DIGITAL ASSET
INTELLIGENCE

WHITEPAPER
NR. 10 · 2026

RECHT · DIGITALE VERMÖGENSFORENSIK

Blockchain-Forensik im Wandel

Warum technische Transaktionsanalysen allein künftig nicht mehr ausreichen — mit vertiefter Betrachtung der strafprozessualen Vermögenssicherung und Einziehung aus Sicht der Geschädigten, aktueller Rechtsprechung aus Deutschland, dem Vereinigten Königreich und den USA sowie Kapiteln zu Smart Contracts, NFT, RWA-Tokenisierung, MiCA und dem Berufsbild des digitalen Vermögensforensikers.

19 KAPITEL · RECHTSPRECHUNG DE/UK/USA

FINANZ FORENSIK GMBH · STAND 28. JULI 2026 · ÜBERARBEITETE FASSUNG

EXECUTIVE SUMMARY

Die Blockchain zeigt Transaktionen — nicht Eigentum

Klassische Gutachten beantworten, wohin Kryptowährungen transferiert wurden. Gerichte, Staatsanwaltschaften und Insolvenzverwalter verlangen zunehmend mehr: Wem gehören sie rechtlich? Hat ein Eigentumswechsel stattgefunden? Welche Ansprüche bleiben bestehen? Und: Fließen gesicherte Kryptowerte am Ende tatsächlich an die Geschädigten zurück?

FINANZ·FORENSIK · FINANCIAL INTELLIGENCE & BLOCKCHAIN FORENSICS WHITEPAPER 10 / 2026

32 Mrd. $
On-Chain-Wert tokenisierter RWA, Juni 2026 (11,8 Mrd. $ ein Jahr zuvor)

≈ 210
vollständige CASP-Lizenzen in der EU (von über 1.200 Anbietern)

3 Länder
ausgewertete Rechtsprechung: Deutschland, UK, USA

3. Kategorie
digitale Assets als eigene Eigentumsklasse (UK, Gesetz seit 2025)

Die Blockchain-Forensik hat sich in den vergangenen Jahren zu einem unverzichtbaren Instrument bei der Aufklärung von Kryptowährungsdelikten entwickelt. Moderne Analyseplattformen ermöglichen die Rekonstruktion komplexer Transaktionsketten über zahlreiche Wallets, Blockchains und Dienstleister hinweg.

Die steigende Komplexität digitaler Vermögenswerte führt jedoch dazu, dass eine rein technische Betrachtung der Blockchain künftig häufig nicht mehr genügt. Während klassische Gutachten in erster Linie beantworten, wohin Kryptowährungen transferiert wurden, verlangen Gerichte, Staatsanwaltschaften, Insolvenzverwalter und Rechtsanwälte zunehmend Antworten auf weitergehende Fragestellungen:

- Wem gehören die Kryptowährungen rechtlich?
- Hat tatsächlich ein Eigentumswechsel stattgefunden?
- Welche Auswirkungen haben Swaps, Bridges, Smart Contracts oder Exchange-Dienstleister auf bestehende Eigentumsrechte?
- Bleibt ein Vermögenswert trotz technischer Umwandlung wirtschaftlich identisch?
- Welche Ansprüche können daraus abgeleitet werden?
- Können gesicherte oder eingezogene Kryptowerte tatsächlich an Geschädigte zurückfließen – und über welchen strafprozessualen Weg?

Die Blockchain dokumentiert technische Vorgänge. Sie beantwortet jedoch nicht automatisch die zivilrechtlichen, strafprozessualen, wirtschaftlichen oder regulatorischen Konsequenzen dieser Vorgänge. Wie real diese Lücke bereits ist, zeigt ein Blick in die aktuelle Rechtsprechung: Deutsche Ober- und Landgerichte, US-Behörden und -Gerichte sowie der englische Court of Appeal haben in den vergangenen Jahren jeweils Entscheidungen getroffen, die genau die in diesem Beitrag beschriebene Trennung zwischen technischem Vorgang und rechtlicher Zuordnung bestätigen.

Gegenüber der ursprünglichen Fassung wurde dieser Beitrag um fünf Themenfelder erweitert, die diese Entwicklung zusätzlich beschleunigen bzw. für die forensische Praxis konkretisieren: Smart Contracts und DeFi, NFT, die Tokenisierung realer Vermögenswerte (RWA), die neue europäische Aufsichtsarchitektur rund um MiCA sowie – neu in dieser Fassung – die strafprozessuale Vermögenssicherung und Einziehung bei Kryptowerten aus Sicht der Geschädigten (Kapitel 14). Ergänzend entwirft der Beitrag ein eigenständiges Berufsbild für die Sachverständigen, die diese Aufgaben künftig bewältigen müssen.

