate revisions, AIDA risks lacking the enforcement mechanisms needed for effective and agile AI governance. Strengthening AIDA through these proposed amendments will not only provide the legal clarity needed to navigate AI's complexities, but also position Canada as a global leader in responsible AI innovation. Canada must balance AI innovation with regulatory accountability to protect the individual rights of Canadians.

BIBLIOGRAPHY

LEGISLATION

Bill C-11, *An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to Make Consequential and Related Amendments to Other Acts*, 2nd Sess, 43rd Parl, 2020 (first reading 17 November 2020), online: <parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading> [perma.cc/5N3E-UWGW].

Bill C-27, *An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022), online: <parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading> [perma.cc/QE5C-YW6W].

Canadian Charter of Rights and Freedoms, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] 2016 L 119/1, art 35.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

JURISPRUDENCE

Drummond v The Cadillac Fairview Corp Ltd, 2018 ONSC 5350.

Hussein v Canada (Immigration, Refugees and Citizenship), 2025 FC 1060.

McMaster University (Re), 2024 CanLII 17583 (ON IPC).

Ontario (Finance) (Re), 2017 CanLII 143361.

Zhang v Chen, 2024 BCSC 285.

GOVERNMENT DOCUMENTS

Crampton, Paul S, *Notice to the Parties and Profession: The Use of Artificial Intelligence in Court Proceedings* (Ottawa: FCC, 2024), online: <fct-cf.ca/Content/assets/pdf/base/FC-Updated-AI-Notice-EN.pdf>.

FCC, *Interim Principles and Guidelines on the Court's Use of Artificial Intelligence* (Ottawa: FCC, 2023), online: <fct-cf.ca/en/pages/law-and-practice/artificial-intelligence>.

SECONDARY MATERIALS: MONOGRAPHS

Martin-Bariteau, Florian & Teresa Scassa, eds, *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada Inc, 2023).

SECONDARY MATERIALS: JOURNAL ARTICLES

Arancibia-Albornoz, Amaya, “Concerns in the Age of Intelligence: Shaping Regulatory Frameworks for AI in Canada” (2023/24) 14 Queen’s Pol’y Rev 147.

Attard-Frost, Blair, Ana Brandusescu & Kelly Lyons, “The Governance of AI in Canada: Findings and Opportunities from a Review of 84 AI Governance Initiatives” (2024) 41:2 Government Information Q 101929, DOI: <[10.1016/j.giq.2024.101929](https://doi.org/10.1016/j.giq.2024.101929)>.

Dahl, Matthew et al, “Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models” (2024) 16:1 J Leg Analysis 64, DOI: <[10.1093/jla/laae003](https://doi.org/10.1093/jla/laae003)>.

Kaminski, Margaret E, “The Developing Law of AI: A Turn to Risk Regulation” (2023) Digital Soc Contract: Lawfare Paper Series 24, DOI: <[10.2139/ssrn.4692562](https://doi.org/10.2139/ssrn.4692562)>.

Intahchomphoo, Channarong et al, “References to Artificial Intelligence in Canada’s Court Cases” (2020) 20:1 Leg Info Mgmt 39, DOI: <[10.1017/S1472669620000080](https://doi.org/10.1017/S1472669620000080)>.

Scassa, Teresa, “Regulating AI in Canada: A Critical Look at the Proposed *Artificial Intelligence and Data Act*” (2023) 101:1 Can Bar Rev 1.

SECONDARY MATERIALS: NEWS SOURCES

Castaldo, Joe, “How Will Canada Regulate AI? Ottawa Will Figure It Out Later” *Globe and Mail* (17 April 2023), online: <[theglobeandmail.com/business/article-canada-ai-regulation-bill](https://www.theglobeandmail.com/business/article-canada-ai-regulation-bill)>.

Gibbs, Samuel, “Elon Musk: Artificial Intelligence Is Our Biggest Existential Threat” *Guardian* (27 Oct 2014), online: <[theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat](https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat)>.

Karadeglija, Anja, “Can AI Be an Author? Federal Court Asked to Decide New Copyright Case” *CTV News* (13 July 2024), online: <[ctvnews.ca/sci-tech/article/ottawa-weighing-plans-on-ai-and-copyright-as-openai-fights-ontario-court-jurisdiction](https://www.ctvnews.ca/sci-tech/article/ottawa-weighing-plans-on-ai-and-copyright-as-openai-fights-ontario-court-jurisdiction)>.

Mach, Jessica, “CanLII Sues AI Legal Assistant Caseway AI for Copyright Infringement” *Canadian Lawyer Mag* (7 November 2024), online: <[canadianlawyermag.com/resources/legal-technology/canlii-sues-ai-legal-assistant-caseway-ai-for-copyright-infringement](https://www.canadianlawyermag.com/resources/legal-technology/canlii-sues-ai-legal-assistant-caseway-ai-for-copyright-infringement)>.

Merken, Sara, “AI ‘Hallucinations’ in Court Papers Spell Trouble for Lawyers” *Reuters* (18 February 2025), online: <[reuters.com/technology/artificial-intelligence/ai-hallucinations-court-papers-spell-trouble-lawyers-2025-02-18](https://www.reuters.com/technology/artificial-intelligence/ai-hallucinations-court-papers-spell-trouble-lawyers-2025-02-18)>.

Metz, Cade & Karen Weise, “A.I. Is Getting More Powerful, but Its Hallucinations Are Getting Worse” *New York Times* (6 May 2025), online: <[nytimes.com/2025/05/05/technology/ai-hallucinations-chatgpt](https://www.nytimes.com/2025/05/05/technology/ai-hallucinations-chatgpt)>.

Proctor, Jason, “B.C. Lawyer Reprimanded for Citing Fake Cases Invented by ChatGPT” *CBC News* (26 February 2024), online: <[cbc.ca/news/canada/british-columbia/lawyer-chatgpt-fake-precedent](https://www.cbc.ca/news/canada/british-columbia/lawyer-chatgpt-fake-precedent)>.

