

Secondary Market Misrepresentation in Crypto: Insights from the Ontario Superior Court of Justice

September 27, 2026

A recent decision by the Ontario Superior Court of Justice in *Banach v. Galaxy Digital Holdings Ltd.*, 2026 ONSC 4534 is emerging as a critical reference point for digital asset investors, class actions, and corporate disclosure obligations. The judgment establishes decisive principles regarding secondary market misrepresentations, the assessment of materiality for cryptocurrency disclosures, and the liability associated with the promotion of algorithmic stablecoins. The ruling also sheds light on the broader implications for the permissibility and opportunity of class action crypto disputes globally. **Background** The precedent case arose from a class action against Galaxy Digital Holdings Ltd. ("Galaxy"), an investment company heavily engaged in the digital asset industry, and its senior management. The plaintiff alleged that Galaxy failed to disclose material risks associated with its core digital asset holdings, specifically Luna and its associated algorithmic stablecoin, TerraUSD. Between May 2021 and May 2022, Galaxy's CEO heavily promoted Luna. However, in May 2022, Luna and TerraUSD entered a "death spiral," wiping out \$40 billion in market value globally, which resulted in a 42.9% drop in Galaxy's share price and a \$300 million quarter-to-date loss.

The plaintiff claimed that Galaxy's public disclosures during the class period contained misleading omissions regarding the operation and inherent risks of the Terra blockchain and algorithmic stablecoins, particularly the risk of a "death

spiral,” whilst simultaneously selling their Luna holdings.

The Court’s Key Findings The Ontario Superior Court granted the plaintiff leave to proceed under the Ontario Securities Act and certified the action as a class proceeding. The Court’s detailed judgment provided several critical findings:

- **Materiality Exceeds Strict Percentages:** The defendants argued that Luna was a relatively small portion of Galaxy’s total portfolio during most of the class period and was therefore not legally material. The Court rejected this quantitative defense in full. It held that the test for materiality is whether the omitted information would significantly alter the “total mix of information” available to a reasonable investor. The intense promotional campaign by Galaxy’s CEO made Luna fundamentally material to the company’s valuation in the eyes of the market, demonstrating that risks cannot be ignored based on percentage alone.
- **Public Corrections:** Following the collapse of Luna, the CEO issued public statements acknowledging the risks of algorithmic stablecoins and the resulting losses. The defendants dismissed these as *ex post facto* musings. However, the Court categorized these statements as actionable “public corrections,” revealing to the market the material facts and risks that Galaxy was obligated to disclose all along.

Comparing Permissibility of Class Action Crypto Disputes in Global Jurisdictions The *Banach* decision highlights Canada’s permissive “opt-out” class action regime, which seamlessly aggregates massive retail investor claims. For digital asset issuers and exchanges operating globally, the permissibility of class action crypto disputes varies drastically across other major jurisdictions:

- **London (England & Wales):** The English legal system does not possess a direct equivalent to the North American opt-out class action for securities fraud. Claimants

generally rely on Group Litigation Orders (GLOs) under the Financial Services and Markets Act (FSMA) or representative actions. GLOs operate on an “opt-in” basis, requiring upfront funding from each claimant. Representative actions require all claimants to share the “same interest,” making it exceedingly difficult to aggregate the claims of retail investors who purchased digital assets at varying times and prices.

- **Hong Kong & Singapore:** Neither Hong Kong nor Singapore currently supports a statutory class-action regime. Mass claims are limited to traditional representative proceedings, which mandate a rigid “same interest” test. Consequently, mass retail actions over crypto market misrepresentations face significant procedural hurdles. These jurisdictions heavily favor bilateral commercial litigation and institutional arbitration for digital asset disputes, limiting the threat of plaintiff-driven mass securities torts.
- **DIFC (Dubai) & ADGM (Abu Dhabi):** As leading offshore common law jurisdictions in the Middle East, the DIFC and ADGM provide highly sophisticated courts capable of handling complex digital asset disputes. While they offer mechanisms for group litigation, these operate on an opt-in basis. Neither jurisdiction permits the sweeping, opt-out class actions seen in Ontario, thereby providing an efficient venue for organized institutional investors but inherently shielding token issuers from the asymmetric exposure of North American retail class actions.

Looking Ahead The Ontario Court’s decision serves as a definitive warning that generic risk disclosures are insufficient for complex digital assets and that public promotional activities can elevate an asset’s legal materiality. Categorizing bespoke digital assets under generic umbrellas constitutes a material misrepresentation if unique structural risks are omitted. For global practitioners and

stakeholders operating in this space, navigating the distinct procedural realities of global financial hubs will be essential for effective collective redress and mitigating exposure to class actions.

Author: Mahmoud Abuwaseel

Title: Partner – Disputes

Email: mabuwaseel@waselandwaseel.com

Profile:

<https://waselandwaseel.com/about/mahmoud-abuwaseel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseel.com

business@waselandwaseel.com

Enforcing Arbitral Awards After the Abolition of the DIFC-LCIA: The Ontario Court of Appeal's Pragmatic Approach

September 27, 2026

The abrupt abolition of the Dubai International Financial Centre Arbitration Institute (the DIFC-LCIA Arbitration Centre) by the government of Dubai in September 2021 left the international dispute resolution community with a pressing dilemma. With the enactment of “Decree 34,” the rights and obligations of the DIFC-LCIA were transferred to the Dubai International Arbitration Centre (DIAC). This raised a critical question: does the extinguishing of the DIFC-LCIA structure prejudice the enforcement of an award rendered under the substituted DIAC rules, when the underlying contract explicitly referenced the now-defunct DIFC-LCIA provisions?

Recently, the Court of Appeal for Ontario provided a clear answer for Canada (or at least Ontario) in its unanimous decision, *InFrontier AF LP v. Rahmani*, 2026 ONCA 289. The Court confirmed that the dissolution of the DIFC-LCIA structure does not inherently prejudice the enforcement of an award, charting a thoughtful path forward based on contractual interpretation.

The Background of the Dispute

The dispute arose from a September 2020 Term Loan Agreement involving a United Kingdom-based private equity firm, InFrontier AF LP, and Rozen Rahmani, who guaranteed a substantial loan. The parties explicitly agreed that disputes were to be resolved by arbitration in the Dubai International Financial Centre under the DIFC-LCIA Rules.

By the time the respondent commenced arbitration proceedings in 2023 for an alleged default, Decree 34 had abolished the DIFC Arbitration Institute. A joint press release by DIAC and the London Court of International Arbitration subsequently confirmed that arbitrations commenced after March 21, 2022, under agreements referencing the DIFC-LCIA Rules, would be administered under the new DIAC Rules.

Over the appellant's objections, the arbitration was conducted under the DIAC Rules, culminating in an award ordering him to pay over \$2.5 million USD. When the respondent sought to recognize and enforce this award in Ontario, the appellant resisted. Relying on Article V 1(d) of the New York Convention, he argued that the arbitral procedure "was not in accordance with the agreement of the parties" because they had contracted for the DIFC-LCIA Rules, not the DIAC Rules.

The Court's Analysis: Contractual Interpretation

Writing for the Court, Justice Zarnett upheld the enforcement of the award. Rather than viewing the application of the DIAC Rules as an unlawful override by a foreign state, the Court

framed the issue primarily as a matter of contractual interpretation.

Justice Zarnett observed that the application judge “did not, contrary to the Convention, allow the law of the place of arbitration to oust or override the parties’ agreement as to the applicable procedure. Rather, he interpreted their agreement to determine what procedure they had agreed to.” The Court closely examined the Preamble to the DIFC-LCIA Rules, which provided that agreeing parties were bound by those rules or “such amended version of those rules as the DIFC-LCIA Arbitration Centre may have adopted hereafter to take effect before the commencement of the arbitration”.

Addressing the appellant’s concern that relying on Dubai law to determine the applicable rules was improper, the Court respectfully disagreed. Justice Zarnett explained that “the parties’ Agreement about procedure makes the law of the place of arbitration relevant to the question of what rules the parties agreed to.” Because the parties had agreed to an evolving framework, the application judge was entitled to consider the foreign decree to determine that the DIAC Rules legally constituted the amended version of the DIFC-LCIA Rules.

The Court also dismissed the appellant’s public policy arguments, recalling the high threshold required: “to succeed on [the public policy ground] the award must fundamentally offend the most basic and explicit principles of justice and fairness in Ontario, or evidence intolerable ignorance or corruption on the part of the Arbitral Tribunal.”