BEGRIFFSKLÄRUNG: „DIGITALE VERMÖGENSFORENSIK"

Für die in diesem Beitrag beschriebene, über die reine Blockchain-Analyse hinausgehende Disziplin verwenden wir konsequent den Begriff „digitale Vermögensforensik" (engl. Digital Asset Forensics). **Blockchain-Forensik im engeren Sinne** bezeichnet die technische Analyse von Transaktionsdaten auf einer oder mehreren Blockchains. **Digitale Vermögensforensik** umfasst darüber hinaus die wirtschaftliche, zivilrechtliche, strafrechtliche und regulatorische Einordnung digitaler Vermögenswerte – einschließlich Smart Contracts, NFT, tokenisierter realer Vermögenswerte, der strafprozessualen Vermögenssicherung und der Anforderungen aus MiCA und angrenzenden Regelwerken.

Der Begriff ist bislang nicht standardisiert. Dieser Beitrag verwendet ihn bewusst als Arbeitsbegriff für eine Entwicklung, die in der Praxis längst begonnen hat, terminologisch aber noch keine einheitliche Bezeichnung gefunden hat.

Abbildung 1 Vom technischen Fund zur rechtlichen Auskehr – der rote Faden dieses Whitepapers

Die folgende Übersicht bildet die neun Stationen ab, die ein Kryptowert auf dem Weg von der ersten on-chain-Beobachtung bis zur Auskehr an Geschädigte typischerweise durchläuft. Sie fasst zugleich die Struktur dieses Beitrags zusammen: Die ersten sechs Stationen sind Gegenstand der technischen Blockchain-Analyse (Kapitel 1–13), die letzten drei Stationen sind Gegenstand der strafprozessualen Vermögenssicherung (Kapitel 14). Nach Auffassung der Finanz Forensik GmbH liegt genau an der Naht zwischen der sechsten und der siebten Station – zwischen Exchange und Arrest – die in der Praxis am häufigsten unterschätzte Bruchstelle: Wer sie forensisch nicht sauber dokumentiert, riskiert, dass Geschädigte trotz lückenloser technischer Nachverfolgung am Ende leer ausgehen.

Wie dieser Weg in einem konkreten Fall aussieht, zeigt das Praxisbeispiel in Kapitel 3, das im weiteren Verlauf dieses Beitrags mehrfach wieder aufgegriffen wird.

01 Die Blockchain zeigt Transaktionen – nicht Eigentum

Eine Blockchain dokumentiert ausschließlich technische Ereignisse. Sie zeigt,

- welche Wallet eine Transaktion signiert,
- wann diese ausgeführt wurde,
- welche Kryptowährung übertragen wurde,
- in welcher Höhe der Transfer erfolgte,
- welche Gebühren angefallen sind,
- auf welcher Blockchain die Transaktion stattfand.

Nicht dokumentiert wird dagegen,

- wem die Vermögenswerte tatsächlich gehören,
- aufgrund welchen Rechtsgrundes sie übertragen wurden,
- ob eine Verfügung überhaupt wirksam war,
- ob der Übertragende verfügungsberechtigt war,

- ob zivilrechtliche Ansprüche fortbestehen.

Genau hier endet die rein technische Blockchain-Analyse.

02 Technische Verfügungsgewalt ist nicht automatisch Eigentum

In vielen Verfahren wird angenommen: Wer den Private Key besitzt, ist Eigentümer der Kryptowährungen. Juristisch ist diese Aussage jedoch deutlich komplexer. Der Besitz eines Private Keys begründet zunächst lediglich die technische Möglichkeit, über eine Wallet zu verfügen. Ob daraus gleichzeitig ein Eigentumsrecht entsteht, hängt unter anderem ab von

- vertraglichen Vereinbarungen,
- Verwahrungsverhältnissen,
- Treuhandkonstruktionen,
- Unternehmensvermögen,
- Erbfällen,
- Insolvenzverfahren,
- strafrechtlichen Vermögensverschiebungen,
- Betrug, Diebstahl, Phishing, Hacking.

Ein Blockchain-Gutachten muss deshalb künftig deutlich stärker zwischen technischer Kontrolle, wirtschaftlicher Zuordnung und rechtlicher Eigentumslage unterscheiden.