Stavis-Gridneff, Matina, “Major Canadian News Outlets Sue OpenAI in New Copyright Case” *New York Times* (29 November 2024), online: <[nytimes.com/2024/11/29/world/canada/canada-openai-lawsuit-copyright](https://www.nytimes.com/2024/11/29/world/canada/canada-openai-lawsuit-copyright)>.

Zajko, Mike, “Canada Is Failing to Regulate AI amid Fear and Hype” *Policy Options* (13 January 2023), online: <[policyoptions.irpp.org/2023/06/canada-failing-ai-regulation-fear-hype](https://www.policyoptions.irpp.org/2023/06/canada-failing-ai-regulation-fear-hype)>.

SECONDARY MATERIALS: ELECTRONIC SOURCES

Arai, Maggie, “Five Things to Know About Bill C-27” (18 October 2022),
online: <srinstitute.utoronto.ca/news/five-things-to-know-about-bill-c-27>.

Wylie, Bianca, “ISED’s Bill C-27 + AIDA. Part 4: Calling on Federal MPs For a
Necessary Defense of Democratic Process” (22 April 2023), online:
<biancawylie.medium.com/iseds-bill-c-27-aida-part-4-calling-on-federal-mps-for-necessary-defense-of-democratic-process>.

Canadian Law Review Quarterly
Volume 1 Issue 3
December 2025

**CANADA’S CRYPTO REGULATORY CROSSROADS:
THE NEED FOR LEGAL EVOLUTION IN A
GLOBALIZED ECONOMY**

Thomas Tudor-Doonan

ABSTRACT

Cryptocurrency is rapidly transforming global finance, yet Canada’s regulatory response remains fragmented, reactive, and constitutionally constrained. Unlike the United States—where adaptive frameworks have supported innovation—Canada’s lack of a coordinated strategy has created legal uncertainty, discouraged institutional participation, and eroded competitiveness. This paper examines key gaps in securities law, anti-money laundering enforcement, and taxation as relevant to cryptocurrency regulation. The collapse of QuadrigaCX and Binance’s recent exit from the Canadian market serve as instructive case studies of the consequences of these gaps. This paper argues that reform is both urgent and constitutionally achievable through federal-provincial coordination. Drawing on comparative models and legal precedent, it proposes a set of targeted reforms to clarify legal standards, modernize taxation, and strengthen federal enforcement. Together, these changes would create a more coherent and responsive regulatory foundation for Canada’s digital asset sector.

Tudor-Doonan, Thomas, “Canada’s Crypto Regulatory Crossroads: The Need for Legal Evolution in a Globalized Economy” (2025) 1:3 Can L Rev Q 18.

I. INTRODUCTION

The increasingly digital and technologically driven nature of finance has positioned cryptocurrency as a central force in the transformation of global financial systems. Cryptocurrencies are digital assets that rely on encryption and distributed networks, typically underpinned by blockchain technology. Blockchain is a digital system consisting of a decentralized, tamper-resistant ledger in which batches of transactions are grouped into chronologically linked “blocks.” These blocks are validated through a network-wide agreement process known as consensus, whereby independent participants called nodes collectively verify and approve each block of transactions instead of relying on a single central authority. By enabling peer-to-peer exchanges of value, these assets challenge conventional financial systems and introduce new models of ownership, investment, and payment. Consequently, cryptocurrencies have started to redefine the structural foundations of global commerce and financial regulation. While major jurisdictions like the United States, the European Union, and China are integrating digital assets into their regulatory frameworks, Canada remains without a unified national strategy or legal approach.

While cryptocurrency in Canada is subject to regulatory oversight, this oversight takes the form of a fragmented patchwork issued by various provincial and federal bodies such as the Canadian Securities Administrators (CSA) and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). These bodies serve as Canada’s Financial Intelligence unit, responsible for monitoring and analyzing financial transactions to detect money laundering and terrorist financing.¹ However, there is currently no comprehensive legislation regulating cryptocurrency at either the provincial or federal level. As a result, Canada’s regulatory framework remains divided, legally uncertain, and inefficient. In the absence of a responsive, innovation-oriented framework, Canada risks long-term strategic decline. Constitutional constraints further complicate centralized reform, making federal-provincial cooperation essential. The 2011 *Reference re Securities Act* underscores this point. In that decision, the Supreme Court unanimously determined that day-to-day oversight of trading and securities professionals falls within provincial jurisdiction under section 92(13) of the *Constitution Act, 1867*. Parliament’s proposed federal *Securities Act* was deemed to exceed its trade-and-commerce power by intruding on those provincial matters. However, the

¹ Canadian Securities Administrators, *Regulatory Framework for Crypto-Asset Trading Platforms* (29 Mar 2021), online: <[securities-administrators.ca/investor-tools/crypto-assets/regulation-of-crypto-assets](https://www.securities-administrators.ca/investor-tools/crypto-assets/regulation-of-crypto-assets/)>; Financial Transactions and Reports Analysis Centre of Canada, *Financial Transactions and Reports Analysis Centre of Canada* (Ottawa: FINTRAC, 2020), online: <fintrac-canafe.canada.ca/intro-eng>.

Court clarified that federal authority may still apply to genuinely national issues, such as systemic risk management and national securities data collection.²

This paper argues that Canada's current regulatory approach to cryptocurrency is outdated, fragmented, and constitutionally inadequate for the demands of a rapidly evolving digital economy. To address these shortcomings, it proposes a modernized legal strategy grounded in constitutional principles and comparative policy analysis. The paper proceeds in three parts. First, it outlines the existing Canadian regulatory framework and its jurisdictional constraints. Second, it conducts a cross-border comparison with the US to highlight divergent approaches to innovation and oversight. Third, it sets out targeted policy recommendations designed to establish a coherent, constitutionally-sound foundation for digital asset regulation that promotes investor protection, fosters innovation, and reinforces Canada's global competitiveness in financial technology.

