# Sovereign Heists, Stablecoin Freezes, and the ADGM Proprietary Injunction: Inside the $6.3 Billion Binance Recovery Architecture

November 19, 2026

The Abu Dhabi Global Market (ADGM) Courts' issuance of a proprietary injunction ordering 18 major cryptocurrency companies to freeze billions of dollars in stolen digital assets marks a pivotal moment in cross-border digital asset recovery [Reuters]. Following the October 29, 2026 cyberattack on wallets operated by Binance, a $6.3 billion breach attributed by United States authorities to North Korea and standing as the largest heist in cryptocurrency history [Reuters; Arabian Business], the world's largest cryptocurrency exchange turned to the courts of its global operational hub in Abu Dhabi to restrict the movement of stolen tokens [Reuters]. Counsel from Gibson Dunn representing Binance described the relief in a statement as *"one of, if not the, largest publicly known freezing orders ever made"* [Reuters]. Applying to stablecoin issuers Circle (operator of USDC) and World Liberty Financial (operator of USD1), alongside 16 other firms, none of which were accused of wrongdoing by the court [Reuters; Arabian Business], the interim order sets the stage for a key return hearing scheduled for December 1, 2026 [Reuters].

For practitioners handling high-stakes Digital Asset Claims and cross-border enforcement, the ADGM Court's order represents a live test of the legal, custodial, and regulatory infrastructure developed across the United Arab Emirates in

recent years. Drawing on the analysis of over one hundred UAE digital asset judgments in *UAE Crypto Litigation* and Wasel & Wasel's ongoing Intelligence coverage of global Web3 jurisprudence, four core legal dimensions define this proceeding: the jurisdictional shift to ADGM's common law framework, the legal mechanics binding non-wrongdoer intermediaries, the operational distinction between issuer-controlled stablecoins and native tokens, and the intersection of sovereign cyber operations with institutional risk frameworks.

## Why Abu Dhabi? From "Binance Operators" to the ADGM Common Law Hub

Binance previously disclosed that the ADGM financial center serves as its global hub and that Abu Dhabi's Financial Services Regulatory Authority (FSRA) is its primary regulator [Reuters; Arabian Business]. In a January 9, 2026 briefing, *The Cost of Clarity: Inside Binance's 2026 Terms and the New Dispute Resolution Regime*, Wasel & Wasel examined Binance's transition, effective January 5, 2026, into a regulated corporate structure within the ADGM.

Prior to 2026, Binance's legacy user terms relied on an overarching counterparty construct termed "Binance Operators," an arrangement that faced judicial criticism for corporate opacity in *CFTC v. Zhao* and in *Lochan v. Binance Holdings Limited*, 2023 ONSC 6714, which Wasel & Wasel analyzed in *Crypto Disputes in Arbitration or Court? Impact of the Lochan v. Binance Judgment*. Under the 2026 restructuring analyzed in *The Cost of Clarity*, Binance segregated its operations across three distinct ADGM-licensed entities: **Nest Exchange Limited** (Recognized Investment Exchange), **Nest Clearing and Custody Limited** (Recognized Clearing House and digital asset custodian), and **Nest Trading Limited** (Broker-Dealer).

Alongside shifting user-facing disputes to three-member ICC arbitral tribunals seated in the ADGM, anchoring the

platform's primary regulatory and custodial nexus in the ADGM carried significant substantive consequences under property law. As examined in the Introduction to *UAE Crypto Litigation*, while the UAE's onshore federal and local courts adjudicate digital asset claims within a civil law statutory framework, the ADGM and the Dubai International Financial Centre (DIFC) operate as autonomous common law jurisdictions. As H.E. Justice Michael Black KC noted in the Foreword to *UAE Crypto Litigation*, this pluralistic legal architecture places specialized common law courts alongside the onshore judiciary, equipping the UAE to address complex transnational blockchain disputes.

In *The Cost of Clarity*, Wasel & Wasel specifically noted that because ADGM law directly incorporates English common law, which recognizes crypto-assets as property capable of being the subject of proprietary claims (*AA v Persons Unknown* [2019] EWHC 3556 (Comm)), digital assets tied to the ADGM structure may be subject to **proprietary injunctions**. In the wake of the October 29 breach, Dugan Bliss, Deputy General Counsel at Binance, stated: *"We will continue using every lawful tool available to trace, freeze and recover stolen assets, support our partners in returning funds where possible, and keep those assets out of the hands of the attackers"* [Reuters; Arabian Business]. Establishing its global hub in the ADGM positioned Binance within a common law jurisdiction empowered to issue proprietary freezing relief directed at tracing and immobilizing misappropriated assets across international markets.