AKTUELLE RECHTSPRECHUNG — OLG BRAUNSCHWEIG, BESCHL. V. 18.09.2024 – 1 WS 185/24

Wie eng technische Verfügungsgewalt und rechtliches Eigentum tatsächlich auseinanderfallen können, zeigt eine vielbeachtete Entscheidung des OLG Braunschweig: Ein IT-Administrator hatte einem Dritten beim Einrichten einer Wallet geholfen und dabei die 24-Wort-Seedphrase behalten. Später übertrug er rund 25 Millionen dem Geschädigten zugeordnete Token auf eigene Wallets.

Das OLG bestätigte die Aufhebung eines zuvor vom LG Göttingen angeordneten Vermögensarrests in Höhe von knapp 2,5 Millionen Euro und verneinte sowohl Diebstahl (§ 242 StGB, mangels „fremder beweglicher Sache“) als auch Ausspähen von Daten (§ 202a StGB), Computerbetrug (§ 263a StGB) und Datenveränderung (§ 303a StGB).

Der Fall belegt exakt die These dieses Beitrags: Die Blockchain kennt keine Verfügungsrechte im rechtlichen Sinne, sondern ausschließlich kryptografisch verifizierte Verfügungsfähigkeit. Bemerkenswert – und Ausgangspunkt für Kapitel 14 dieses Beitrags – ist zugleich, dass mit der Verneinung der Vortat auch die strafprozessuale Sicherung (§ 111e StPO) in sich zusammenfiel: Ohne tragfähige Anknüpfungstat kein Vermögensarrest, ohne Vermögensarrest keine spätere Auskehr an die Geschädigten. Die Entscheidung ist in der Fachliteratur nicht unumstritten und wird auch als kriminalpolitisch nachbesserungsbedürftig diskutiert.

Nach Auffassung der Finanz Forensik GmbH wird die Gleichsetzung von Private-Key-Besitz und Eigentum in der Praxis noch immer unterschätzt – nicht nur von Laien, sondern gelegentlich auch in vorschnell formulierten Gutachten. Unsere praktische Erfahrung aus einer Vielzahl forensischer Untersuchungen zeigt: Wer die Frage „Wer hat wann über welche Wallet verfügt?“ mit der Frage „Wem gehört der Vermögenswert?“ gleichsetzt, riskiert Gutachten, die technisch zutreffend, rechtlich aber angreifbar sind – mit unmittelbaren Folgen für die Erfolgsaussichten von Sicherungsmaßnahmen, wie der Fall OLG Braunschweig zeigt.

03 Die neue Herausforderung: Eigentumswechsel

Die eigentliche juristische Fragestellung lautet häufig nicht: Wohin sind die Kryptowährungen geflossen? – sondern vielmehr: Hat sich dadurch auch das Eigentum geändert? Diese Frage gewinnt insbesondere Bedeutung bei

- Recovery-Scams,
- Anlagebetrug,
- Wallet-Hacks,
- Ransomware,

- Insolvenzverfahren,
- Vermögensabschöpfung und strafprozessualer Vermögenssicherung *(vertieft in Kapitel 14)*,
- Arrestverfahren,
- Erbschaftsstreitigkeiten,
- Scheidungsverfahren,
- Unternehmensverkäufen.

Der Sachverständige muss künftig deutlich häufiger beurteilen, ob ein Eigentumsübergang erfolgt sein könnte, welche rechtlichen Auswirkungen sich daraus ergeben und welche Ansprüche möglicherweise bestehen bleiben.

Unsere praktische Erfahrung aus einer Vielzahl forensischer Untersuchungen zeigt, dass sich diese abstrakte Fragestellung am schnellsten anhand eines konkreten, in seiner Struktur typischen Falles greifen lässt. Das folgende – anonymisierte und zu Illustrationszwecken vereinfachte – Praxisbeispiel begleitet diesen Beitrag ab hier durch mehrere Kapitel.

PRAXISBEISPIEL (ANONYMISIERT): DER WEG VON ZWEI BITCOIN

Ausgangslage. Ein Geschädigter hatte bereits zuvor Kryptowerte durch einen Anlagebetrug verloren. Ein vermeintlicher „Recovery-Dienst" meldet sich telefonisch, verspricht die Wiederbeschaffung des Verlorenen und bewegt ihn dazu, zur „Freischaltung" 2,0 BTC an eine ihm zugewiesene Wallet zu überweisen – ein klassischer Recovery-Scam (vgl. die Aufzählung in diesem Kapitel).

Weiterleitung. Die Täter transferieren die 2,0 BTC umgehend über den Wechseldienst ChangeNOW in USDT auf dem Tron-Netzwerk (vgl. Kapitel 7) und zahlen den Betrag auf ein Kundenkonto bei der Handelsplattform HTX ein.