Global Perspectives: A Fractured Consensus

The Ontario Court of Appeal’s decision is particularly noteworthy when viewed alongside judgments from other jurisdictions grappling with the exact same institutional transition. As the Court politely acknowledged in a footnote,

the international consensus remains fractured.

The courts of Singapore have taken a restrictive view. In *DFL v DFM*, [2024] SGHC 71 (affirmed at [2024] SGCA 41), the Singaporean judiciary viewed the differences between the two sets of rules as significant, demonstrating a reluctance to enforce awards where parties were subjected to a substituted institutional framework.

Conversely, the United States Court of Appeals for the Fifth Circuit adopted a pro-enforcement stance in *Baker Hughes Saudi Arabia Company Limited v. Dynamic Industries, Incorporated*, 126 F (4th) 1073 (5th Cir. 2025), dismissing concerns by characterizing the two sets of rules as “nearly identical.”

Ontario has charted a sophisticated middle ground. By rooting its decision firmly in the contractual interpretation of the phrase “such amended version,” the Court of Appeal elegantly sidestepped the need to conduct a comparative analysis of the institutional rules. As Justice Zarnett noted regarding the debate over whether the rules were materially different or nearly identical, “In view of the conclusion above, it is unnecessary to consider either question.”

Conclusion

With *InFrontier AF LP v. Rahmani*, the Court of Appeal for Ontario has provided a straightforward and commercially sensible judgment. By meticulously interpreting standard institutional preambles to encompass state-mandated amendments, the Court successfully ensured that the extinguishing of the DIFC-LCIA structure does not prejudice the enforcement of arbitral awards in Canada. It is a welcome decision that respects party autonomy while offering a practical solution to unexpected shifts in international dispute resolution.

Author: Mahmoud Abuwaseel
Title: Partner – Disputes
Email: mabuwaseel@waselandwaseel.com
Profile:
<https://waselandwaseel.com/about/mahmoud-abuwaseel/>

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwaseel.com
business@waselandwaseel.com

Piercing the Blockchain Veil: The Ontario Court's Novel Pushback on Crypto Norwich Orders (Compared with the UK and DIFC)

September 27, 2026

Introduction: The Maturation of Crypto Asset Recovery

As digital asset markets expand, global courts are increasingly tasked with untangling complex, cross-border cryptocurrency disputes. When tokens are misappropriated, the immediate legal reflex for claimants is to pierce the pseudonymity of the blockchain. Universally, litigators have turned to the *Norwich Pharmacal* order (or *Bankers Trust* order), an equitable pre-action discovery tool used to compel innocent third parties, such as cryptocurrency exchanges, to disclose user identities and wallet transaction histories.

In recent years, jurisdictions like the United Kingdom (UK) and the Dubai International Financial Centre (DIFC) have adapted these common-law remedies to the speed of the digital era, granting disclosure orders against global exchanges to freeze and trace stolen crypto. However, a novel judgment from the Ontario Superior Court of Justice in May 2026, *Nivora*

Group LLC v. Ping et al., 2026 ONSC 2943, signals a critical procedural divergence.

By refusing to grant a Norwich order against major crypto exchanges in a multi-million-dollar token dispute, the Ontario court has established a strict procedural boundary: the novel nature of cryptocurrency does not grant litigants reason to bypass traditional rules of civil discovery.

The Ontario Approach: Striking a Balance Between Discovery and Privacy

The *Nivora* case involved a cross-border dispute over the creation and distribution of a “meme coin” known as TDCCP. The plaintiffs, corporate entities based in the UAE and the US, alleged that the Canadian developers of the token misappropriated over \$6.2 million USD worth of Solana (SOL) and USDC, funneling the assets into wallets controlled by the defendants via the Kraken and VirgoCX exchanges.

To trace the ultimate destination of these funds, the plaintiffs sought a Norwich order compelling the exchanges to produce the wallet owners’ identities and transaction records.

The Ontario Superior Court dismissed the motion, providing a rigorous check on the bounds of equitable relief. While the Court confirmed the modern reality that Norwich orders *can* legally be made against cryptocurrency exchanges (equating them to traditional financial institutions), it strictly applied the equitable test for necessity.

The novelty of the Ontario Court’s decision lies in its refusal to treat a crypto dispute as inherently exempt from standard civil procedure. The Court denied the order on several key grounds:

1. **The “Known Defendant” Distinction:** In most crypto hacks, the perpetrators are anonymous “John Does,” making an exchange the *only* practical source of information. In

Nivora, the plaintiffs knew exactly who the defendants were, had already sued them, and the defendants were participating in the litigation.

2. **Circumvention of Standard Discovery:** The Court emphasized that a Norwich order is an “intrusive and extraordinary remedy,” not a cost-saving shortcut. Because the plaintiffs could seek the same information through standard pre-trial discovery (or via an Ontario Rule 30.10 motion for third-party production), the Norwich application was deemed an improper attempt to bypass the normal litigation regime.
3. **The *Mareva* Litmus Test:** A hallmark of urgent crypto tracing is the *ex parte* Norwich application paired with a *Mareva* (freezing) injunction to prevent the rapid dissipation of digital assets. The plaintiffs in *Nivora* waited months to bring the motion, brought it on notice to the defendants, and did not seek a freezing order. The Court noted that if the assets were truly at high risk of dissipation, they likely would have already vanished due to the delay. Thus, the privacy interests of unknown third-party wallet holders outweighed the plaintiffs’ demand for immediate disclosure.

The UK Stance: The Proactive Standard for “Persons Unknown”

The Ontario ruling presents a stark contrast to the highly proactive stance of the English Commercial Courts. In the UK, judges view the speed and borderless nature of blockchain transactions as an existential threat to asset recovery.

While the UK courts apply a similar necessity test, their jurisprudence is heavily geared toward the “persons unknown” jurisdiction. English courts routinely issue *ex parte* Norwich Pharmacal and Bankers Trust orders against out-of-jurisdiction exchanges specifically to strip the pseudonymity of hackers. Recognizing the commercial reality of crypto tumbling and mixing, the UK courts frequently attach gagging orders to prevent platforms from tipping off the account holders,

followed immediately by worldwide freezing injunctions.

The DIFC Perspective: Agility and the “Enforcement Principle”

Parallel to London, the DIFC Courts in Dubai have positioned themselves as a highly agile and pragmatic forum for digital asset tracing, applying English common-law principles through the lens of regional commercial realities.

Supported by robust statutory frameworks, the DIFC Courts actively utilize injunctions and disclosure orders to prevent bad actors from moving assets beyond the reach of justice. The DIFC’s willingness to support cross-border tracing is rooted deeply in its mandate to support international enforcement and prevent the thwarting of jurisdictional reach.

This is clearly illustrated in the recent DIFC Digital Economy Court judgment, *Techteryx Ltd v Aria Commodities DMCC [2025] DIFC DEC 001*. While assessing the continuation of sweeping proprietary and worldwide freezing injunctions (WFOs) involving hundreds of millions of dollars in allegedly misappropriated stablecoin reserves, H.E. Justice Michael Black KC emphasized the rationale for deploying such powerful interim remedies in aid of foreign proceedings:

“The object of the policy of the ‘Enforcement Principle’... is to prevent the jurisdiction of the primary court from being thwarted... the Court must determine (1) whether there is a sufficient likelihood that a judgment enforceable through the process of the DIFC Courts will be obtained, and (2) a sufficient risk that without a freezing injunction execution of the judgment will be thwarted, to justify the grant of relief.”

For the DIFC Courts, if a claimant can demonstrate a good arguable case of fraud and a real risk of dissipation, the court is highly likely to deploy its equitable arsenal, including WFOs and disclosure orders against digital asset platforms, to ensure that the ultimate judgment is not

rendered hollow by the blockchain's speed. However, as the Ontario ruling cautions, these tools must be tethered to actual urgency and the prevention of thwarted jurisdiction, not abused as shortcuts to standard discovery.

Strategic Takeaways for Cross-Border Crypto Disputes

As global courts continue to adapt their traditional equitable frameworks to the cross-jurisdictional novelties of Web3 litigation, the contrast between the *Nivora* judgment and the approaches of courts in the UK and the DIFC provides a valuable strategic guide for managing international crypto disputes:

- **Sequencing Discovery Based on Defendant Identity:** The identity and litigation status of the alleged wrongdoer play a significant role in determining the appropriate discovery mechanism. In scenarios involving anonymous actors or "persons unknown," an equitable disclosure order against an exchange is often an essential tool for tracing. However, where defendants are known and actively participating in the litigation, parties must proactively assess whether standard civil discovery or conventional domestic third-party production rules should be pursued prior to seeking extraordinary equitable relief, as some forums will strictly require the exhaustion of these standard avenues first.
- **Synchronizing Interim Relief with Case Objectives:** Courts rigorously balance a claimant's need for information against the privacy rights of third-party account holders. When a disclosure application is based on the high risk of rapid crypto dissipation, parties should carefully align their procedural steps with that stated risk. Evaluating whether an *ex parte* application coupled with asset preservation measures, such as a worldwide freezing order (WFO) or *Mareva* injunction, is procedurally appropriate can help present a cohesive

narrative of immediate urgency and necessity to the presiding adjudicator.