## Anatomy of the Proprietary Injunction: Innocent Intermediaries and Procedural Exposure

It was announced that the 18 companies named in the legal action are **not accused of any wrongdoing** [Reuters; Arabian Business]. Several market participants had already intercepted or frozen stolen tokens shortly after the October 29 incident, with Binance previously reporting that approximately **$2.85**

**billion** (roughly **45.2%** of the $6.3 billion stolen) had been frozen or intercepted by third parties [Reuters]. David Wachsman, spokesman for World Liberty Financial, stated: *"As the security incident unfolded in real time, World Liberty received an alert from onchain data identifying the issue. We acted decisively to protect our users and our partners"* [Reuters]. Similarly, a spokesperson for Circle stated that the company continues to coordinate with Binance and law enforcement, while declining to comment on specific legal proceedings [Reuters].

From an asset-recovery and Major Litigation perspective, formalizing pre-existing voluntary freezes through an ADGM proprietary injunction serves four concrete legal functions:

**Proprietary Relief vs. Personal (*Mareva*) Freezing Orders:** In cross-border fraud recovery, where Wasel & Wasel advises on obtaining *Mareva* injunctions and has represented respondents in USD 88 million worldwide freezing order (WFO) proceedings, a critical distinction separates a personal freezing injunction from a **proprietary injunction**. Whereas a *Mareva* order restrains a defendant from dealing with their own assets to preserve a future judgment sum, a proprietary injunction attaches to specific claimed assets in which the claimant asserts a proprietary interest [Reuters]. As Wasel & Wasel examined in *Piercing the Blockchain Veil: The Ontario Court's Novel Pushback on Crypto Norwich Orders (Compared with the UK and DIFC)*, citing *Techteryx Ltd v Aria Commodities DMCC* [2025] DIFC DEC 001, common law courts in the UAE apply the "Enforcement Principle" to prevent the court's jurisdiction from being thwarted by rapid on-chain dissipation.

**Prohibiting Lending, Swapping, and Mixing to Preserve Traceable Title:** Under the ADGM Court's order, Circle, World Liberty Financial, and the 16 other named companies must maintain the freeze pending further court proceedings and are expressly **barred from lending, swapping, or mixing** the tokens with other assets [Reuters]. In *Misappropriated Mining*

*Hardware and Newly Minted Tokens: Analysis of Yimiao v 3V (Supreme Court of Victoria) — Opportunity Loss, Unjust Enrichment, and Constructive Trusts*, Wasel & Wasel examined how common law courts treat stolen property as held on an institutional constructive trust from the moment of theft, whereas downstream derivative proceeds can complicate third-party "knowing receipt" claims if direct proprietary lineage is broken. Likewise, as detailed across *UAE Crypto Litigation*, UAE Virtual Asset Service Provider (VASP) regulations strictly prohibit commingling and unauthorized rehypothecation of virtual assets in order to preserve an auditable, one-to-one ownership record. Enjoining lending, swapping, and mixing prevents the claimed corpus from being absorbed into omnibus liquidity pools where proprietary tracing could be contested.

**Judicial Safe Harbor Against Third-Party Holder Claims:** When an issuer or exchange unilaterally freezes a wallet address without a court order or law-enforcement directive, it faces potential litigation from downstream wallet holders alleging breach of contract or tortious interference, a tension highlighted in Wasel & Wasel's August 2026 analysis, *A Reading of the High Court of Australia Transcript on the Nature of Cryptocurrency in Poulton v Conrad*, regarding strict-liability conversion and good-faith purchaser defenses. As analyzed in Chapter 68 of *UAE Crypto Litigation* (examining Dubai Court of Appeal Case No. 233/2023), compliance with a binding legal freeze order from a competent authority negates the element of "fault" required to establish civil liability against a financial intermediary. A formal ADGM injunction converts voluntary blacklisting into compliance with a judicial mandate.