Zugriff. Im Rahmen des daraufhin eingeleiteten Ermittlungsverfahrens identifizieren die Ermittlungsbehörden das betreffende HTX-Konto und lassen es im Wege eines Vermögensarrests einfrieren (vgl. Kapitel 14).

Die zentrale Frage. Ist der auf dem HTX-Konto eingefrorene USDT-Bestand rechtlich noch derselbe Vermögenswert wie die ursprünglich überwiesenen 2,0 BTC? Und wenn ja: Über welchen Weg gelangt er zurück zum Geschädigten – und was, wenn der BTC-Kurs zwischen Tatzeitpunkt und Auskehr erheblich gestiegen oder gefallen ist?

04 Wechseldienste verändern die Anforderungen an die digitale Vermögensforensik

Eine der größten Veränderungen der vergangenen Jahre ist die zunehmende Nutzung sogenannter Exchange- oder Swap-Dienstleister. Hierzu gehören beispielsweise ChangeNOW, FixedFloat, SimpleSwap, SideShift, Exolix sowie weitere Cross-Chain-Exchange-Dienstleister. Diese Anbieter ermöglichen nahezu beliebige Kombinationen zwischen Blockchains und Kryptowährungen. Dadurch entstehen vollkommen neue forensische Fragestellungen.

05 Netzwerkwechsel

Ein Vermögenswert bleibt wirtschaftlich identisch. Technisch findet jedoch ein Wechsel der Blockchain statt. Beispiele:

> **USDT Ethereum → USDT Tron · USDT Tron → USDT Solana · ETH Mainnet → Arbitrum · ETH → Base · ETH → Optimism**

Für den Blockchain-Forensiker bedeutet dies: Die Nachverfolgung endet nicht an der Einzahlung des Wechseldienstes. Sie muss auf einer anderen Blockchain fortgesetzt werden.

06 Kryptowährungswechsel

Noch komplexer wird die Situation beim eigentlichen Asset-Tausch. Beispiele:

> Bitcoin → Ethereum · Ethereum → Solana · Litecoin → Bitcoin · XRP → USDT

Hier stellt sich erstmals die juristische Frage: Liegt lediglich eine wirtschaftliche Umwandlung vor? Oder entsteht tatsächlich ein neuer Vermögensgegenstand? Diese Fragestellung kann erhebliche Auswirkungen auf Herausgabeansprüche, Schadensersatz, Arrest, Insolvenz und Vermögensabschöpfung haben.

07 Kombination aus Netzwerk- und Assetwechsel

In der Praxis findet häufig beides gleichzeitig statt. Beispielsweise:

> Bitcoin → ChangeNOW → USDT (Tron) · Ethereum → SimpleSwap → Solana

Hier entstehen mehrere technische Vorgänge gleichzeitig: Einzahlung, interner Tausch, Liquiditätsbereitstellung, Auszahlung, Blockchainwechsel und Assetwechsel. Für Außenstehende wirkt dies häufig wie eine Unterbrechung der Nachverfolgung. Tatsächlich beginnt hier jedoch oftmals die eigentliche forensische Arbeit.

Zurück zum Praxisbeispiel aus Kapitel 3: Genau diese Kombination liegt dem dort geschilderten Fall zugrunde – 2,0 BTC werden über ChangeNOW in USDT auf dem Tron-Netzwerk getauscht. Technisch endet die Bitcoin-Blockchain-Spur an der Einzahladresse von ChangeNOW; die eigentliche forensische Arbeit beginnt erst mit der Fortsetzung der Nachverfolgung auf der Tron-Blockchain bis zum HTX-Konto. Nach unserer Erfahrung ist gerade dieser Übergang der Punkt, an dem technisch unerfahrene Gutachten die Spur fälschlich für „kalt“ erklären, obwohl sie sich lediglich die Blockchain gewechselt hat.

08 Asset-Transformation statt einfacher Transaktion

Frühere Blockchain-Gutachten konzentrierten sich auf lineare Geldflüsse. Heute müssen zunehmend sogenannte Asset-Transformationen bewertet werden. Hierzu gehören insbesondere

- Coin Swaps
- Token Swaps
- Wrapped Assets
- Bridges
- Layer-2-Transfers
- Liquid Staking Tokens
- Token-Migrationen
- Stablecoin-Konvertierungen

