#2

FEB 2026

BRIEFING

LEXCRYPTA GLOBAL

Snapshot

LexCrypta Global helps lawyers and accountants verify, trace, and recover digital funds with confidence. From redacted bank statements to full-scale blockchain tracing, our secure and compliant workflow turns complex digital activity into clear, court-ready evidence.

www.lexcryptaglobal.com

+1 313 799 3236

1. Industry Context — What the Latest Crypto Crime Data Tells Us

New analysis from Chainalysis' 2026 Crypto Crime Report confirms a trend legal and accounting professionals are already seeing in practice:
crypto-related disputes are becoming more complex, more professionalised, and harder to resolve without forensic verification.
The report highlights three developments that matter directly to recovery and evidentiary work:

1. **Funds are moving faster — and fragmenting earlier.** Illicit and undisclosed crypto activity increasingly involves rapid transfers across wallets, chains, and intermediaries. This shortens the window for effective tracing and raises the evidentiary bar for proving custody and control.

2. Centralised platforms remain pivotal. Despite the growth of self-custody, exchanges and service providers continue to play a critical role — often as points where funds are pooled, frozen, or disclosed through legal process. Recovery frequently turns not on technology alone, but on documentation, timing, and procedure.

3. Professionalization cuts both ways. As bad actors adopt more sophisticated methods, courts and counterparties are responding with higher expectations. Screenshots and assumptions are no longer sufficient. What's required is independently verifiable evidence that can withstand scrutiny

Why this matters for practitioners
The data confirms what courts are already signalling: digital funds can be traced, but only evidence that is verifiable, documented, and procedurally sound will support recovery.

At LexCrypta Global, our verification and tracing framework is designed for this environment — where speed, complexity, and scrutiny coexist.

Our goal is simple: make the invisible undeniable and verifiable.

Crypto was built for secrecy!

As crypto activity professionalizes, so do the expectations of proof. Recovery increasingly depends on verified evidence — not visibility, not volume, and not assumption.

2. Case Law Watch — EU Proving Crypto Ownership Requires Proof of Control

As courts around the world confront disputes involving cryptocurrency, a consistent evidentiary question is emerging: **how do you prove ownership of an asset that exists only as a cryptographic record?**

Recent decisions from the High Anti-Corruption Court (HACC) of Ukraine provide one of the clearest judicial answers to date — and the reasoning is instructive well beyond criminal proceedings or national borders.

Ownership Requires Proof of Control

In a decision dated 9 May 2023 (Case No. 991/2399/23), investigating judges of the HACC Appeals Chamber held that the only acceptable way to confirm ownership of declared cryptocurrency was to demonstrate access to the relevant crypto wallets and to identify the public addresses where the assets were initially held.

The Court rejected the idea that ownership could be established through declarations, balances, or screenshots alone. Instead, it focused on the practical reality of crypto custody: control of private keys equals control of the asset.

This approach aligns closely with how courts already assess possession of other intangible assets — through evidence of control, not assertion.

Device-Level Evidence Becomes Central

A related decision by the Supreme Court of Justice of Ukraine, dated 4 October 2022 (Case No. 991/3721/22), illustrates how that principle operates in practice.

In that case, the Court confirmed possession of cryptocurrency based on evidence recovered from the suspect's personal smartphone, including:

- photographs of seed phrases,
- correspondence relating to crypto transactions, and
- digital artifacts that coincided with activity at known public blockchain addresses.

Crucially, the Court accepted this device-level evidence as decisive because it directly linked the individual to operational control of the wallet — bridging the gap between on-chain activity and a real-world person.

> "Cryptocurrency ownership is proven through control of a wallet — not by screenshots, balances, or assertion."

2. Continued

Across jurisdictions, courts are converging on a shared understanding:

- Visibility on the blockchain is not ownership.
- Ownership must be proven through control.
- Control is established through verifiable linkage — wallets, devices, and behaviour.

Without proof that a party controlled a wallet — not merely that funds passed through an address — recovery efforts stall.

Implications for Practitioners

For lawyers, trustees, accountants, and forensic professionals, these decisions highlight three practical realities:

1. Wallet access matters more than wallet balance.
2. The ability to demonstrate control of a wallet, or access to its keys, outweighs any static snapshot of holdings.
3. Smartphones are often the strongest source of proof.

In many cases, the most compelling evidence sits not on the blockchain, but on personal devices — linking private keys, communications, and transaction intent.

Verification must connect people to addresses.

Successful tracing requires more than following funds; it requires attribution — proving who controlled the wallet at the relevant time.

LexCrypta Insight: Courts are converging on a single test: control proves ownership — and ownership must be proven.