**Divergent Enforcement Sanctions Across UAE Forums:** For global VASPs served with court orders in the UAE, compliance risks differ sharply between common law free zones and mainland execution courts. In the ADGM and DIFC, non-compliance with an injunction engages **contempt of court** powers, an area in which

Wasel & Wasel acted in the first contempt proceedings before the DIFC Courts and provided expert UAE law evidence to the UK High Court in *Commercial Bank of Dubai v. Al Sari* on cross-border WFO disclosure liabilities. By contrast, as Wasel & Wasel detailed in *The Seven-Day Trap: Dubai Courts Impose Strict Liability on Non-Debtor Third Parties – A Comparative Warning for Global Crypto Exchanges*, if parallel recovery actions lead to onshore UAE third-party garnishment notices under Articles 256 and 259 of Federal Decree-Law No. 42 of 2022, a non-debtor exchange that fails to file a formal declaration within seven days can be held **personally liable for the entire underlying debt**.

| Stakeholder / Asset Category | Reported Scope in the $6.3B Breach | Legal & Operational Status | Primary Procedural Mechanism |
|---|---|---|---|
| **Binance (ADGM Global Hub / FSRA Regulated)** | Wallets breached on Oct. 29 for $6.3B; stated it absorbed financial impact and made customers whole [Reuters] | Pursuing recovery via ADGM Courts; return hearing set for Dec. 1, 2026 [Reuters] | Proprietary injunction to prevent transfer and support law enforcement [Reuters] |
| **Circle (USDC), World Liberty Financial (USD1) & 16 Other Firms** | Named among 18 respondents not accused of wrongdoing; part of ~$2.85B (45.2%) frozen/intercepted [Reuters] | Required to maintain freeze; barred from lending, swapping, or mixing tokens [Reuters] | ADGM Court proprietary order pending Dec. 1 continuation terms [Reuters] |

| Stakeholder / Asset Category | Reported Scope in the $6.3B Breach | Legal & Operational Status | Primary Procedural Mechanism |
|---|---|---|---|
| **Tether (USDT — El Salvador)** | Previously disclosed freezing $1.5B of stolen funds; not included in ADGM court order [Reuters] | Direct bilateral coordination with Binance in consultation with authorities [Reuters] | Token reissuance workflow achieving functional restitution *in specie* |
| **Remaining Unintercepted Assets (~$3.45B)** | ~54.8% of total stolen tokens outside reported $2.85B third-party interceptions [Reuters] | Subject to ongoing on-chain tracing and law-enforcement tracking [Reuters] | Forensic ledger screening and targeted freezes at VASP off-ramps |

## Centralized Stablecoin Control, Token Reissuance, and Restitution *In Specie*

The division between the **$2.85 billion** (**45.2%**) already frozen or intercepted and the **$3.45 billion** (**54.8%**) remaining outside initial third-party freezes [Reuters] underscores the structural difference between centralized stablecoins and decentralized native protocols.

In *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)*, Wasel & Wasel analyzed how courts increasingly look past the "borderless" narrative of blockchain networks when adjudicating centralized digital asset structures, anchoring control to identifiable corporate entities and infrastructure. Fiat-pegged stablecoins such as USDC, USD1, and USDT [Reuters]

incorporate smart-contract administrative controls enabling their corporate issuers to freeze specific addresses on-chain. Functionally, that protocol-level authority operates much like the tripartite Account Control Agreements and "Notices of Sole Control" examined in *UAE Crypto Litigation*, which enable a secured or authorized party to halt unauthorized dispositions without the wallet holder's cooperation.

Equally noteworthy is the distinct path taken with El Salvador-based Tether. Although Tether previously disclosed that it had frozen **$1.5 billion** worth of stolen USDT, Tether was not included among the 18 companies in the ADGM Court order [Reuters]. Bliss stated that Binance was working directly with Tether on the return of those frozen assets, and a Tether spokesperson stated: *"In consultation with the relevant authorities, we will work directly with Binance in respect of reissuing the tokens"* [Reuters].

From a remedies standpoint, burning or permanently immobilizing compromised stablecoins and reissuing replacement tokens to the rightful holder achieves the functional equivalent of **restitution *in specie***. As examined in Chapters 42 and 63 of *UAE Crypto Litigation* and in Wasel & Wasel's February 2026 briefing, *UAE Crypto Litigation: Specific Performance and the Return of the Asset In Specie*, the Dubai Court of Cassation (Judgment of 14 November 2024 in Case No. 433/2024) has affirmed under Article 386 of the UAE Civil Transactions Law that the primary remedy for misappropriated digital assets is specific performance, returning the exact digital asset in kind, resorting to monetary valuation at the time of judgment only where *in specie* return is impossible. Where token reissuance is not resolved bilaterally alongside law enforcement, a court-sanctioned proprietary determination provides the formal legal basis that regulated issuers and custodians require before extinguishing or transferring frozen balances.