- **Navigating Forum-Specific Equitable Thresholds:** While blockchain technology is inherently borderless, the legal remedies to trace and recover digital assets remain distinctly territorial. The global landscape for crypto asset tracing is not uniform; forums like the DIFC and the UK High Court have developed jurisprudence emphasizing the “Enforcement Principle” to facilitate rapid third-party disclosure and prevent the thwarting of jurisdictional enforcement. Conversely, other common-law jurisdictions may place equal or greater weight on the strict sequence of standard civil procedure and third-party privacy. Parties must map their asset recovery strategies to the specific evidentiary, equitable, and procedural thresholds of the chosen forum to optimize their prospect of recovery.

Wasel & Wasel advises on complex commercial disputes, international arbitration, and digital asset litigation. The firm possesses deep expertise in navigating cross-border fraud, tracing misappropriated funds, and securing interim equitable relief such as worldwide freezing injunctions and disclosure orders. By bridging the gap between local procedural frameworks and global common-law standards, Wasel & Wasel provides robust representation for corporate entities, tech developers, and international investors operating within the digital economy.

Author: Mahmoud Abuwasel

Title: Partner – Disputes

Email: mabuwasel@waselandwasel.com

Profile:

<https://waselandwasel.com/about/mahmoud-abuwasel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwasel.com

business@waselandwasel.com

Artificial Intelligence Hallucinations in Arbitration: Analyzing the Landmark Award Annulment in *ARIHQ c. Santé Québec*

September 27, 2026

The advent of generative artificial intelligence (AI) has brought unprecedented capabilities and efficiencies to the legal profession. However, alongside its benefits come profound risks, particularly when AI is employed in adjudicative decision-making. The recent landmark ruling by the Quebec Superior Court in *Association des ressources intermédiaires d'hébergement du Québec (ARIHQ) c. Santé Québec* (2026 QCCS 1360) serves as a stark warning to the international and domestic arbitration communities. In an unprecedented move, the Court annulled an arbitral award after finding that the sole arbitrator had implicitly delegated his decision-making authority to a generative AI tool, which resulted in the inclusion of “hallucinated” jurisprudence and legal doctrine.

This article unpacks the *ARIHQ* judgment, explores the comparative international grounds for setting aside such awards under the New York Convention and the UNCITRAL Model Law, surveys the growing global judicial consensus on AI, and proposes practical safeguards for inclusion in arbitration agreements and Terms of Reference.

The Judgment: *ARIHQ c. Santé Québec*

The dispute originated from an unpaid retroactive remuneration claim between a healthcare intermediary resource (Osman) and a Montreal health authority (CCSMTL, now Santé Québec). An arbitrator dismissed the claim on preliminary grounds, ruling that the contractual notice periods had expired. The claimants sought to annul the award before the Quebec Superior Court, relying on two grounds: first, that the award violated public policy by modifying statutory prescription periods; and second, that the arbitral procedure was not respected because the arbitrator relied on non-existent legal authorities, strongly suggesting the use of generative AI.

The Honourable Martin F. Sheehan swiftly dismissed the public policy argument, affirming the well-established principle that a mere error of law—even concerning public policy provisions—does not justify setting aside an arbitral award unless the outcome itself is fundamentally repugnant to public order.

However, the Court decisively upheld the procedural challenge. Reviewing the award, the Court verified that the central doctrinal and jurisprudential authorities cited by the arbitrator to support the validity of the forfeiture clause simply did not exist. The arbitrator had referenced a fabricated doctrinal article by a real author and hallucinated judgments ostensibly from the Quebec Court of Appeal and the Superior Court (e.g., fictitious citations for *Ville de Montréal c. Syndicat des cols bleus* and *Tremblay c. Commission scolaire de la Jonquière*).

The Court emphasized the *intuitu personae* nature of arbitration—the principle that an arbitrator is chosen for their personal expertise, judgment, and authority. Relying on an AI tool to formulate the substantive reasoning without verifying the output violated the fundamental maxim *delegatus non potest delegare* (a delegate cannot delegate) and breached the secrecy of deliberations.

Translating the crucial analytical and operative parts of the judgment, Justice Sheehan concluded:

“The preponderance of the evidence therefore leads to the conclusion that the Arbitrator’s authority was delegated and that he abdicated his role to review the result. This conclusion is inevitable given that all of the doctrinal and jurisprudential references on which the Arbitrator relies are non-existent and ‘hallucinated’. For this reason, the Award must be annulled.”

The Court, however, added a critical caveat: not every use of AI will automatically lead to annulment. If the AI usage is minimal, or if the hallucinated references do not form the crux of the reasoning, the award might survive if the breach did not fundamentally taint the proceedings. But in this case, the breach struck at the very heart of the arbitrator’s reasoning and affected the confidence of the parties in the arbitration regime.

The operative part (*dispositif*) reads:

“FOR THESE REASONS, THE COURT: ANNULS the arbitral award rendered on August 8, 2025, by the impleaded party, Mr. Michel A. Jeanniot; ORDERS the parties to choose a new arbitrator within 60 days of this judgment; THE WHOLE, with legal costs.”

Domestic Set-Aside Grounds and Comparative International Frameworks

The Quebec Code of Civil Procedure (C.C.P.) is deeply influenced by the UNCITRAL Model Law, making this judgment highly instructive for international practitioners. The Court annulled the award under Article 646(3) of the C.C.P., which allows set-aside where “the applicable arbitral procedure was not respected.”

The UNCITRAL Model Law and the New York Convention

Under Article 34(2)(a)(iv) of the UNCITRAL Model Law, and identically under Article V(1)(d) of the New York Convention, an award may be set aside or refused enforcement if “the arbitral procedure was not in accordance with the agreement of the parties.”

When parties agree to arbitrate, they contract for a bespoke dispute resolution process wherein a specific human tribunal exercises independent intellectual judgment. The use of an unverified Large Language Model (LLM) to draft the award’s substantive reasoning is a structural deviation from this agreed procedure. Furthermore, feeding confidential submissions into a public AI tool violates the confidentiality and secrecy of deliberations inherent in arbitration.

The Public Policy Exception

While the Quebec Court dismissed the substantive public policy argument, an award heavily reliant on AI hallucinations could trigger the procedural public policy exception under Article 34(2)(b)(ii) of the Model Law and Article V(2)(b) of the New York Convention. An award anchored in fabricated law deprives the losing party of the right to a fair hearing and the opportunity to present its case (*audi alteram partem*). The parties cannot possibly address or distinguish phantom precedents during the proceedings. Enforcement courts in major hubs like London, New York, or Singapore would view the abdication of the adjudicative function to a “black box” algorithm as a severe affront to fundamental notions of justice, procedural fairness, and due process.

Global Court Directions on AI Usage in Proceedings

The *ARIHQ* judgment resonates with an emerging global judicial consensus that demands strict guardrails around the use of generative AI in dispute resolution. Courts and tribunals worldwide have recently confronted the consequences of “AI hallucinations” and have responded with firm directives.

United States

The U.S. has been ground zero for AI in litigation, notably following the infamous *Mata v. Avianca* case, where lawyers were sanctioned for submitting AI-generated fictitious case law. Consequently, numerous federal and state judges have issued standing orders. These orders typically mandate that counsel file a certificate attesting that no generative AI was used in drafting, or that if it was, a human attorney rigorously verified the accuracy of all citations and legal propositions. The focus is squarely on human accountability and preventing the waste of judicial resources on fabricated jurisprudence.

United Kingdom

In late 2023, the UK Courts and Tribunals Judiciary issued official guidance for judicial office holders. While acknowledging the utility of AI for administrative tasks, the guidance explicitly warns judges about the severe risks of hallucinations and deepfakes. The UK Master of the Rolls has emphasized that judges remain personally responsible for their judgments and must not delegate legal analysis or substantive drafting to AI tools, safeguarding the integrity of the “judicial mind.” Furthermore, it firmly warns against entering any confidential case information into public AI chatbots.