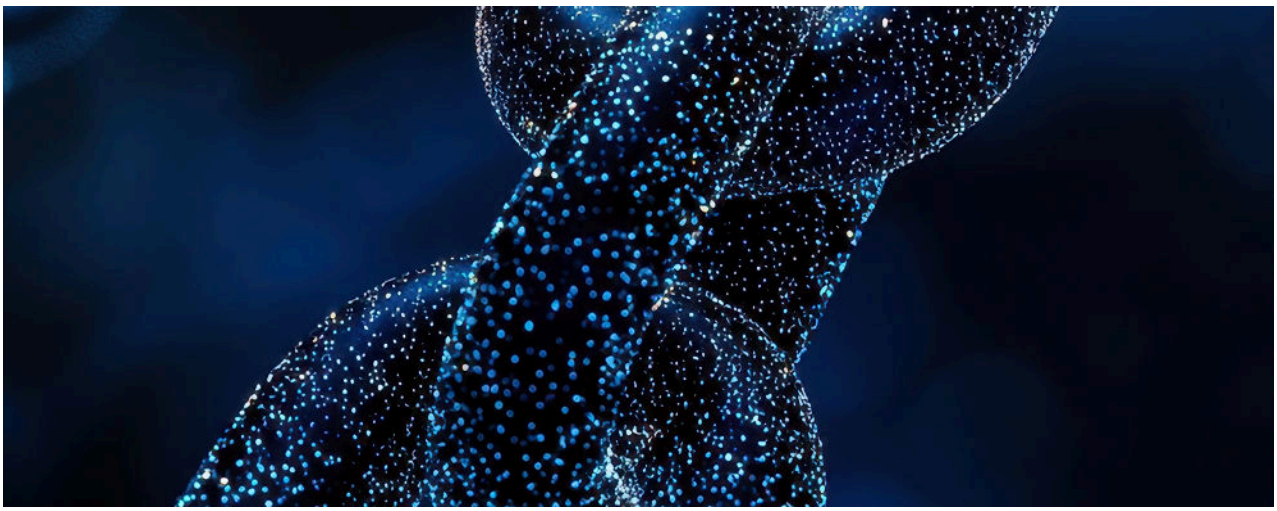
Die Blockchain zeigt lediglich den technischen Ablauf. Die rechtliche Einordnung muss durch den Sachverständigen erfolgen.

09 Cross-Chain-Bridges

Auch Blockchain-Bridges verändern die klassische Nachverfolgung erheblich. Beispiel:

> Ethereum → Bridge → Arbitrum → Optimism → Base → Polygon → Avalanche

Hier entstehen teilweise völlig neue Transaktionsketten. Die wirtschaftliche Identität eines Vermögenswertes bleibt möglicherweise erhalten. Technisch existieren jedoch mehrere unterschiedliche Token. Diese Unterschiede können sowohl technisch als auch juristisch relevant sein.



Eine Kette technisch verbundener, aber rechtlich eigenständiger Glieder. *Über Swaps und Bridges bleibt der Vermögenswert wirtschaftlich häufig identisch — technisch entstehen jedoch mehrere unterschiedliche Token, deren Eigentumszuordnung gesondert zu prüfen ist.*

10 Smart Contracts, DeFi und die zweite Abstraktionsebene

Ein weiterer, in der bisherigen Praxis oft unterschätzter Komplexitätstreiber liegt darin, dass ein Wallet heute häufig gar nicht mehr direkt an eine andere Wallet überträgt. Stattdessen interagiert der Nutzer mit Smart Contracts – etwa im Rahmen von DeFi-Protokollen, Lending, Staking, Liquiditätspools oder dezentralen autonomen Organisationen (DAOs). Die Blockchain zeigt dann nicht mehr einfach eine Überweisung von Wallet zu Wallet, sondern lediglich: *Wallet → Smart Contract*.

Die eigentliche wirtschaftliche Wirkung – etwa eine Kreditvergabe, eine Verzinsung, ein Tausch innerhalb eines Liquiditätspools oder eine Abstimmung in einer DAO – liegt dann nicht mehr in der Transaktion selbst, sondern im Programmcode des Smart Contracts. Für die digitale Vermögensforensik bedeutet das: Ohne eine Analyse der aufgerufenen Vertragsfunktionen, der zugrunde liegenden Protokolllogik und – soweit verfügbar – des Quellcodes lässt sich die wirtschaftliche und rechtliche Bedeutung einer Transaktion oft gar nicht mehr vollständig erschließen.

Zwei aktuelle US-Verfahren zeigen, wie ungeklärt die rechtliche Einordnung von Smart Contracts, Protokollen und den dahinterstehenden Organisationen noch ist.