For the remaining **$3.45 billion** not yet captured in reported

freezes, recovery confronts the evidentiary realities of decentralized networks. As detailed in Chapter 11 of *UAE Crypto Litigation* (analyzing Dubai Court of First Instance Case No. 2915/2023), when misappropriated assets are dispersed across dozens or hundreds of unattributed wallets, raw blockchain immutability proves asset movement but does not by itself establish legal attribution in court. Intercepting those flows requires combining real-time distributed ledger tracing software, a mandatory technical control for licensed VASPs under UAE regulatory rulebooks, with rapid injunctive and disclosure applications at the centralized off-ramps where laundered clusters eventually seek fiat or stablecoin liquidity.

**Geopolitical Attribution, Balance-Sheet Protection, and Strategic Imperatives Ahead of December 1**

The attribution of the October 29 heist to **North Korea** by US authorities [Reuters; Arabian Business] situates this recovery squarely at the intersection of Major Litigation and Sensitive Geopolicy. In *War Series: The Cyber-Kinetic Blur , 27+ Data Center Strikes in Active Conflicts, the NotPetya Precedent, and "Acts of War" in Arbitration* and *The Private Sector's Increasing Control on National Security*, Wasel & Wasel analyzed how private digital infrastructure increasingly sits on the frontline of state-sponsored cyber operations, and how Lloyd's Market Association Bulletin Y5381 (the LMA5564 clauses) shifted systemic state-backed cyber risks away from standalone insurance policies and onto corporate balance sheets.

In its blog post, Binance stated that while it had absorbed the financial impact of the stolen funds and made customers whole, it had a duty and responsibility to pursue the stolen assets and support law enforcement [Reuters; Arabian Business]. Within the UAE's virtual asset regulatory architecture, where Wasel & Wasel has arbitrated and litigated complex exchange disputes involving platform security,

liquidation engines, and insurance fund deployment, maintaining 100% one-to-one reserve backing for client liabilities is a foundational regulatory requirement. Where customer balances are made whole, downstream recovery litigation focuses directly on the platform's proprietary claims to trace, freeze, and reclaim stolen assets from attackers and intermediary pools.

With the ADGM Court scheduled to consider on **December 1, 2026** whether the proprietary injunction should continue and on what terms [Reuters; Arabian Business], institutional market participants, OTC desks, and global VASPs face three immediate operational priorities:

**Enforce Contractual Provenance Warranties and Compliance Rejection Rights:** US attribution of the breach to North Korea [Reuters] creates acute sanctions and secondary-freeze exposure across OTC and DeFi liquidity pools. Institutional counterparties should review master trading and custody agreements to exercise **Compliance Rejection Rights** and enforce express warranties that delivered tokens carry clean, unencumbered title free from unlawful provenance or regulatory freezes, as detailed in *UAE Crypto Litigation*.

**Isolate Flagged Balances from Automated Treasury Sweeps:** VASPs and issuers bound by, or put on notice of, the ADGM proprietary order must ensure that technical wallet architectures disable automated lending sweeps, liquidity rebalancing, or omnibus commingling on flagged addresses to comply strictly with the court's prohibition against lending, swapping, or mixing [Reuters].

**Coordinate Multi-Forum Procedural Responses Within Statutory Windows:** Where cross-border tracing extends across the ADGM, DIFC, onshore UAE courts, and foreign jurisdictions, legal and compliance teams must map response protocols to each forum's exact procedural thresholds, distinguishing common law return hearings and contempt standards from the strict seven-day

declaration window applicable to onshore UAE execution attachments.

As the December 1 return hearing approaches [Reuters], the ADGM Court's proprietary freeze demonstrates how far digital asset dispute resolution has evolved. While cryptographic exploits can move billions of dollars across ledgers in minutes, the ultimate recovery of institutional capital turns on regulatory foresight, forensic on-chain tracing, and the decisive deployment of common law equity.

Mahmoud Abuwasel is a Disputes Partner at Wasel & Wasel, with offices across Abu Dhabi, Dubai, Melbourne, Toronto, and Washington D.C., and is the author of UAE Crypto Litigation. For urgent inquiries regarding ADGM or DIFC freezing injunctions, VASP compliance protocols, or cross-border digital asset recovery, contact Wasel & Wasel's Digital Asset Claims and Crypto Fraud Protection team at **business@waselandwasel.com**.

**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