Middle East (QFC and ADGM)

Progressive commercial courts in the Middle East have taken decisive action against AI misuse. In the Qatar Financial Centre (QFC), the Civil and Commercial Court’s late-2025 judgment in *Sheppard v Jillion LLC* found a lawyer in contempt for repeatedly citing AI-generated fake cases. This prompted the QICDRC to issue Practice Direction No. 1 of 2026, which established a comprehensive framework requiring lawyers to independently verify AI-generated submissions. Similarly, in the Abu Dhabi Global Market (ADGM), the Court in *Arabyads v*

Gulrez Alam [2025] ADGMCFI 0032 ordered severe wasted costs against a legal team that submitted a defense riddled with false, AI-generated legal authorities, concluding that unverified AI use amounts to reckless professional conduct.

Proposed Directions for Terms of Reference and Arbitration Agreements

The *ARIHQ* decision underscores a critical vulnerability: waiting for a court to set aside a tainted award means the parties have already suffered the immense costs and delays of a compromised arbitration. To proactively mitigate these risks, parties should expressly regulate the use of AI in their Arbitration Agreements, or more practically, in the Terms of Reference (ToR) and Procedural Order No. 1 (P01).

Practitioners should consider integrating the following AI protocols:

- **Explicit Prohibition of Delegation:** The ToR should clearly state that the arbitral tribunal must not delegate its adjudicative, analytical, or substantive decision-making functions to any generative AI tool. The arbitrator must assume full, personal responsibility for the reasoning, legal research, and drafting of the award.
- **Permitted Uses and Mandatory Verification (Human-in-the-Loop):** Parties can define acceptable AI use, such as utilizing AI for translation, formatting, or document summarization, provided it does not replace substantive analysis. P01 should include an affirmative obligation for both the tribunal and counsel to strictly verify any AI-assisted output against primary legal sources. The tribunal could be required to issue a “Statement of Human Authorship” within the final award confirming that all citations and factual references have been manually verified.
- **Confidentiality and Data Security Guardrails:** To protect

the secrecy of deliberations and party confidentiality, the ToR must prohibit the uploading of confidential case information, pleadings, or evidence into open-source or publicly accessible generative AI models (e.g., public versions of ChatGPT). Only secure, closed-loop enterprise AI systems that do not retain data for model training should be permitted.

- **Transparency and Disclosure:** If a party intends to rely on materials or legal submissions substantially generated by AI, they should be required to disclose this fact to the tribunal and opposing counsel. Likewise, the tribunal should disclose if AI tools were used for any significant administrative or drafting assistance.

Conclusion

The Quebec Superior Court's annulment of the award in *ARIHQ c. Santé Québec* serves as a defining precedent in the modern era of dispute resolution. It establishes a clear boundary: while technology can enhance the efficiency of the arbitral process, it cannot usurp the human judgment that parties contractually bargained for. As generative AI tools become ubiquitous, the international arbitration community must proactively regulate their use. By embedding robust AI guidelines into Terms of Reference, parties can protect the integrity of their proceedings, safeguard confidentiality, and insulate their awards from the devastating consequences of digital hallucinations.

Author: Mahmoud Abuwasel

Title: Partner – Disputes

Email: mabuwasel@waselandwasel.com

Profile:

<https://waselandwasel.com/about/mahmoud-abuwasel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwasel.com

business@waselandwasel.com

Universal Jurisdiction and the Situs of Centralized Digital Assets: An Analysis of Crypto Server Location in *Iakovlev v. Epayments Systems Ltd.* (Ontario Superior Court of Justice)

September 27, 2026

Introduction

In the rapidly expanding world of digital finance, courts face a novel challenge: determining the legal location, or *situs*, of supposedly borderless crypto assets. When a digital asset is lost or stolen on an international platform, where exactly does the legal harm occur? The Ontario Superior Court of Justice recently addressed this critical issue head-on in *Iakovlev v. Epayments Systems Ltd.*, 2026 ONSC 1296.

In a decision that will undoubtedly resonate across global legal frameworks, Associate Justice R. Frank granted a motion by the defendant, ePayments Systems Limited, “for an order dismissing the plaintiff’s claim as against it on the basis that this court has no jurisdiction over it.”

The ruling firmly rejects the notion that the residency of a crypto owner dictates the jurisdiction of the digital asset. More importantly, it tackles the technological realities of centralized crypto custody, providing much-needed clarity and a formidable defense against judicial overreach in cross-border crypto disputes.

The Dispute and the Question of *Situs*

In this action, “the plaintiff seeks damages for alleged misrepresentation and civil conspiracy,” claiming that “due to the bankruptcy of DSX Global, the plaintiff has been deprived of the six bitcoins he purchased.” The plaintiff attempted to establish assumed jurisdiction in Ontario by arguing that “his retirement savings, an Ontario-based asset, were the source of the funds invested on the platform,” and therefore, he suffered financial loss in his home province.

Under Canadian common law, “an actionable conspiracy occurs in the jurisdiction where the alleged harm is suffered, regardless of where the wrongful conduct occurred.” Therefore, the Court had to determine exactly where the legal harm involving the loss of the digital assets took place.

Paragraph 47: Defining the Location of Digital Assets

Associate Justice R. Frank systematically dismantled the plaintiff’s argument that localized financial impact equates to localized legal harm. In paragraph 47, the Court provided a profound analysis of the location of digital assets, prioritizing the physical infrastructure and the custodial entity over the domicile of the investor:

“[47] Further, even if some or all of the funds used by the plaintiff to purchase the allegedly lost crypto assets had originated in Ontario – which is not supported by the evidence – the plaintiff’s digital assets were held on servers in the European Union. Those crypto assets were never held on servers in Ontario or anywhere in Canada, nor were they held by or through an entity located in or with any connection to Ontario or Canada. As such, the alleged harm and loss did not occur in Ontario.”

The Court highlighted the extreme danger of adopting the plaintiff’s logic, warning that it would effectively subject

global platforms to litigation everywhere simply because their users are distributed worldwide:

“If the plaintiff’s position were accepted and taken to its logical conclusion, then damages would occur in Ontario whenever an Ontario resident suffers a loss of one of their assets located outside Ontario, regardless of whether the asset has any connection to Ontario other than its ownership by the Ontario resident. In my view, the fact that an Ontario resident suffers a loss of or damage to an asset located outside Ontario does not, on its own, mean that the harm occurs in Ontario. That would be akin to universal jurisdiction, a result that the Supreme Court has cautioned against in Van Breda.”

The Technical Reality vs. The “Borderless” Myth: Anchoring Crypto to Servers

To fully appreciate the weight of the Court’s ruling, one must understand the technical tension at the heart of the digital asset industry. In the mainstream consciousness, cryptocurrencies like Bitcoin are frequently championed as strictly “borderless”, built on decentralized, globally distributed public ledgers where the underlying assets theoretically exist everywhere and nowhere simultaneously.

However, *Iakovlev* introduces a vital technical distinction by piercing this “borderless” myth in the context of centralized platforms and payment gateways. When an investor purchases cryptocurrency on a centralized platform like DSX Global or uses a service like ePayments, they are not usually holding the private keys directly on the decentralized public blockchain. Instead, they hold a custodial right, an IOU, recorded on the platform’s proprietary, centralized internal databases.

Justice Frank acutely recognized this technical reality. By explicitly observing that “the plaintiff’s digital assets were

held on servers in the European Union” and “never held on servers in Ontario,” the Court established a tangible, physical nexus based on the technological hardware managing the platform’s internal database. The court brilliantly bridged the gap between decentralized technology and traditional legal geography by tethering the *situs* of the asset to these physical servers, and the fact that they were never “held by or through an entity located in” Ontario. It aligned legal jurisdiction with the technical reality of centralized digital asset custody infrastructure, rather than the abstract, borderless nature of the blockchain protocol.

Global Ramifications and Effects on Common Law Jurisdictions

The global ramifications of *Iakovlev* are immense. By ruling that a platform’s “presence in Ontario was virtual only, and passive,” and by anchoring the *situs* of digital assets to the jurisdiction where they are “held on servers” or “held by or through an entity,” the Court has erected a powerful shield against forum shopping across the digital asset industry.

Because the legal geography of cryptocurrency is still actively being mapped, this physical infrastructure-based precedent will heavily influence other major common law and international financial hubs:

- **The United Kingdom (UK):** English courts have frequently grappled with the *lex situs* of crypto assets. In earlier rulings, UK courts have suggested that a crypto asset is legally located where its owner is domiciled. *Iakovlev* introduces a compelling counter-approach. By stating that “the fact that an Ontario resident suffers a loss... does not, on its own, mean that the harm occurs in Ontario,” the Canadian court directly challenges the domicile-based model. UK litigators defending foreign Virtual Asset Service Providers (VASPs) will undoubtedly cite *Iakovlev* to argue that the true *situs* of custodial assets lies with the centralized server infrastructure

and the hosting entity, not the claimant's residence.