AKTUELLE RECHTSPRECHUNG — DAOS UND SMART CONTRACTS IN DEN USA

CFTC v. Ooki DAO, U.S. District Court for the Northern District of California, Default Judgment v. 08.06.2023: Das Gericht bewertete die Ooki DAO als „Person" im Sinne des Commodity Exchange Act und damit als haftungsfähige, nicht rechtsfähige Vereinigung („unincorporated association"). Die DAO wurde zur Zahlung von rund 643.542 US-Dollar verurteilt und der Betrieb ihrer Website dauerhaft untersagt. Die Entscheidung gilt als erste gerichtliche Feststellung, dass eine DAO selbst haftungsfähig sein kann – ihre dezentrale Struktur schützt die Beteiligten also nicht automatisch vor regulatorischer Verantwortlichkeit.

Van Loon v. Department of the Treasury, U.S. Court of Appeals for the Fifth Circuit, Entsch. v. 26.11.2024: Der Fifth Circuit entschied, dass unveränderliche („immutable") Smart Contracts des Krypto-Mixers Tornado Cash keine „Property" im Sinne der US-Sanktionsgesetze (IEEPA) darstellen und die US-Sanktionsbehörde OFAC ihre Befugnisse mit der Sanktionierung dieser Smart Contracts überschritten hatte. Das Finanzministerium hob die Sanktionen daraufhin im Frühjahr 2025 auf. Die Entscheidung zeigt, wie offen selbst in einer hochentwickelten Rechtsordnung wie den USA noch ist, ob und wie Programmcode rechtlich als Vermögensgegenstand oder als bloßes Werkzeug einzuordnen ist.

Für Sachverständige folgt daraus: Wallet-Attribution und Transaktionsanalyse allein reichen bei DeFi-Sachverhalten nicht mehr aus. Erforderlich wird zunehmend auch eine Protokoll- und Smart-Contract-Analyse, die technisch nachvollzieht, was ein Vertrag bei Aufruf tatsächlich bewirkt – und rechtlich einordnet, wem die daraus entstehenden Ansprüche, Zinsen oder Anteile zuzurechnen sind.

Nach Auffassung der Finanz Forensik GmbH wird diese zweite Abstraktionsebene in der forensischen Praxis noch zu häufig übersprungen: Ein Gutachten, das lediglich feststellt „Wallet X hat mit Smart Contract Y interagiert", beantwortet die eigentlich entscheidende Frage – was diese Interaktion wirtschaftlich und rechtlich bewirkt hat – gerade nicht.

11 NFT: Eigentum, Mitgliedschaft und Lizenzrecht in Tokenform

Non-Fungible Token (NFT) werden in der öffentlichen Wahrnehmung noch immer vor allem mit digitaler Kunst assoziiert. Für die digitale Vermögensforensik ist das nur ein Randaspekt. Relevanter ist, dass NFT technisch beliebige Rechte abbilden können, etwa

- Eigentumsrechte an digitalen oder realen Gegenständen,
- Mitgliedschaften in Clubs, Plattformen oder DAOs,
- Lizenzrechte an Software, Marken oder Inhalten,
- digitale Zertifikate, etwa Nachweise, Tickets oder Berechtigungen.

Damit stellt sich bei jedem NFT-Sachverhalt zunächst die Frage, welches Recht der Token tatsächlich verkörpert – und ob dieses Recht überhaupt wirksam entstanden und übertragen wurde. Dass NFT als eigenständiger Vermögensgegenstand gerichtlich anerkannt und geschützt werden können, zeigt ein frühes, richtungsweisendes Verfahren aus dem Vereinigten Königreich.

AKTUELLE RECHTSPRECHUNG — OSBOURNE V PERSONS UNKNOWN & ORS [2022] EWHC 1021 (COMM)

Nachdem der Geschädigten zwei NFT aus der Serie „Boss Beauties“ unbefugt aus ihrer Wallet entzogen worden waren, erwirkte sie im März 2022 vor dem High Court eine einstweilige Verfügung zur Sicherung der NFT sowie eine Offenlegungsanordnung gegenüber den beteiligten Handelsplattformen. In einem weiteren Verfahrensschritt (Osbourne v Persons Unknown & Ors [2023] EWHC 340 (KB)) wurde zudem eine Zustellung an unbekannte Beklagte im Wege eines eigens dafür geprägten „Service-NFT“ zugelassen.

Der Fall gilt als eines der ersten weltweit, in dem ein Gericht NFT ausdrücklich als eigentumsfähigen Vermögensgegenstand behandelt, dem gerichtlich durchsetzbare Rechte und Schutzmechanismen zukommen können – mit unmittelbarer Bedeutung für die forensische Sicherung und Rückverfolgung gestohlener NFT.