II. CANADA'S CRYPTOCURRENCY REGULATION: CHALLENGES, GAPS, AND COMPLIANCE BARRIERS

Current cryptocurrency regulation in Canada is shaped by oversight from both federal and provincial regulatory agencies and primarily deals with concerns related to financial stability, securities compliance, anti-money laundering (AML), and taxation.³ While the Canadian government acknowledges the increasing influence of cryptocurrency in the financial system, the accompanying legal framework remains fragmented and frequently reactive rather than proactive. In several key respects, it is inadequate to address the evolving challenges posed by digital assets. This fragmented regulatory structure has led to persistent challenges for businesses, investors, and consumers navigating the Canadian cryptocurrency market.

a. Securities Regulation and Cryptocurrency Oversight in Canada

In Canada, the regulation of cryptocurrency primarily falls within the domain of provincial securities regulators, as the federal government lacks constitutional authority to enact a unified national securities regime. This jurisdictional arrangement is led by the CSA, which has taken the position that most Crypto Trading Platforms offering custodial services qualify as securities dealers. In 2021,

² Reference re Securities Act, 2011 SCC 66.

³ Canadian Securities Administrators, *Regulatory Framework for Crypto-Asset Trading Platforms*, *supra* note 1.

the CSA clarified that such platforms must register with securities regulators and comply with provincial securities laws, mirroring the obligations imposed on traditional investment firms.⁴ The legal basis for this position draws from provincial securities statutes such as Ontario’s *Securities Act*, which define a “security” as investment contracts and instruments that function like traditional financial products such as stocks, bonds, and mutual fund units.⁵ This interpretation has played a key role in shaping how cryptocurrency assets are treated under securities law; its rationale lies in the functional similarities between many digital asset platforms and traditional brokerages, particularly when they offer custodial services and facilitate trading. If a platform offers custody (i.e., it holds users’ crypto on their behalf) and facilitates trading, it may resemble a marketplace or brokerage and therefore invoke relevant obligations under securities law. These obligations include compliance with “Know Your Client” procedures, which require platforms to verify users’ identities, as well as financial disclosure requirements and market integrity standards.⁶

Platforms that fail to comply have faced legal action. For instance, in 2021, the Ontario Securities Commission initiated proceedings against KuCoin and Poloniex for operating without proper registration with the CSA.⁷ In 2023, the CSA took a firmer stance by issuing Pre-Registration Undertakings, requiring Crypto Trading Platforms to meet strict regulatory standards while awaiting full registration. That same year, it introduced a conditional ban on stablecoin trading, a form of digital asset pegged to fiat currency, meaning government-issued money such as the Canadian dollar or US dollar, unless issuers obtained regulatory pre-approval and satisfied transparency requirements. In addition to the CSA, the Canadian Investment Regulatory Organization has imposed compliance obligations on cryptocurrency firms, mirroring the regulatory framework applied to traditional investment dealers.⁸ However, the absence of formal federal legislation

⁴ *Ibid.*

⁵ *Securities Act*, RSO 1990, c S5.

⁶ Canadian Securities Administrators, *Regulatory Framework for Crypto-Asset Trading Platforms*, *supra* note 1.

⁷ Ontario Securities Commission, *OSC Takes Action Against Second Non-Compliant International Crypto Asset Trading Platform* (2021), online: <osc.ca/en/news-events/news/osc-takes-action-against-second-non-compliant-international-crypto-asset-trading-platform>.

⁸ Canadian Investment Regulatory Organization, “CIRO Proposes New Guidance for Order Execution Only Dealers” (12 Aug 2025), online: <ciro.ca/newsroom/publications/ciro-proposes-new-guidance-order-execution-only-dealers>; Canadian Securities Administrators, “CSA Staff Notice 21-332 Crypto Asset Trading Platforms: Pre-Registration Undertakings – Changes to Enhance Canadian Investor Protection” (22 Feb 2023), online: <osc.ca/en/securities-law/instruments-rules-policies/2/21-332/csa-staff-notice-21-332-crypto-asset-trading-platforms>.

specifically addressing stablecoins has contributed to a regulatory environment that remains unpredictable for businesses and investors.

b. Anti-Terrorist Financing Regulation

Enforcement of AML and anti-terrorist financing in Canada's cryptocurrency sector is mandated under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and carried out by FINTRAC.⁹ In 2020, Canada became one of the first jurisdictions to classify cryptocurrency exchanges as Money Services Businesses, bringing them under federal AML reporting obligations. Under this framework, crypto firms must conduct Know Your Client checks and report suspicious or large transactions (over \$10,000 CAD) to FINTRAC. They are also subject to the Travel Rule, which requires sender and recipient information to be transmitted with cross-border crypto transfers.¹⁰ While these requirements align with international standards set by the Financial Action Task Force, their implementation remains difficult. The decentralized nature of crypto networks, combined with the rise of privacy-enhancing cryptocurrencies like Monero and Zcash and peer-to-peer trading platforms, limits traceability and frustrates traditional enforcement methods.¹¹ Without intermediaries or centralized control, authorities often struggle to identify transaction origins, verify counterparties, or monitor flows in real time. These limitations have created blind spots in the regulatory system, allowing illicit financial activity to persist.¹² Addressing these gaps will require FINTRAC to expand its technological capabilities and adopt a more robust, coordinated approach to oversight across Canada's crypto sector.

c. QuadrigaCX Scandal and Regulatory Failures

The collapse of QuadrigaCX in 2018 remains one of the clearest illustrations of regulatory failure in Canada's cryptocurrency sector. At its peak, QuadrigaCX was the country's largest digital asset exchange. The platform ceased operations

pre-registration-undertakings-changes>.

⁹ *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17; Financial Transactions and Reports Analysis Centre of Canada, *Financial Transactions and Reports Analysis Centre of Canada*, *supra* note 1.

¹⁰ Financial Action Task Force, "The FATF Recommendations" (Jun 2025) Recommendation 16 and Interpretive Note 16/INR.16, online: <fatf-gafi.org/en/publications/Fatfrecommendations/Fatfrecommendations>; see also Financial Action Task Force, "Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (28 Oct 2021) at paras 15–16, online: <fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021>.