Why LexCrypta Global Exists

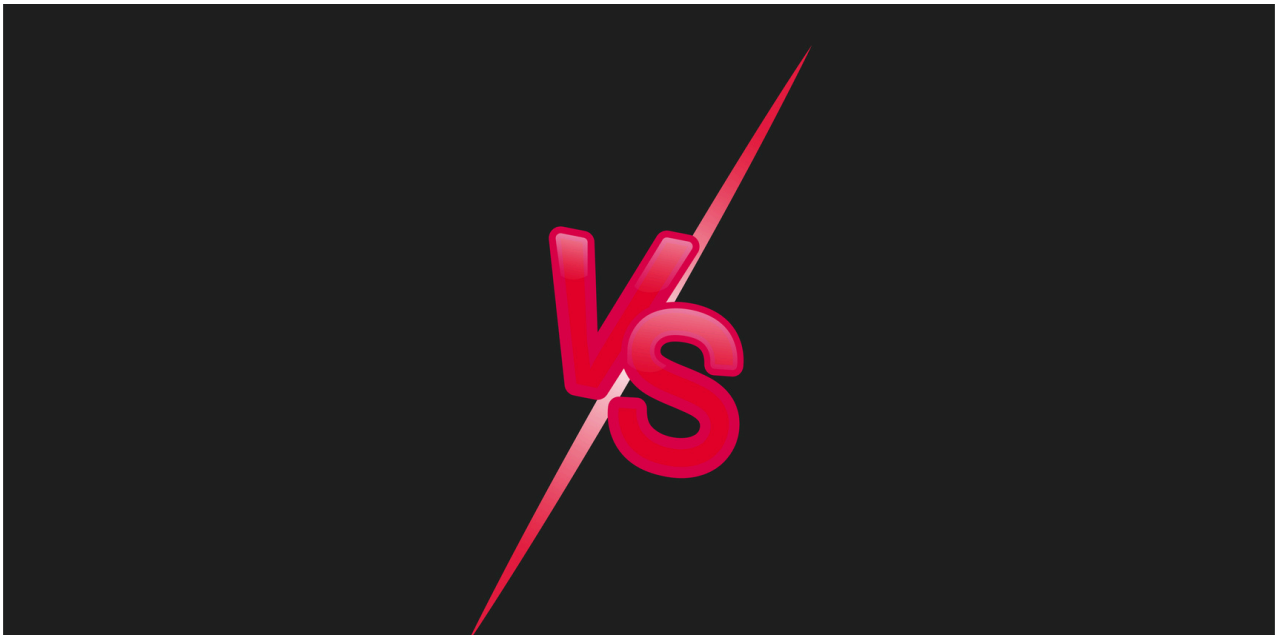
These cases illustrate why digital-fund disputes increasingly require forensic verification, not assumption.

At LexCrypta Global, our verification framework is designed to meet this exact evidentiary threshold — combining:

- on-chain tracing,
- bank-statement analysis,
- device and behavioral linkage (where available), and
- digitally signed, proof-of-existence reports suitable for court scrutiny.

Because in the digital asset context, data alone is not evidence and evidence requires verification.

source: https://yur-gazeta.com/



3. What Is the Difference Between Hot and Cold Wallets?

The difference between hot and cold wallets is not about temperature — it's about access, exposure, and proof.

A hot wallet is connected to the internet. Examples include mobile apps, browser extensions, and desktop wallets. Hot wallets are designed for convenience and frequent use. They tend to generate more transaction activity, interaction with applications, and signing behaviour.

A cold wallet is kept offline, typically as a hardware device or offline storage. Cold wallets are designed for security and long-term holding. Activity is infrequent, deliberate, and often limited to transfers in or out.

For legal and recovery matters, the distinction matters because evidence looks different. Hot wallets often produce more behavioural data — transaction frequency, application usage, and interaction patterns — which can help establish control. Cold wallets may show little activity, but when funds can be traced into them, they often support stronger inferences of deliberate custody.

Hot wallets are often the first point of entry, as they are quick to deploy, usually free, and suited to regular use and transaction activity.

Feature	Hot Wallet	Cold Wallet
Connectivity	Connected to the internet	Kept offline
Typical Examples	Mobile apps, browser extensions, desktop wallets	Hardware wallets, offline storage
Private Key Control	Held on an internet-connected device	Held offline on a physical device
Security Profile	Higher exposure to remote compromise	Highly resistant to remote compromise
Transaction Activity	Frequent, ongoing	Infrequent, deliberate
Evidence Characteristics	More behavioural data and transaction history	Fewer transactions; stronger custody inference when funded
Attribution Challenges	Can involve obfuscation or rapid movement	Often hinges on proving funding source and access
Common Use Case	Day-to-day transfers, application interaction	Long-term holding, asset storage
Recovery Considerations	Easier to trace activity; harder to restrain	Harder to observe; stronger control arguments if linked
Cost	Usually free	Typically USD $50–$200

4. What Happens If Crypto Is on an Exchange and in Pooled Funds?

When crypto is held on an exchange, the user typically does not control the private keys. Instead, assets are held in pooled (commingled) wallets, with ownership tracked on the exchange's internal ledger. Examples of exchanges are Coinbase, Kraken, Binance.