- **Singapore and Hong Kong:** As premier crypto hubs in Asia, Singapore and Hong Kong have definitively recognized cryptocurrencies as property capable of being held in trust. However, identifying the geographical nexus for cross-border torts remains highly contested. *Iakovlev* provides the legal certainty that centralized platforms operating in these regions desire. If an exchange incorporated in Singapore or Hong Kong stores client assets on local servers, *Iakovlev* provides highly persuasive authority that foreign plaintiffs cannot easily sue these exchanges in their home countries just because the “borderless” assets were accessed globally.
- **DIFC and ADGM (United Arab Emirates):** The Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM) operate under English common law principles and have enacted bespoke, entity-focused digital asset property laws to attract Web3 businesses. The *Iakovlev* judgment inherently strengthens their jurisdictional appeal. By reinforcing that digital assets are tied to where they are “held by or through an entity located in” a specific region, digital asset firms licensed within the DIFC or ADGM can be confident that international courts will respect these hardware and corporate boundaries, preventing foreign users from bypassing UAE forums based solely on localized economic harm.
- **Australia:** Australian courts apply strict “real and substantial connection” tests for assumed jurisdiction and are highly cautious regarding extraterritorial overreach. In dealing with class actions or individual claims against international crypto exchanges, Australian courts will find the *Iakovlev* reasoning highly persuasive. The judgment provides a technologically grounded metric, the location of the

servers, for dismissing claims where the only domestic connection is the plaintiff's residency, preventing Australian courts from exercising what "would be akin to universal jurisdiction."

Conclusion

Iakovlev v. Epayments Systems Ltd. represents a triumph of established jurisdictional principles and technological pragmatism in the face of decentralized finance. By decisively ruling that the physical location of servers and custodial entities dictates the legal location of digital assets, the Ontario Superior Court of Justice has successfully blocked a backdoor to "universal jurisdiction." As common law courts around the globe continue to navigate the complexities of the crypto industry, this judgment stands as a vital reminder: while the blockchain network may be borderless, the corporate infrastructure and servers that hold these assets remain firmly tethered to physical reality.

Author: Mahmoud Abuwaseh

Title: Partner – Disputes

Email: mabuwaseh@waselandwaseh.com

Profile:

<https://waselandwaseh.com/about/mahmoud-abuwaseh/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseh.com

business@waselandwaseh.com

Taxing Unrealized Crypto Gains: Canada's Tax Court Guidance to Global

Policymakers on Crypto Volatility

September 27, 2026

The intersection of digital currency and the tax collector has always been a point of friction, but a recent judgment from the Tax Court of Canada has provided a clarifying jolt to the system. In *Amicarelli v. The King*, 2025 TCC 185, delivered in December 2025, Justice John A. Sorensen stripped away the technological hype of cryptocurrency to reveal its bare economic bones. While the case adjudicated the specific misfortune of a taxpayer caught in the notorious collapse of the QuadrigaCX exchange, the principles articulated in the decision offer a profound warning to global policymakers currently flirting with the taxation of unrealized gains. As nations from the United States to Australia consider expanding their tax nets to capture the paper wealth of the digital age, the *Amicarelli* decision stands as a testament to the dangers of taxing value that can vanish in a heartbeat.

To understand the legal and economic implications, one must start with the asset itself. The court provided a definition of Bitcoin that is remarkable for its clarity and its exclusion of traditional financial attributes. The judgment accepted that Bitcoin “subsists on a blockchain, which is a decentralized and encrypted ledger of information.” It noted that while the asset “exists in a virtual, digital domain,” it lacks the fundamental characteristics of income-generating property. Unlike a bond that pays interest or a stock that yields dividends, the court stated explicitly: “Bitcoin does not generate interest or dividends. It is a medium of exchange and temporary store of value.”

This definition is crucial. It establishes that the only way to make money with Bitcoin, barring some exotic derivative

structure, is through the mechanism of price appreciation. You buy it, you hold it, and you hope it goes up. In the case of Jeanette Amicarelli, she did more than just hope. She engaged in what the court described as “optimistic behaviours” to fund her acquisition of Bitcoin in 2017. She took out a second mortgage at an interest rate of nearly 12 percent, cleared out her retirement savings, and used high-interest credit cards. The court observed that “only a person with a bona fide belief that they were going to enjoy positive financial outcomes would engage in such costly financing.”

Because of this aggressive pursuit of profit, the court ruled that her trading activities constituted an “adventure or concern in the nature of trade.” This legal determination meant that her subsequent loss, nearly half a million dollars that evaporated when QuadrigaCX failed, was a business loss, not a capital loss. The distinction allowed her to deduct the full amount against her other income, a victory for the taxpayer that hinged on the court’s recognition of her intent and the reality of her loss.

However, the deeper lesson of *Amicarelli* lies in its implicit critique of the “mark-to-market” taxation philosophies gaining traction globally. In the United States, political debates have cycled through proposals to tax the unrealized gains of high-net-worth individuals, essentially asking taxpayers to pay cash taxes on the increase in value of their assets, even if those assets haven’t been sold. Similar ideas circulate in the European Union under the guise of wealth equalization, while countries in East Asia and Australia continue to refine the timing of capital gains events.

The *Amicarelli* judgment exposes the peril of these approaches by highlighting the concept of symmetry. Justice Sorensen wrote what should be a guiding maxim for tax authorities everywhere: “Ultimately, to the extent that material profits earned in a market frenzy are fully taxable regardless of the risk profile of the market, losses, including catastrophic

losses, must be given symmetrical treatment.”

Consider the timeline of the *Amicarelli* case through the lens of taxing unrealized gains. In late 2017, the taxpayer’s account balance reportedly swelled to over two million dollars. In a regime that taxes paper wealth, the government might have assessed a massive tax liability on those gains at the end of the fiscal year. Yet, just weeks later, the exchange collapsed, and the balance “inexplicably fallen to nil.” If the taxman had already taken a cut of the two million dollars, the taxpayer would have been left destitute, having paid taxes on wealth she never truly possessed and could never access.

The court’s recognition that cryptocurrency is merely a “temporary store of value” underscores the volatility that makes taxing unrealized gains so dangerous. Assets in this sector are not stable; they are prone to “modern cryptocurrency surges” that the judgment compared to “Dutch tulip mania” or the “dot com bubble.” When a government steps in to tax the upside of a bubble before it bursts, they effectively become a partner in the speculation. The *Amicarelli* decision confirms that if the state wants a share of the “market frenzy,” it must also underwrite the “catastrophic losses” that follow.

Furthermore, the judgment acknowledges the unique risks of the crypto ecosystem. The court accepted that “asset loss due to theft or fraud is a business risk.” In the unregulated “wild west” of digital exchanges, where platforms “operate outside the purview of securities regulators,” wealth is far more precarious than it is in traditional banking. Taxing the theoretical value of a Bitcoin wallet as if it were a savings account ignores the reality that the wallet can be emptied by a hacker or a fraudster in seconds.

In jurisdictions like Japan, where crypto income is often treated as miscellaneous income upon realization, or

Australia, where Capital Gains Tax events are strictly defined by disposal, the tax codes generally align with the “realization” principle upheld in *Amicarelli*. These systems wait until the money is real before asking for a share. The Canadian ruling reinforces the wisdom of this caution. It reminds us that “Bitcoin is property” but it is a distinct, volatile, and intangible form of property that “can even be stolen.”

Ultimately, *Amicarelli v. The King* is a vindication of economic reality over theoretical valuation. The court looked at the taxpayer’s “actual conduct”, her borrowing, her daily monitoring, her “scheme for profit making”, and determined that she was running a business. Because she was running a business, she was entitled to deduct her losses when the business failed due to “malfeasance.”

For global policymakers, the warning is clear. If you rewrite the rules to tax the phantom wealth of a rising market, you must be prepared to refund those taxes when the market crashes or the assets disappear. As Justice Sorensen concluded, the tax system must provide “symmetrical treatment.” Without that symmetry, the tax code becomes a mechanism for confiscation rather than contribution, punishing taxpayers for the ephemeral spikes of a volatile market while offering no shelter when the screen goes black.