12 Tokenisierung realer Vermögenswerte (RWA): die nächste Komplexitätsstufe

Neben rein kryptonativen Vermögenswerten gewinnt die Tokenisierung realer Vermögenswerte („Real World Assets“, RWA) zunehmend an Bedeutung. Beispiele reichen von Immobilien-Token über Gold-Token, Wertpapier-Token und tokenisierte Unternehmensanteile bis hin zu tokenisierten Kunstwerken. Das Marktvolumen zeigt, dass es sich hierbei nicht um ein Randphänomen handelt: Nach Marktdaten erreichte der On-Chain-Wert tokenisierter RWA im Juni 2026 rund 32 Milliarden US-Dollar – gegenüber etwa 11,8 Milliarden US-Dollar ein Jahr zuvor. Allein tokenisierte US-Staatsanleihen machen davon rund 15 Milliarden US-Dollar aus; der BUIDL-Fonds von BlackRock kam auf ein Volumen von rund 2,9 Milliarden US-Dollar und wird inzwischen über mehrere Blockchains hinweg geführt.

Bei einem RWA-Token stellt sich die Eigentumsfrage auf zwei Ebenen gleichzeitig: Wer verfügt über den Token auf der Blockchain – und wem gehört tatsächlich der zugrunde liegende reale Vermögenswert? Beide Ebenen können auseinanderfallen, etwa wenn ein Emittent insolvent wird, der Token entgegen den Emissionsbedingungen mehrfach ausgegeben wurde oder das zugrunde liegende Register – wie das Handelsregister, ein Grundbuch oder ein depotrechtliches Register – von der Blockchain-Zuordnung abweicht.

In Deutschland hat der Gesetzgeber mit dem Gesetz über elektronische Wertpapiere (eWpG) bereits seit 2021 einen rechtlichen Rahmen geschaffen, der neben zentralen auch dezentrale, DLT-basierte Kryptowertpapierregister vorsieht; die Führung solcher Register bedarf einer Erlaubnis der BaFin. Auf europäischer Ebene ergänzt die sogenannte DLT-Pilotregelung diesen Rahmen um befristete regulatorische Erleichterungen für den Handel und die Abwicklung tokenisierter Finanzinstrumente. Für die digitale Vermögensforensik folgt daraus eine neue Aufgabe: Ein Gutachten zu einem RWA-Token ist ohne einen Abgleich mit dem jeweils maßgeblichen zivil- oder aufsichtsrechtlichen Register unvollständig.

13 MiCA, CASPs und die neue europäische Aufsichtsarchitektur

Mit der EU-Verordnung über Märkte für Kryptowerte (Markets in Crypto-Assets Regulation, MiCA) verfügt Europa seit Ende 2024 erstmals über ein einheitliches Aufsichtsregime für Kryptowerte und die Anbieter von Kryptowerte-Dienstleistungen (Crypto-Asset Service Provider, CASP). Wer in der EU Kryptowerte verwahrt und verwaltet, mit Kryptowerten handelt oder eine Handelsplattform betreibt, benötigt seither grundsätzlich eine CASP-Zulassung. Die nationalen Übergangsfristen sind inzwischen weitgehend ausgelaufen; nach Marktbeobachtungen haben bislang nur rund 210 von über 1.200 zuvor tätigen Anbietern eine vollständige CASP-Lizenz erhalten, während Deutschland mit über 50 zugelassenen CASPs zu den Vorreitern zählt.

Für die digitale Vermögensforensik ist dies aus zwei Gründen relevant. Erstens verlagert sich ein wachsender Teil der Ermittlungsarbeit von der reinen Blockchain-Analyse hin zur Auswertung von Compliance-Daten der CASPs selbst: KYC-Angaben, Wallet-Screening-Ergebnisse und interne Risikobewertungen werden zu einer zusätzlichen, oft aussagekräftigeren Erkenntnisquelle als die Blockchain allein. Zweitens gilt seit dem 30. Dezember 2024 auch für Kryptowerte-Transfers die europäische Geldtransferverordnung in ihrer überarbeiteten Fassung (sogenannte Travel Rule): CASPs müssen Angaben zu Auftraggeber und Begünstigtem eines Transfers erheben und an die jeweils nächste Station in der Transaktionskette weiterreichen – anders als im klassischen Zahlungsverkehr grundsätzlich ohne Bagatellgrenze. Für Sachverständige bedeutet das: Ein vollständiges Bild eines Kryptowerte-Sachverhalts setzt künftig regelmäßig auch die Anforderung und Auswertung von Travel-Rule- und KYC-Daten der beteiligten CASPs voraus – nicht nur die Analyse der öffentlich sichtbaren Blockchain-Daten.