¹¹ Douglas W Arner et al, "The Financialisation of Crypto: Designing an International Regulatory Consensus" (2024) 53 *Computer L & Security Rev* 105970, DOI: <10.1016/j.clsr.2024.105970>; Financial Action Task Force, "Updated Guidance," *supra* note 10.

¹² Arner et al, "The Financialisation of Crypto," *supra* note 11.

following the abrupt death of its CEO, Gerald Cotten, who had maintained exclusive access to the exchange’s customer funds. In the wake of Cotten’s death, more than \$215 million CAD in customer assets went missing, prompting investigations that revealed a long-standing pattern of mismanagement, fraudulent internal transactions, and the absence of basic financial safeguards.¹³ The scale of the losses and the failure to detect misconduct over several years exposed a regulatory vacuum that left consumers unprotected and underscored the urgent need for oversight in Canada’s cryptocurrency sector.

The regulatory failure in the QuadrigaCX case was twofold. First, the platform had operated for years without meaningful oversight from FINTRAC, provincial securities regulators, or any federal financial authority. QuadrigaCX was not subject to AML reporting requirements or capital reserve obligations, allowing Cotten to engage in unaudited internal transactions and unauthorized fund withdrawals. This level of operational freedom—granted to an unregistered exchange managing hundreds of millions in customer funds—would not have been possible in any traditionally regulated financial institution.¹⁴ Second, regulatory action only materialized after the scandal had already resulted in substantial financial losses, highlighting the reactive nature of Canada’s regulatory approach. FINTRAC implemented AML rules for cryptocurrency firms in 2020, two years after QuadrigaCX’s collapse, revealing the delayed and inadequate enforcement mechanisms governing Canada’s digital asset market.¹⁵

d. Binance’s Exit from Canada

The implications of Canada’s stringent regulatory approach were evident in May 2023, when Binance—the world’s largest cryptocurrency exchange—announced it was leaving the Canadian market. The company pointed to the CSA’s Pre-Registration Undertaking requirements, saying the compliance costs and regulatory hurdles made it impossible to continue operating in Canada. Binance’s withdrawal was followed by similar exits from other major cryptocurrency exchanges, including OKX and Paxos, further illustrating the growing difficulty of operating in Canada’s increasingly restrictive regulatory landscape.¹⁶ The

¹³ Ontario Securities Commission, *QuadrigaCX: A Review by Staff of the Ontario Securities Commission* (Toronto: OSC, 2020), online: <osc.gov.on.ca/quadrigacxreport>.

¹⁴ Financial Transactions and Reports Analysis Centre of Canada, *Financial Transactions and Reports Analysis Centre of Canada*, *supra* note 9.

¹⁵ *Ibid.*

¹⁶ Tracy Wang, “Binance Announces Exit from Canada, Citing Regulatory Tensions” *Coindesk* (15 May 2023), online: <coindesk.com/business/2023/05/12/binance-announces-exit-from-canada-citing-regulatory-tensions>.

departure of these key industry players suggests that Canada’s regulatory approach, while prioritizing investor protection, may inadvertently be stifling innovation and discouraging foreign investment in the digital asset space. While the QuadrigaCX scandal revealed the dangers of regulatory neglect, Binance’s departure illustrates the risks of overcorrecting without a flexible or innovation-oriented framework. Canada’s challenge lies not in choosing between regulation and deregulation, but in designing a regime that is both robust and responsive.

III. CANADA & THE UNITED STATES: COMPARATIVE ANALYSIS OF CRYPTOCURRENCY REGULATION

As cryptocurrency continues to transform global finance, Canada and the US have responded with sharply different regulatory strategies. Both face similar challenges—uncertain classifications, evolving technologies, and competing priorities—but their approaches diverge in clarity and adaptability. In Canada, the CSA has taken the position that most trading platforms offering custody services fall under provincial securities laws, requiring them to register as securities dealers. This view, reinforced through bulletins and enforcement actions by bodies like the Ontario Securities Commission, frames many digital assets as securities by default.¹⁷ Conversely, the US remains divided on classification: the Securities and Exchange Commission treats many tokens as securities while the Commodity Futures Trading Commission claims jurisdiction over Bitcoin and Ethereum as commodities.¹⁸ Although this overlap creates friction, it also opens space for judicial interpretation and flexible, state-level experimentation—giving American firms room to operate while legal clarity evolves.

a. Institutional Participation and Financial Sector Engagement

Another point of divergence lies in institutional adoption. In the US, major financial institutions such as BlackRock, Fidelity, and JPMorgan Chase have embraced digital assets. JPMorgan’s crypto-based payment system has processed billions of dollars in transactions and digital asset exchange-traded funds (ETFs) are growing in market presence. By contrast, Canada’s early leadership in the

¹⁷ Canadian Securities Administrators, “CSA Staff Notice 21-332,” *supra* note 8; Ontario Securities Commission, *OSC Takes Action*, *supra* note 7.

¹⁸ US Securities and Exchange Commission, *Enforcement Actions: Crypto Assets* (Washington, DC: SEC, 2025), online: <sec.gov/about/divisions-offices/division-enforcement/cyber-crypto-assets-emerging-technology/enforcement-actions>; United States, Commodity Futures Trading Commission, *Digital Assets* (Washington, DC: CFTC, 2025), online: <cftc.gov/digitalassets/index>.

sector, as the first country to approve a Bitcoin-based ETF, has since faded. Institutions remain wary due to capital requirements imposed by the Office of the Superintendent of Financial Institutions (OSFI)—the federal agency responsible for regulating and supervising banks and other federally regulated financial institutions, and ongoing regulatory ambiguity. Canadian banks and pension funds have largely avoided the space, curbing liquidity and slowing adoption.¹⁹ As a result, Canada has failed to capitalize on institutional demand despite early momentum.

b. Jurisdictional Models: Federalism vs Fragmentation

Both nations operate under federal systems, but the allocation of power affects how cryptocurrency is regulated. In the US, federal bodies like the Securities and Exchange Commission and the Commodity Futures Trading Commission regulate national markets, while states create localized pro-crypto environments. Wyoming and Florida have enacted laws granting banking charters to digital asset firms and permitting the use of cryptocurrency for certain government services, transforming them into regional hubs for digital innovation, particularly in blockchain and cryptocurrency technologies.²⁰