Author: Mahmoud Abuwasel

Title: Partner – Disputes

Email: mabuwasel@waselandwasel.com

Profile:

<https://waselandwasel.com/about/mahmoud-abuwasel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwasel.com

business@waselandwasel.com

The Legal Characterization of Cryptocurrency and Contractual Authorization Protocols: Analysis of HoneyBadger Enterprises Ltd. v Bue

September 27, 2026

The judgment of the King's Bench for Saskatchewan in [*HoneyBadger Enterprises Ltd. v Bue*, 2025 SKKB 123](#), provides salient guidance on the interpretation of payment authorization agreements in the context of cryptocurrency transactions and the allocation of loss following third-party fraud. The decision also engages with the persistent question of the legal classification of digital assets under existing statutory frameworks, particularly concerning contract and tort law.

The matter required the Court to adjudicate a dispute between HoneyBadger Enterprises Ltd. ("HoneyBadger"), a cryptocurrency vendor, and the Defendant, a customer. Both parties were victims of a fraud perpetrated by unknown third parties. The Defendant had established a Pre-Authorized Debit (PAD) Agreement with HoneyBadger. Subsequently, \$240,000 CAD was utilized to purchase cryptocurrency, which was transferred to a wallet controlled by the fraudsters. While the Defendant authorized the initial \$40,000 in transactions, he had also granted the fraudsters remote access to his computer. The fraudsters utilized this access to initiate the remaining \$200,000 in purchases via the Defendant's email account,

without his knowledge. The financial institution reversed the payments, leading HoneyBadger to seek recovery.

The Characterization of Cryptocurrency: Contractual and Tortious Implications

A preliminary issue concerned the applicability of *The Sale of Goods Act (Saskatchewan)* (SOGA). The Defendant contended that the contract for the purchase of cryptocurrency was unenforceable under the statute for want of a written agreement. This required the Court to consider whether cryptocurrency constitutes “goods,” defined in the Act as “all chattels personal other than things in action or money.”

Richmond J. observed the inherent difficulty in applying historical legislation to novel asset classes [29]. The judgment referenced jurisprudence reflecting judicial caution in this area, including *Copytrack Pte Ltd. v Wall*, 2018 BCSC 1709, where the court declined to characterize cryptocurrency in a summary proceeding, deeming it a complex and undecided question [30].

The characterization of cryptocurrency is material not only to contract law under SOGA but also to the availability of proprietary torts. The Court cited *Ramirez v Ledn Inc.*, 2023 ONSC 3716, where the Ontario Superior Court held that “Bitcoin is intangible property,” thereby precluding the application of the tort of conversion [31].

This characterization is significant. The tort of conversion is generally restricted to tangible property (chattels personal or choses in possession). If cryptocurrency is classified as intangible property, potentially as a *chose in action*, it not only limits the availability of certain proprietary torts but also places the asset outside the SOGA definition of “goods,” which explicitly excludes “things in action.”

In *HoneyBadger*, the Court ultimately circumvented a definitive

classification. Richmond J. held that regardless of whether cryptocurrency is a “good,” the statutory defence failed because the transactions were evidenced by sufficient memoranda in writing, namely the email exchanges and the PAD Agreement [32].

Contractual Formation and Authorization Protocols

The central contractual dispute concerned the validity of the two unauthorized transactions totaling \$200,000. The Court accepted the evidence that these purchases were initiated by fraudsters impersonating the Defendant [12]. Consequently, there was no objective manifestation of the Defendant’s intention to be bound by those specific agreements.

HoneyBadger argued it had followed the agreed procedure, relying on instructions from the Customer’s established email address, and therefore the Defendant remained contractually bound. HoneyBadger relied upon *Du v Jameson Bank*, 2017 ONSC 2422, where a bank was found not liable for acting on fraudulent instructions received from a customer’s compromised email account.

Richmond J. distinguished *Du* based on the specific contractual terms. In *Du*, the account agreement explicitly authorized the bank to rely on electronic communications purporting to be from the customer and included robust limitation of liability clauses that placed the onus of securing electronic access squarely on the customer [37]. The agreement between HoneyBadger and the Defendant contained no such risk allocation provisions [38].

Conversely, the interpretation of the PAD Agreement proved decisive. Clause 8, addressing sporadic payments, stipulated:

“I/we agree that a password or security code or other signature equivalent will be issued [emphasis added] and will constitute valid authorization...” [24].

The Court found that HoneyBadger's practice of relying solely on incoming emails from the Defendant's address did not satisfy this requirement. The term "issued" implies a positive obligation on the Payee (HoneyBadger) to provide a verification mechanism. An email confirmation originating from the Payor's side does not constitute a security measure "issued" by the Payee [27]. HoneyBadger's reliance on the established pattern of communication did not override the express terms of the PAD Agreement [28].

Allocation of Loss

The case required an adjudication between two victims of fraud. While the Defendant's actions in granting fraudsters access to his computer facilitated the fraud [44], the Court determined that HoneyBadger's non-compliance with Clause 8 was also a direct cause of the loss regarding the unauthorized transactions. Had HoneyBadger implemented the required verification process, the fraud might have been prevented [50].

Applying principles of shared responsibility, the Court distinguished the initial \$40,000, which the Defendant actively authorized. Compliance with the PAD verification requirements would not have altered that outcome. For the remaining \$200,000, the Court found shared responsibility and apportioned the loss equally [55]. This judgment underscores that vendors must rigorously adhere to the security protocols stipulated in their contractual agreements.

The Characterization of Cryptocurrency in General Transactions

The judgment in *HoneyBadger* necessarily engages with the persistent challenge of characterizing cryptocurrency within established legal frameworks governing commercial transactions. While Richmond J. ultimately circumvented a definitive classification by resolving the SOGA defence on evidentiary grounds [32], the legal nature of digital assets

remains a critical issue in contract and tort law.

The difficulty arises from the application of traditional common law categories of personal property, choses in possession (tangible assets capable of physical possession) and choses in action (intangible rights enforceable only by legal action). Cryptocurrency does not fit neatly within these definitions. It is intangible, yet it does not typically represent a claim against a counterparty, distinguishing it from conventional choses in action like debts.

The characterization is material. In contract law, if cryptocurrency is not classified as a “good”, which SOGA defines by excluding “things in action or money” [29], transactions involving its sale are not subject to the statutory implied conditions and warranties regarding title, quality, or fitness for purpose. Parties must instead rely solely on express contractual terms and common law principles governing the transfer of intangibles.

In tort law, the classification dictates the availability of proprietary remedies. As noted in the judgment, citing *Ramirez v Ledn Inc.*, the characterization of Bitcoin as “intangible property” precludes the application of the tort of conversion [31]. Conversion is historically restricted to wrongful interference with tangible chattels. This limits recovery mechanisms in cases of misappropriation, often necessitating reliance on equitable claims such as unjust enrichment or tracing.

In the context of *HoneyBadger*, the cryptocurrency functioned as the subject matter of the sale, akin to a commodity or investment asset, rather than the means of payment (which was fiat currency). The unique features of these assets, specifically their intangibility and the technical irreversibility of transfers once executed on the blockchain [3], heighten the importance of the contractual mechanisms used to facilitate their exchange. The *HoneyBadger* decision

illustrates a pragmatic judicial approach, focusing not on the ontological nature of the asset, but on the interpretation and application of the specific authorization protocols agreed upon by the parties. Absent definitive statutory guidance, the precise terms of the underlying contract remain the primary determinant of risk allocation and liability.

Author: Mahmoud Abuwaseel

Title: Partner – Disputes

Email: mabuwaseel@waselandwaseel.com

Profile:

<https://waselandwaseel.com/about/mahmoud-abuwaseel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseel.com

business@waselandwaseel.com

BC Court of Appeal Affirms Application of Traditional Contract Law to Bitcoin Loan Agreements

September 27, 2026

The British Columbia Court of Appeal's decision in *Tambosso v. Nguyen*, 2025 BCCA 338, provides a salient analysis of how established Canadian contract law principles apply to loan agreements involving cryptocurrency. While the judgment was rendered in chambers on a procedural application to extend time for an appeal, the court's reasons offer significant insight into the judicial treatment of digital asset transactions. The analysis, which required a thorough review of the proposed appeal's merits, affirms that the unique

characteristics of cryptocurrency do not inherently displace foundational legal doctrines concerning contract formation, interpretation, and remedies.

The dispute arose from a short-term loan of cryptocurrency. The respondent loaned a total of 22 Bitcoin (BTC) to the appellant in September 2021. The loan was documented in two written agreements. The purpose of the loan was to facilitate the appellant's participation in a security protocol called the "Bypass Procedure" with a third party, which he believed would yield significant profits.