This changes how tracing and recovery work.
On-chain analysis can often identify that funds reached a particular exchange. What it usually cannot show is which customer owned those funds once pooled. Attribution then depends on off-chain evidence — including bank statements, payment gateways, account records, emails, or disclosure obtained through legal process.

Pooling does not make recovery impossible — but it shifts the problem from technology to procedure. Success often turns on timing, jurisdiction, and whether the exchange will respond to lawful requests.

On-chain tracing can take you to the exchange. Evidence and procedure take you to the person.

LexCrypta Global maintains active intelligence on more than 200 cryptocurrency exchanges worldwide — including platforms such as Coinbase, Binance, Kraken, Bitstamp, OKX, and Gemini — mapping jurisdictional location, disclosure pathways, and response patterns to support effective recovery strategies.

5. Is It Worth Recovering?

This is the most important question — and the one asked too late.
Recovery feasibility depends less on how much crypto exists and more on four practical factors:

1. Evidence quality
Are there reliable starting points — wallet addresses, transaction IDs, bank statements, or gateway records?

2. Custody reality
Are funds self-custodied (hot or cold wallet), or sitting on an exchange in pooled funds?

3. Jurisdiction and cooperation
Is there a realistic path to disclosure, freezing, or restraint?

4. Value versus friction
Does the potential recovery justify the cost, complexity, and time required?
Many matters fail not because recovery was impossible, but because teams pursued the wrong target or underestimated evidentiary friction.

Sometimes the most professional decision is to proceed. Sometimes it is to stop.

Behind exchanges, wallet value is often indeterminate on-chain because balances are tracked on the exchange's internal ledger, not at the public address level. That is precisely why subpoenas and disclosure requests matter.

6. Trend Watch

In many cases, crypto is not disclosed because it is not recognized. The matter is rarely labelled “crypto” at the outset. Instead, it appears as a mismatch between spending, behavior, and provable assets.

A common indicator is when money spent does not align with the assets a party can demonstrate. Practitioners increasingly encounter digital-fund issues in the following forms:

- Unexplained bank transfers, particularly to overseas institutions or unfamiliar counterparties
- Gaps in financial disclosure, where balances decline without corresponding asset acquisition
- Funds routed through payment gateways or exchanges, rather than held in traditional accounts
- Inconsistencies between what a client believes they hold and what can be independently proven

In these matters, the problem is not always concealment — it is misclassification.

Digital funds move through systems that do not resemble traditional banking, leaving few familiar markers unless they are actively looked for.

Why This Matters Now

Recent high-profile collapses and insolvencies continue to highlight the same issue: large sums move offshore, yet no recoverable assets can be identified, and the trail appears to end. In many cases, reporting stops at statements such as “the money is gone” or “funds cannot be traced,” without clarity as to how, where, or through which mechanisms value actually moved.

These cases illustrate a growing reality, when funds pass through non-traditional rails, conventional asset searches are often insufficient. This is where early pattern recognition matters.

Once funds have moved beyond familiar financial systems, delay increases friction, and recoverability becomes harder to assess.

Case Study on the $1 Billion Superfund Collapse in Australia coming soon

LexCrypta Global assists law firms, trustees, and regulators in the verification, tracing, and recovery of digital assets.

Our specialisations include:
Verify — Reviewing bank statements and payment gateways to identify crypto activity, and issuing digitally-signed, proof-of-existence reports.
Trace — Following funds on-chain and behind exchanges to locate hidden or pooled assets and assess recovery potential.
Vault — Providing secure custody, subpoena, and disclosure support for court-managed assets and verified evidence.

Want future issues? Email theteam@lexcryptaglobal.com

Next Issue: How Do Crypto Exchanges Actually Work?

Exchanges often split:

- incorporation (e.g. Cayman, Seychelles)
- operations (e.g. Estonia, Ireland)
- custody / tech stack (cloud, third-party providers)
- compliance functions (regional subsidiaries)

LexCrypta Insight: The place you sue is rarely the place that holds the keys.

Questions we will answer:

- Where Do You Send the Subpoena — and Why It's Rarely the Head Office
- Who Actually Controls the Funds: Legal Entity vs Technical Reality
- When Timing Fails: How Delays Kill Recoverability