Conversely, Canada faces a number of constitutional limits on federal authority to regulate securities markets through a unified national framework. The Supreme Court’s decision in *Reference re Securities Act* confirmed that securities regulation falls under provincial jurisdiction pursuant to section 92(13) of the *Constitution Act, 1867*. As a result, oversight is divided across a patchwork of provincial regimes coordinated by the CSA, but lacking national harmonization. In contrast, the US operates under a centralized regime through the Securities and Exchange Commission (SEC), which enables uniform federal oversight of capital markets. Canada’s constitutional structure precludes such a model, leaving platforms to navigate a fragmented system. This has led to the duplication of registration processes, compliance obligations, and disclosure requirements across jurisdictions, resulting in conflicting rules and lengthy approval timelines that create friction for firms attempting to operate or scale across multiple provinces.²¹

¹⁹ Office of the Superintendent of Financial Institutions, *Capital and Liquidity Treatment of Crypto-Asset Exposures (Banking) – Guideline* (Ottawa: OSFI, 2025), online: <osfi-bsif.gc.ca/en/guidance/guidance-library/capital-liquidity-treatment-crypto-asset-exposures-banking-guideline>.

²⁰ US Securities and Exchange Commission, *Enforcement Actions*, *supra* note 18; United States, Commodity Futures Trading Commission, *Digital Assets*, *supra* note 18; Frank Emmert, “Blockchain and Private International Law: The Perspective of the United States of America” in Matthias Lehmann, ed, *Blockchain and Private International Law* (Leiden: Brill Nijhoff, 2023) 709 at 709, DOI: <10.1163/9789004514850_025>.

²¹ *Reference re Securities Act*, *supra* note 2.

c. Adapting Infrastructure for a Digital Asset Economy

Compared to Canada, the US has adopted more innovation-friendly policies, particularly in its regulatory approach to digital assets and financial technology. President Biden's 2022 *Executive Order on Ensuring Responsible Development of Digital Assets* emphasized coordination, consumer protection, and exploration of a digital currency regulated by the central bank. Several states offer regulatory sandboxes for financial tech firms to experiment under supervision, lowering entry barriers and enabling agile policy evolution.²² A regulatory sandbox allows companies to test innovative products or services under relaxed regulatory oversight, typically within a controlled environment and for a limited time.

Canada lacks a unified sandbox program or innovation strategy. While provincial regulators provide guidance, there is no national mechanism encouraging pilot programs or safe experimentation. Binance, for instance, cited inflexible securities requirements as a primary reason for its 2023 exit from the Canadian market, illustrating the cost of Canada's regulatory rigidity.²³ Without reform, Canada will continue losing ground to more nimble jurisdictions.

The US has established itself as a global hub for crypto investment, infrastructure, and talent. Regulatory complexity has not deterred participation; rather, it has spurred innovation in the development of new financial products, blockchain-based services, and institutional crypto offerings. This innovation is supported by a system of overlapping jurisdictions and evolving legal guidance that accommodates experimentation while maintaining oversight. Most notably, the White House recently directed agencies to explore a strategic Bitcoin reserve and a national digital asset stockpile, signaling long-term commitment to integration.²⁴ In contrast, Canada is witnessing a talent drain; projects like Aave and dYdX have shifted abroad to avoid domestic restrictions.²⁵

Though the American framework is imperfect, it is strategically responsive—tolerant of risk, open to market signals, and committed to forward-looking integration. Canada's system, by contrast, is cautious to a fault. Without national

²² Executive Office of the President of the United States, *Executive Order on Ensuring Responsible Development of Digital Assets* (Washington, DC: White House, 2022), online: <[bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets](https://www.bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets)>.

²³ Wang, "Binance Announces Exit from Canada," *supra* note 16.

²⁴ Executive Office of the President of the United States, *Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile* (Washington, DC: White House, 2025), online: <[whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile](https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile)>.

²⁵ Arner et al, "The Financialisation of Crypto," *supra* note 11.

coordination and legal modernization, Canada risks becoming irrelevant in the global digital economy. While the division of powers must be respected, regulatory paralysis is not constitutionally required; reform is both possible and urgent.

IV. CONSTITUTIONAL CONSTRAINTS & COORDINATED REGULATION

Canada's fragmented approach to cryptocurrency regulation cannot be fully understood without addressing the constitutional division of powers. This division represents a foundational barrier that has long complicated efforts to implement national financial oversight. The federal government's inability to unilaterally establish a national securities regime is well established in Canadian constitutional jurisprudence. In *Reference re Securities Act* the Supreme Court held that securities regulation falls within provincial jurisdiction under section 92(13) of the *Constitution Act, 1867*, as it pertains to property and civil rights.²⁶ The Court reaffirmed that, while Parliament can legislate on matters of national concern, it cannot do so at the expense of provincial legislative authority over localized economic activities. As a result, any federal attempt to create a unified securities law framework absent provincial consent would represent constitutional overreach.²⁷

However, the Court did not foreclose the possibility of federal involvement in complementary or intersecting domains. In fact, federal jurisdiction remains intact in several areas directly implicated by the rise of cryptocurrency, including money laundering, criminal law, banking, and taxation. For instance, Parliament retains full authority to legislate under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, which governs many of the compliance obligations currently imposed on cryptocurrency platforms through FINTRAC. Similarly, the federal government oversees banking institutions under section 91(15), and is responsible for criminal enforcement mechanisms under section 91(27), including laws against fraud, market manipulation, and financial misconduct involving digital assets. Moreover, the federal *Income Tax Act* governs the taxation of capital gains and income derived from cryptocurrency transactions.²⁸

These existing areas of federal jurisdiction create a robust foundation for coordinated regulation. Indeed, the development of a functional and constitutionally sound regulatory framework need not rely on federal supremacy

²⁶ *Reference re Securities Act*, *supra* note 2.