The contracts contained critical terms. They stipulated that the appellant was to repay the principal loan of 22 BTC within 48 hours, irrespective of the success or failure of the Bypass Procedure. Furthermore, the agreements expressly provided that the respondent would bear no responsibility for the actions or omissions of any third party involved.

The Bypass Procedure ultimately failed, appearing to be a fraudulent scheme perpetrated by the third party. The appellant did not repay the loan. The respondent commenced a civil claim and was granted summary judgment by the Supreme Court of British Columbia for approximately \$1.2 million, representing the value of the 22 BTC, plus interest and costs (*Respondent v. Appellant*, 2024 BCSC 1551). The trial judge found the loan agreements to be valid and enforceable contracts, which the appellant had breached.

The appellant sought to appeal the trial decision. In assessing his application for an extension of time to file his appeal record, the Court of Appeal was required to consider whether the proposed appeal had any prospect of success. The appellant's arguments centered on three primary areas: contract formation, the applicability of certain contractual defenses, and the overarching proposition that the law must adapt to the novel context of cryptocurrency fraud. The Court of Appeal's methodical rejection of these arguments is

instructive.

First, on the issue of contract formation, the appellant contended that no valid contracts existed. He argued that minor, un-initialed deletions he made to the first agreement constituted a counter-offer that the respondent never accepted. He further argued the supplementary agreement was invalid because the respondent had not signed it. The Court found these arguments unpersuasive. Justice Iyer affirmed the trial judge's finding that the deletions did not alter the essential terms of the agreement. More significantly, the Court reiterated the established principle that acceptance of an offer can be implied by conduct. The respondent's act of transferring the additional 4 BTC after receiving the supplementary agreement constituted objective acceptance of its terms, consistent with authorities such as *Saint John Tug Boat Co. Ltd. v. Irving Refinery Ltd.*, [1964] S.C.R. 614.

Second, the Court addressed the appellant's proposed defenses of mistake, frustration, and duress. The appellant argued that both parties were mistaken as to the legitimacy of the Bypass Procedure. He also submitted that its fraudulent nature was an unforeseeable event that frustrated the contract's purpose. The Court found no merit in these positions, concurring with the trial judge that the contracts had explicitly and intentionally allocated the risk of the Bypass Procedure's failure to the appellant. The doctrine of frustration applies only when an unforeseen event makes performance radically different from what was contemplated, not when the contract itself provides for the very contingency that occurred (*Naylor Group Inc. v. Ellis-Don Construction Ltd.*, 2001 SCC 58). Here, the failure of the third-party venture was the specific risk the appellant agreed to bear.

Regarding duress, the appellant argued that psychological manipulation by the third-party fraudsters nullified his consent to the loan agreements with the respondent. The Court noted that the jurisprudence does not typically support a

finding of duress where the alleged coercion is imposed by a third party unknown to the other contracting party. The respondent was not a party to, nor did he take advantage of, the alleged duress.

The most significant aspect of the decision is its treatment of the appellant's submission that established legal doctrines must be interpreted differently for contracts involving cryptocurrency due to the prevalence of sophisticated digital fraud. The Court acknowledged the trial judge's finding that the appellant was likely the victim of a "nefarious scheme." However, it firmly rejected the notion that the subject matter of the contract necessitates a departure from core legal principles.

Justice Iyer concluded: "[A]s [the chambers judge] found, the complexity of cryptocurrency does not mean that all contracts involving cryptocurrency are necessarily complex or that contract law doctrines must change dramatically to respond to them. The Contracts here were straightforward loan agreements, and the judge made no reviewable error in characterizing them as such."

This statement underscores a crucial point for legal practitioners and participants in the digital asset market. Courts will look to the substance of an agreement, not merely its context. Where parties enter into a conventional legal structure, such as a loan, the transaction will be analyzed through the well-established lens of contract law. The fact that the asset loaned was digital did not transform a simple loan with clear risk allocation into a joint venture or an instrument requiring novel interpretive rules. The decision reinforces the principle of commercial certainty: clearly drafted terms, particularly those allocating risk, will be upheld.

Author: Mahmoud Abuwaseh
Title: Partner – Disputes
Email: mabuwaseh@waselandwaseh.com
Profile:
<https://waselandwaseh.com/about/mahmoud-abuwaseh/>

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwaseh.com
business@waselandwaseh.com

Preventing a ‘Rug Pull’: Ontario Superior Court on Risk of Crypto-Asset Flight and Freezing NFTs

September 27, 2026

In a recent decision of the Ontario Superior Court of Justice, **McRae-Yu v. Profitly Incorporated et al.**, Hooper J. granted and then upheld a Mareva injunction in the context of an allegedly fraudulent non-fungible token (“NFT”) collection called “Boneheads.” The judgment offers an important illustration of how courts may approach NFTs, “minting,” and the potential dissipation of crypto-assets in fraud-based litigation. (*McRae-Yu v Profitly Inc. et al.*, [2024 ONSC 1593](#))

Early in the Reasons for Decision, the Court describes NFTs as “cryptocurrency-based assets” that “can be developed within a collection wherein the developers create numerous NFTs to be offered to the public at the same time” (para. 5). This “offering of a collection for public sale” is referred to by Hooper J. as the “minting” of the NFTs (para. 5). The Court also explains that an NFT sale is governed by a “smart contract— a self-executing contract formed when certain conditions are fulfilled,” whose terms “are transparent”

(para. 6). Each NFT “is given a unique identification number which allows it to be distinguishable from all other NFTs” (para. 6), meaning its ownership and transactional history can be tracked on a blockchain.

The Court situates the case within the broader backdrop of NFTs, acknowledging that “NFTs can be anything digitally tokenized on a blockchain” and that “one popular form of NFT is a piece of digital art” (para. 7). Citing the “excitement and anticipation surrounding an NFT collection,” Hooper J. points out that, although the NFT market has become volatile, certain collections can draw in consumers with “a roadmap of benefits and privileges” to spur confidence in the value of the tokens (para. 7-9). According to the Court, when the Boneheads project minted in 2021, NFTs were “seen to be a potentially valuable investment” (para. 8).

Minting and the Alleged Fraud

The Plaintiff in this action claimed that the Boneheads development team had promised substantial post-mint benefits for NFT owners, as well as promotional giveaways—namely “one lucky randomized token holder would get a monetary mystery box valued at a quarter million dollars, ‘revealed instantly at the end of the mint’” (para. 12). Almost immediately after the sale, investors began to suspect “a rug pull,” which Hooper J. defines as “a scam in which an NFT developer props up the product with fake promises, mints the collection, and then takes the proceeds of the mint and disappears” (para. 15). Although the team remained sporadically present, the Plaintiff characterized the situation as a “slow rug pull,” which the Court describes as “a modified scam where the NFT developer continues to make false promises to pacify disappointed consumers with false hope, never intending to fulfill those promises” (para. 15).

Crucially, the Boneheads project had garnered approximately “950.5 ETH,” which was worth around “\$4,005,047.38 CAD” at the

time of mint (para. 13). These digital assets were then distributed into three crypto wallets. In reviewing the trajectory of these wallet transfers, the Plaintiff and other investors accused the Defendants of fraud and, fearing dissipation of the NFTs' proceeds, successfully moved for a Mareva injunction that froze the Defendants' bank accounts and crypto wallets.

Crypto-Assets and the Risk of Dissipation

The Court's analysis of whether to continue the Mareva injunction centered on the fact that NFTs and cryptocurrencies can be "instantly and anonymously" moved (para. 37). Hooper J. stresses that a Mareva injunction is an "extraordinary remedy" (para. 22) because it effectively amounts to "pre-judgment execution against the defendant's assets" (para. 22). Yet in cases of alleged fraud, the Court indicated that "the courts have found it can be appropriate for the initial motion to be brought without notice," precisely because "if any further assets are dissipated, that dissipation can be remedied through the contempt powers of the court" (para. 23).

Acknowledging that cryptocurrency's very nature facilitates swift asset flight, the Court cites and applies the principle that "it is not necessary to show that the defendant has bought an air ticket to Switzerland, has sold his house and has cleared out his bank accounts" (para. 39, quoting from another authority). Rather, "it should be sufficient to show that all the circumstances, including the circumstances of the fraud itself, demonstrate a serious risk that the defendant will attempt to dissipate assets or put them beyond the reach of the plaintiff" (para. 39). Hooper J. then observes that the Defendants offered "extremely vague" evidence as to how the minted funds had been used, thus adding to the Court's inference of a "real risk of dissipation of assets" (para. 41).

