UAE Crypto Litigation: The "Man in the Middle" and the Duty of Delivery

February 28, 2026

The following is an excerpted analysis of topics discussed in the book UAE Crypto Litigation, a treatise on the judicial evolution of digital asset disputes in the United Arab Emirates, available at www.uaecryptolitigation.com.

A defining feature of blockchain transactions is their irreversibility. If an asset is sent to the wrong address, there is no central authority to reverse the transaction. This technical reality creates complex legal questions when a transaction is intercepted or misdirected by a malicious third party; a "Man in the Middle" attack. In China, the US, and the UK, courts have often placed strict liability on OTC desks to verify the identity of the recipient. The UAE courts, applying general principles of contract law, have allocated this risk strictly against the seller in the context of delivery obligations.

The Dubai Court of Appeal recently analysed a dispute arising from a Peer-to-Peer (P2P) sale of USDT. The buyer had paid for the assets, and the seller transferred the USDT to a wallet address provided by a third-party intermediary who was facilitating the deal. The intermediary, upon verifying the transfer, vanished with access to that wallet, leaving the buyer empty-handed.

The court held the seller liable for the buyer's loss. It established a high standard for the duty of delivery, ruling that the obligation to deliver sold goods is not met by merely dispatching them to a provided address. The seller must ensure

the successful *receipt* of the assets into the buyer's effective control. By relying on an untrusted intermediary's instructions without verifying the wallet's ownership with the buyer directly, the seller assumed the risk of fraud.

This judgment reinforces the "perfect tender" rule in the context of digital assets. It serves as a caution to OTC traders who rely on brokers on platforms like Telegram. The legal duty is result-oriented: the contract is only performed when the buyer has the tokens, not when the seller has sent them. If the intermediary provides a fraudulent address, the party sending the funds bears the loss.

To navigate the risks of P2P transactions and intermediary liability, see more in 'UAE Crypto Litigation' book publication available at www.uaecryptolitigation.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