²⁷ *Ibid*; *Constitution Act, 1867*, 30 & 31 Vict, c 3 (UK), s 92(13).

²⁸ *Income Tax Act*, RSC 1985, c 1 (5th Supp); *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, *supra* note 9.

over securities law. Rather, it can be achieved through institutional cooperation. One such instance is the Cooperative Capital Markets Regulatory System (CCMR): a joint initiative between the federal government and several provinces—including Ontario, British Columbia, and New Brunswick—that proposes a unified, yet jurisdictionally respectful, capital markets authority. The CCMR aims to harmonize standards across provinces while preserving their core regulatory powers. Though not fully implemented, the CCMR demonstrates a viable pathway for the development of national frameworks that respect provincial autonomy. Its enabling legislation, particularly the proposed *Capital Markets Stability Act*, seeks to address systemic risk, criminal enforcement, and interjurisdictional coordination—areas that map directly onto the needs of cryptocurrency regulation.²⁹

A nationally-harmonized strategy for digital asset oversight does not require federal intrusion into provincial securities jurisdiction. Instead, the federal government can exercise its existing powers to establish interoperable technical standards, develop shared AML enforcement tools, and incentivize provincial participation through tax measures and regulatory support. Provinces would retain their authority to classify and regulate digital assets under securities law. This cooperative division of regulatory responsibilities aligns with the constitutional framework affirmed by the Supreme Court in 2011 and offers a practical, efficient model for policy coordination. A federal-provincial framework is thus both legally viable and the most effective path toward timely, cohesive regulation in a rapidly-advancing digital economy.

V. POLICY RECOMMENDATIONS: A NEW APPROACH FOR CANADA

As demonstrated throughout this paper, Canada’s approach to cryptocurrency regulation is hindered by constitutional constraints, legal fragmentation, and a lack of harmonized oversight. Nonetheless, these challenges can be addressed through targeted, cooperative reform. By building on existing statutory powers, jurisprudential foundations, and collaborative models, the federal and provincial governments can jointly establish a modernized framework that is both constitutionally sound and innovation oriented. The following policy recommendations outline a practical path toward achieving that goal.

²⁹ Canada, *Memorandum of Agreement regarding the Cooperative Capital Markets Regulatory System* (Ottawa: Government of Canada, 2015), online: <canada.ca/content/dam/fin/migration/n15/docs/moa-pda-yukon-eng.pdf>; Department of Finance Canada, *Capital Markets Stability Act Consultation Document* (Ottawa: Department of Finance Canada, 2015), online: <fin.canada.ca/drleg-apl/2014/cmsa-lsmc-l-eng.pdf>.

Canada must first establish a coordinated national framework through voluntary provincial participation. Under current constitutional doctrine, securities regulation falls primarily under provincial jurisdiction as affirmed in *Reference re Securities Act*, however, the Court also upheld the legitimacy of joint federal-provincial initiatives.³⁰ One such initiative is the CCMR which proposes that provinces and the federal government enact substantively harmonized legislation to regulate capital markets within their respective jurisdictions. Although the CCMR has not been fully implemented, it has garnered the support of several provinces, including Ontario, British Columbia, and New Brunswick. The federal component of this system, the proposed *Capital Markets Stability Act*, provides mechanisms for federal intervention in areas such as systemic risk and criminal enforcement, without encroaching upon provincial autonomy. Extending this model to include digital assets would allow for nationally consistent rules governing registration, investor protection, and trading platforms, while respecting the constitutional boundaries set out in sections 91 and 92 of the *Constitution Act, 1867*.³¹

Secondly, Parliament must modernize the *Income Tax Act* and direct the Canada Revenue Agency (CRA) to issue binding interpretive guidance on the taxation of cryptocurrency. Under current law, cryptocurrency is treated as a commodity rather than a currency. Consequently, nearly all uses including selling, trading, mining, or spending are considered taxable events. The CRA applies two principal frameworks: profits from frequent or profit-oriented activity are taxed in full as business income under section 9, while casual or investment-based gains fall under section 38 as capital gains of which only 50 percent are included in taxable income.³² Additionally, when cryptocurrency is used to make purchases, the transaction is treated as a barter. The fair market value of the goods or services at the time must be reported as income, and the transaction may also be subject to GST or HST.³³

This framework fails to adequately address newer and increasingly prevalent forms of crypto activity. Parliament should amend the *Income Tax Act* to explicitly

³⁰ *Reference re Securities Act*, *supra* note 2.

³¹ Canada, *Memorandum of Agreement*, *supra* note 29; Department of Finance Canada, *Capital Markets Stability Act Consultation Document*, *supra* note 29; *Constitution Act, 1867*, *supra* note 27, ss 91, 92.

³² *Income Tax Act*, *supra* note 28, ss 9(1), 38(a).

³³ BDO Canada LLP, “The CRA’s Position on Cryptocurrency: Income Tax Implications” (Mar 2022), online: <bdo.ca/insights/cra-cryptocurrency-implications>; Canada Revenue Agency, *Information for Crypto-Asset Users and Tax Professionals* (Ottawa: CRA, 2021), online: <canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/cryptocurrency-guide.html>.

state that crypto-to-crypto exchanges constitute a disposition, that staking rewards are taxable when received, and that airdrops and other asset-based income forms are to be treated as either windfalls or business income depending on their context. These clarifications would both reduce uncertainty for taxpayers as well as improve enforcement consistency for the CRA. Internationally, Canada can look to the 2022 Crypto-Asset Reporting Framework published by the Organisation for Economic Co-operation and Development (OECD), which sets out standardized cross-border reporting obligations for digital asset transactions and provides clear, legally operable definitions for crypto-assets and intermediaries. Similarly, the American Internal Revenue Service (IRS) requires taxpayers to report each sale, swap, or disposition of digital assets in detail on Form 8949, ensuring transaction-level transparency.³⁴ These models demonstrate how comprehensive disclosure and legal clarity can enhance both compliance and administrative effectiveness—principles Canada has yet to fully integrate into its tax regime for digital assets.³⁵