In language emphasizing the particular ease of moving crypto-

assets, Hooper J. comments: “I find that the plaintiff is not required to adduce direct evidence showing the defendants are actively dissipating their assets. A serious risk of dissipation is sufficient and may be inferred from the surrounding circumstances. As I have already found there exists a strong prima facie case of fraudulent misrepresentation, I find that the defendants are very likely to attempt to dissipate the remaining assets or remove them from this jurisdiction” (para. 41).

Court’s Willingness To Enjoin Access to Crypto Wallets

From a procedural standpoint, the Court initially granted a broad freeze of both conventional and crypto accounts, later modifying it by consent to allow the Defendants some living expenses. However, the Defendants were still “denied access to their cryptocurrency wallets and cryptocurrency assets under this modified order” (para. 3). In deciding to continue that freeze until trial or further order, the Court found that the stringent requirements for a Mareva injunction had been met, including “a strong prima facie case” of fraud, a serious risk of dissipation, and a balance of convenience favoring the Plaintiff class (para. 30-47).

Hooper J. highlights that crypto-assets’ ease of secretive transfer (and the alleged fraud) weighed heavily in favor of maintaining the injunction. As stated: “Given the fraudulent nature of the launch and the Boneheads’ continued misrepresentations of the benefits attached to this NFT collection, the real risk of dissipation of assets can be proven by inference” (para. 39). Although the Defendants argued legitimate uses of funds, the Court found these explanations insufficiently detailed: “There is insufficient evidence from the defendants to explain how the \$3.5 million was used or what ongoing expenses require access to the frozen funds” (para. 45).

Conclusion and Significance

The judgment underscores the Court's acknowledgment of NFTs and cryptocurrency as novel yet susceptible vehicles for fraud, where "the nature of cryptocurrency makes it easy to instantly and anonymously dissipate" (para. 37). Hooper J. expressly recognized that, while that ease alone does not automatically justify a Mareva injunction, evidence or inference of misrepresentation and potential fraud can shift the balance decisively in favor of freezing the assets. This approach demonstrates the Court's readiness to adapt conventional equitable remedies to the digital realm.

By continuing the injunction against most of the Defendants' crypto wallets, while allowing further hearings to assess legitimate needs such as "payment of legal fees," the judgment confirms the Court's willingness to intervene in order to "ensure that actual and potential wrongdoers do not ignore their obligations" (para. 29, quoting the Supreme Court of Canada). As Hooper J. put it, "if there is a finding of fraud, there is virtually no chance that the defendants, as perpetrators of this fraud will be held accountable without this injunction" (para. 43). This case, therefore, serves as a meaningful precedent for plaintiffs seeking to preserve crypto-assets in disputes where fraud or other misconduct is alleged.

Author: Mahmoud Abuwaseh

Title: Partner – Disputes

Email: mabuwaseh@waselandwaseh.com

Profile:

<https://waselandwaseh.com/about/mahmoud-abuwaseh/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseh.com

business@waselandwaseh.com

When Crypto Claims Collide with Multiple Jurisdictions: Lessons from Coinbase

September 27, 2026

In **Shirodkar v. Coinbase Global, Inc., 2025 ONCA 298**, the Court of Appeal for Ontario grappled with a question that often arises in modern crypto-related disputes. A Canadian plaintiff, seeking to sue a network of Coinbase entities spanning multiple jurisdictions, challenged whether an Ontario court could properly assume authority over all of them. This judgment delves into **jurisdiction simpliciter**, the principle of **forum non conveniens**, and how **user agreements** can affect a court's ability to hear a dispute against global crypto exchanges with tentacles spread across borders.

In the decision, the plaintiff claimed that various Coinbase entities violated **Ontario's Securities Act** by trading or offering what he argued were securities without complying with mandatory disclosure and registration requirements. He aimed to lead a proposed class action on behalf of all Canadians who had transacted in crypto tokens on the Coinbase platform during a specified period. Yet, his biggest hurdle was showing that Ontario was the right (and legally permissible) place to litigate against Coinbase's U.S. and Irish operations, in addition to its Canadian subsidiary.

The Court of Appeal began by analyzing whether there was **consent-based jurisdiction** over the international Coinbase defendants. The plaintiff insisted that a 2023 Canadian User Agreement, which contained a **non-exclusive choice of forum** clause favoring Ontario, applied retroactively to all the Coinbase entities. The motion judge, whose order was under

appeal, found that **only Coinbase Canada** was a party to that Canadian User Agreement. The foreign Coinbase companies were not signatories and thus had not agreed to have all claims against them heard in Ontario. The Court of Appeal endorsed this reading. It concluded that a forum clause in a contract between one Canadian entity and a user cannot automatically rope in non-parties—even if they belong to the same corporate group.

Much of the decision revolves around whether Coinbase's dealings with Ontario securities regulators or the fact that its overall crypto platform is accessible in Ontario could confer jurisdiction over the other foreign-based entities. The appellant argued that Coinbase Global, Coinbase Inc., and Coinbase Europe all should face claims in Ontario because they allegedly operate in an **"intertwined web of Coinbase entities."** The court rejected this argument, emphasizing that the plaintiff must show more than a general connection to Ontario. A regulatory application or any parallel oversight by Canadian authorities is not, in itself, proof that a foreign defendant consented to or expected that private litigants could sue it in Ontario. The mere existence of corporate affiliations also does not automatically expand the reach of Ontario's courts.

On the question of **jurisdiction simpliciter** (whether an Ontario court has the authority to decide the matter at all), the Court of Appeal turned to the criteria developed in **Club Resorts Ltd. v. Van Breda**. Under **Van Breda**, certain "connecting factors" link a defendant to a forum in a way that allows an assumption of jurisdiction. The fact that the plaintiff accessed the Coinbase platform from a computer in Ontario, or suffered financial loss in Ontario, was not by itself enough to pin down the foreign Coinbase entities. Otherwise, as the judgment explained, a global internet company could be sued nearly anywhere in the world, simply because a user clicked "buy" or "sell" from a particular

location.

The final issue was the question of **forum non conveniens**, which arises when a court has jurisdiction but wonders whether another forum would be better suited to hear the dispute. The court recognized that it did have jurisdiction over **Coinbase Canada**, because that entity is domiciled in Ontario and had taken clear steps indicating its presence in the province. Yet, the Court of Appeal affirmed the stay of the action even against Coinbase Canada. The motion judge found that **Ireland** was plainly the more appropriate forum for the dispute, since the relevant agreements and transactions all pointed toward Irish-based Coinbase operations. Ontario's connection to the plaintiff's claims was weak and essentially hinged on the plaintiff's personal decision to trade from within the province at certain points. From a policy standpoint, the court also stressed the **comity** principle. This means courts in one jurisdiction should not take it upon themselves to regulate activity that occurred primarily elsewhere, especially when the dispute could be fairly addressed in the foreign forum.

For investors considering disputes against a **multi-entity, multi-jurisdictional crypto exchange**, this decision underlines the importance of clarifying which corporate entity the claim actually targets. It also shows that **choice of law** and **choice of forum** clauses in standard user agreements can be quite powerful, but they are only binding on those actually signing them. Where an exchange sets up numerous subsidiaries in different countries, an investor must establish clear links between each named entity and the chosen forum. This can be an uphill battle if most platform operations happen abroad or on servers located elsewhere.

Another critical takeaway is that **local regulators** can oversee certain aspects of a global crypto firm's business, but that does not automatically allow investors to sue the entire organization in one forum (court or arbitration). This

decision also signals that, in cross-border disputes, a court might still keep jurisdiction over the local subsidiary, but it can choose to **stay** the claim if a foreign venue is the “clearly more appropriate” forum. Ireland, in this case, was deemed preferable because that is where the primary defendant (Coinbase Europe) is located, and that is where the core of the alleged wrongdoing occurred.

Shirodkar v. Coinbase Global, Inc. underscores how critical **forum selection, corporate structure, and regulatory engagement** are when deciding where to sue a multinational crypto exchange. For anyone considering litigation or arbitration, it is wise to carefully check the **user agreements** they accepted, evaluate how and where the trades took place, and weigh the pros and cons of the available forums. Otherwise, the case might ultimately unfold in the exchange’s home jurisdiction, leaving investors facing unfamiliar procedures.

Author: Mahmoud Abuwaseel

Title: Partner – Disputes

Email: mabuwaseel@waselandwaseel.com

Profile:

<https://waselandwaseel.com/about/mahmoud-abuwaseel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseel.com

business@waselandwaseel.com