Finally, the federal government must strengthen its use of constitutionally-grounded powers in areas where it holds exclusive jurisdiction: banking, criminal law, and AML. Under section 91(15) of the *Constitution Act, 1867*, Parliament is empowered to regulate banking, which includes setting prudential standards for financial institutions engaging with digital assets.³⁶ This authority is already being exercised through OSFI, which, in 2023, released guidelines requiring federally-regulated entities to conduct risk assessments before engaging with crypto products or clients and to maintain internal controls proportionate to their digital asset exposure.³⁷ The guideline. OSFI's guidance is non-legislative but carries enforceable compliance expectations under existing banking regulations. Section 91(27) grants Parliament jurisdiction over criminal law, including fraud, market manipulation, and illicit finance involving digital assets.³⁸ This is operationalized through legislation like the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, which empowers FINTRAC to monitor and report suspicious

³⁴ United States, Internal Revenue Service, *Digital Assets* (Washington, DC: IRS, 2025), online: <irs.gov/filing/digital-assets>.

³⁵ *Income Tax Act*, *supra* note 28, ss 9, 38; Organisation for Economic Co-operation and Development, *International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard* (Paris: OECD Publishing, 2022), DOI: <10.1787/896d79d1-en>; United States, Internal Revenue Service, *About Form 8949, Sales and Other Dispositions of Capital Assets* (Washington, DC: IRS, 2023), online: <irs.gov/forms-pubs/about-form-8949>.

³⁶ *Constitution Act, 1867*, *supra* note 27, s 91(15).

³⁷ Office of the Superintendent of Financial Institutions, *Guideline B-10: Third-Party Risk Management* (Ottawa: OSFI, 2023), online: <osfi-bsif.gc.ca/en/guidance/guidance-library/third-party-risk-management-guideline>.

³⁸ *Constitution Act, 1867*, *supra* note 27, s 91(27).

transactions in the crypto sector.³⁹ Despite this framework, FINTRAC lacks the enforcement infrastructure to deal with decentralized protocols and anonymous wallets. The federal government should expand FINTRAC's mandate, allocate enforcement resources for crypto forensics, and improve interagency data-sharing mechanisms. These reforms would not require provincial involvement and could be implemented unilaterally within the scope of federal powers.⁴⁰

In sum, these policy reforms are neither radical nor constitutionally problematic. They reflect a deliberate re-alignment of jurisdictional authority that draws from Canadian legal precedent and international regulatory practice. Reform is not only compatible with constitutional federalism, it is demanded by the realities of a rapidly evolving digital economy. Canada cannot afford continued inertia. It must act decisively to modernize its crypto regulatory infrastructure while preserving the constitutional balance that defines its governance model.

Some policymakers and legal scholars may argue that Canada's stringent approach to cryptocurrency oversight, while imperfect, reflects an appropriately cautious response to an inherently high-risk sector. From this perspective, the collapse of domestic platforms like QuadrigaCX, coupled with recent global failures such as FTX, has justified a defensive regulatory stance. Strict provincial enforcement and investor restrictions, such as those introduced under the CSA's Pre-Registration Undertaking framework, are seen as necessary measures to uphold market integrity rather than obstacles to innovation.

This perspective is not without merit. In its 2023 consultation, the CSA emphasized the need to prioritize investor protection in light of "heightened operational, custody, and solvency risks" in crypto markets.⁴¹ While these concerns are legitimate, Canada's current model has produced paralysis rather than clarity. As shown through Binance's 2023 exit and the widespread departure of platforms like Paxos and OKX, regulatory uncertainty and duplicative obligations have pushed innovation offshore, rather than protecting domestic stakeholders. In contrast, despite legal disputes between federal regulators, the US has enabled provisional market participation under evolving rules. Financial institutions

³⁹ *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, *supra* note 9.

⁴⁰ *Constitution Act, 1867*, *supra* note 27, ss 91(15), 91(27); Office of the Superintendent of Financial Institutions, *Capital and Liquidity Treatment of Crypto-Asset Exposures*, *supra* note 19.

⁴¹ Canadian Securities Administrators, "Staff Notice 21-330 Guidance for Crypto-Trading Platforms - Requirements relating to Advertising, Marketing and Social Media Use" (23 Sep 2021), online: <osc.ca/en/securities-law/instruments-rules-policies/2/21-330/csa-iroc-staff-notice-21-330-guidance-crypto-trading-platforms-requirements-relating-advertising>; see also *Constitution Act, 1867*, *supra* note 27, s 92(13).

continue to develop digital asset services in this environment, while Canada's ecosystem contracts.

This paper does not advocate for deregulation. Rather, it proposes a collaborative federal-provincial regime grounded in constitutional precedent and modeled after frameworks like the CCMR. Such coordination would enable consistent enforcement, coherent policy design, and more effective consumer protection. The primary concern is not the prospect of reform, but the continued risk of regulatory stagnation.

VI. CONCLUSION

Canada stands at a critical juncture in the development of its regulatory framework for digital assets and its broader position in the global financial technology landscape. As digital assets continue to reshape global finance, the jurisdictions that develop clear, adaptive, and constitutionally grounded regulatory frameworks will lead the next phase of economic and technological advancement. Despite its early promise, Canada's fragmented and reactive approach has stalled innovation, driven investment and talent abroad, and weakened its position in the digital economy. This paper has demonstrated that meaningful reform is both possible and necessary. A coordinated federal-provincial framework modeled on the CCMR can deliver harmonized oversight without compromising constitutional boundaries. This approach must be paired with targeted reforms: modernizing the *Income Tax Act* to address emerging crypto activities, issuing binding CRA guidance to clarify compliance obligations, and fully exercising federal powers in banking and AML. Taken together, these measures form a practical and legally-coherent roadmap for regulatory modernization. The challenge is no longer one of legal authority—it is one of execution. Canada must act with urgency and resolve to secure its role in the future of digital finance.

BIBLIOGRAPHY

LEGISLATION

Constitution Act 1867 (UK), 30 & 31 Vict, c 3.

Income Tax Act, RSC 1985, c 1 (5th Supp).

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c 17.

Securities Act, RSO 1990, c S5.

JURISPRUDENCE

Reference re Securities Act, 2011 SCC 66.

GOVERNMENT DOCUMENTS

Canada Revenue Agency, *Information for Crypto-Asset Users and Tax Professionals* (Ottawa: CRA, 2021), online: <canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/cryptocurrency-guide.html>.

Canada, *Memorandum of Agreement regarding the Cooperative Capital Markets Regulatory System* (Ottawa: Government of Canada, 2015), online: <canada.ca/content/dam/fin/migration/n15/docs/moa-pda-yukon-eng.pdf>.

Department of Finance Canada, *Capital Markets Stability Act Consultation Document* (Ottawa: Department of Finance Canada, 2015), online: <fin.canada.ca/drleg-apl/2014/cmsa-lsmc-l-eng.pdf>.

Executive Office of the President of the United States, *Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile* (Washington, DC: White House, 2025), online: <whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile>.

Executive Office of the President of the United States, *Executive Order on Ensuring Responsible Development of Digital Assets* (Washington, DC: White House, 2022), online: <bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets>.

Financial Transactions and Reports Analysis Centre of Canada, *Financial Transactions and Reports Analysis Centre of Canada* (Ottawa: FINTRAC, 2020), online: <fintrac-canafe.canada.ca/intro-eng>.

Office of the Superintendent of Financial Institutions, *Capital and Liquidity Treatment of Crypto-Asset Exposures (Banking) – Guideline* (Ottawa: OSFI, 2025), online: <osfi-bsif.gc.ca/en/guidance/guidance-library/capital-liquidity-treatment-crypto-asset-exposures-banking-guideline>.

Office of the Superintendent of Financial Institutions, *Guideline B-10: Third-Party Risk Management* (Ottawa: OSFI, 2023), online: <osfi-bsif.gc.ca/en/guidance/guidance-library/third-party-risk-management-guideline>.

Ontario Securities Commission, *OSC Takes Action Against Second Non-Compliant International Crypto Asset Trading Platform* (Toronto: OSC, 2021), online: <osc.ca/en/news-events/news/osc-takes-action-against-second-non-compliant-international-crypto-asset-trading-platform>.

Ontario Securities Commission, *QuadrigaCX: A Review by Staff of the Ontario Securities Commission* (Toronto: OSC, 2020), online: <osc.gov.on.ca/quadrigacxreport>.

United States, Commodity Futures Trading Commission, *Digital Assets* (Washington, DC: CFTC, 2025), online: <cftc.gov/digitalassets/index>.

United States, Internal Revenue Service, *Digital Assets* (Washington, DC: IRS, 2025), online: <irs.gov/filing/digital-assets>.

United States, Internal Revenue Service, *About Form 8949, Sales and Other Dispositions of Capital Assets* (Washington, DC: IRS, 2023), online: <irs.gov/forms-pubs/about-form-8949>.

US Securities and Exchange Commission, *Enforcement Actions: Crypto Assets* (Washington, DC: SEC, 2025), online: <sec.gov/about/divisions-offices/division-enforcement/cyber-crypto-assets-emerging-technology/enforcement-actions>.

SECONDARY MATERIALS: MONOGRAPHS

Organisation for Economic Co-operation and Development, *International Standards for Automatic Exchange of Information in Tax Matters: Crypto-*

Asset Reporting Framework and 2023 update to the Common Reporting Standard (Paris: OECD Publishing, 2022), DOI: <10.1787/896d79d1-en>.

SECONDARY MATERIALS: JOURNAL ARTICLES

Arner, Douglas W et al, “The Financialisation of Crypto: Designing an International Regulatory Consensus” (2024) 53 *Computer L & Security Rev* 105970, DOI: <10.1016/j.clsr.2024.105970>.

SECONDARY MATERIALS: BOOK CHAPTERS

Emmert, Frank, “Blockchain and Private International Law: The Perspective of the United States of America” in Matthias Lehmann, ed, *Blockchain and Private International Law* (Leiden: Brill Nijhoff, 2023) 709, DOI: <10.1163/9789004514850_025>.

SECONDARY MATERIALS: NEWS

Wang, Tracy, “Binance Announces Exit from Canada, Citing Regulatory Tensions” *Coindesk* (15 May 2023), online: <coindesk.com/business/2023/05/12/binance-announces-exit-from-canada-citing-regulatory-tensions>.

SECONDARY MATERIALS: ELECTRONIC SOURCES

BDO Canada LLP, “The CRA’s Position on Cryptocurrency: Income Tax Implications” (Mar 2022), online: <bdo.ca/insights/cra-cryptocurrency-implications>.

Canadian Investment Regulatory Organization, “CIRO Proposes New Guidance for Order Execution Only Dealers” (12 Aug 2025), online: <ciro.ca/newsroom/publications/ciro-proposes-new-guidance-order-execution-only-dealers>.

Canadian Securities Administrators, “CSA Staff Notice 21-332 Crypto Asset Trading Platforms: Pre-Registration Undertakings – Changes to Enhance Canadian Investor Protection” (22 Feb 2023), online: <osc.ca/en/securities-law/instruments-rules-policies/2/21-332/csa-staff-notice-21-332-crypto-asset-trading-platforms-pre-registration-undertakings-changes>.

Canadian Securities Administrators, “Staff Notice 21-330 Guidance for Crypto-Trading Platforms - Requirements relating to Advertising, Marketing and Social Media Use” (23 Sep 2021), online: <osc.ca/en/securities-

law/instruments-rules-policies/2/21-330/csa-iiroc-staff-notice-21-330-guidance-crypto-trading-platforms-requirements-relating-advertising>.

Canadian Securities Administrators, “Regulation of Crypto Assets” (17 Nov 2022), online: <securities-administrators.ca/investor-tools/crypto-assets/regulation-of-crypto-assets>.

Financial Action Task Force, “The FATF Recommendations” (Jun 2025), online: <fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations>.

Financial Action Task Force, “Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers” (28 Oct 2021), online: <fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021>.