Zurück zum Praxisbeispiel aus Kapitel 3: Die Handelsplattform HTX, auf deren Konto die umgetauschten USDT landen, ist in dieser Rolle CASP im Sinne der MiCA. Die dort hinterlegten KYC-Daten und Travel-Rule-Angaben zum vorgelagerten ChangeNOW-Transfer liefern in der Praxis regelmäßig genau die Anknüpfungstatsachen, die für den nachfolgenden Vermögensarrest nach § 111e StPO (Kapitel 14.2) benötigt werden.

14 Strafprozessuale Vermögenssicherung und Einziehung bei Kryptowerten – die Perspektive der Geschädigten

Die Kapitel 1 bis 13 betrachten die Eigentumsfrage überwiegend aus zivilrechtlicher, insolvenzrechtlicher und regulatorischer Perspektive. Für Geschädigte von Anlagebetrug, Recovery-Scams, Wallet-Hacks, Phishing oder Ransomware ist damit jedoch erst die halbe Frage beantwortet. Die für sie entscheidende Anschlussfrage lautet: Können die identifizierten Kryptowerte tatsächlich strafprozessual gesichert und am Ende an sie zurückgeführt werden? Diese Frage wird in Gutachten zur Blockchain-Forensik bislang häufig ausgespart, obwohl sie über den praktischen Erfolg der gesamten Aufarbeitung entscheidet. Dieses Kapitel schließt diese Lücke – die letzten drei Stationen der Abbildung 1 (Arrest, Einziehung, Auskehr) sind sein Gegenstand.

Aus Sicht der Finanz Forensik GmbH ist dieses Kapitel keine juristische Fußnote, sondern der eigentliche Prüfstein eines jeden Gutachtens, das für Geschädigte erstellt wird: Eine technisch brillante Nachverfolgung, die an der Grenze zur strafprozessualen Sicherung endet, beantwortet für den Geschädigten am Ende nicht die einzige Frage, die für ihn zählt.

14.1 Vom Fund zur Auskehr: der mehrstufige Weg

Zwischen der forensischen Identifikation eines Vermögenswertes und seiner tatsächlichen Rückführung an Geschädigte liegen im deutschen Strafverfahren regelmäßig drei rechtlich getrennte Stufen, die jeweils eigenen Voraussetzungen unterliegen und von denen jede eine eigene Fehlerquelle für Geschädigte darstellt:

- **Sicherungsebene** – vorläufige Sicherstellung bzw. Vermögensarrest während des Ermittlungsverfahrens (§§ 111b, 111e, 111f StPO),
- **Entscheidungsebene** – die materiell-rechtliche Einziehungsanordnung im Urteil (§§ 73 ff. StGB),
- **Vollstreckungsebene** – die tatsächliche Auskehr des eingezogenen Gegenstands oder Erlöses an die Geschädigten (§§ 459h, 459k StPO).

Ein forensisches Gutachten, das ausschließlich die on-chain-Beweisführung behandelt, bildet in der Regel nur die Grundlage für Stufe eins ab – ohne die Brücke zu den Stufen zwei und drei herzustellen, bleibt für die Geschädigten offen, ob und wann sie tatsächlich etwas zurückerhalten. Unsere praktische Erfahrung aus einer Vielzahl forensischer Untersuchungen zeigt, dass gerade der Übergang von Stufe eins zu Stufe zwei – also von der Sicherstellung zur späteren Einziehungsentscheidung – in der Praxis am anfälligsten für Verzögerungen und Rückschläge ist, weil er von der materiell-strafrechtlichen Bewertung der Vortat abhängt, die zum Zeitpunkt der Sicherung oft noch nicht abschließend feststeht.

14.2 Sicherungsebene: §§ 111b, 111e, 111f StPO

§ 111b StPO erlaubt die Sicherstellung von Gegenständen zur späteren Einziehung. Die Rechtsprechung behandelt Kryptowerte inzwischen ausdrücklich als einziehungsfähige Vermögensgegenstände, obwohl ihnen die für klassische Vermögensgegenstände typische Körperlichkeit fehlt; maßgeblich ist nach der Auslegung der Norm nicht die Materialität, sondern der wirtschaftliche Wert.

§ 111e StPO ermöglicht darüber hinaus den sogenannten Vermögensarrest: Ist die Annahme begründet, dass die Voraussetzungen einer Einziehung von Wertersatz vorliegen, kann zur Sicherung der späteren Vollstreckung ein Arrest in das gesamte bewegliche und unbewegliche Vermögen des Betroffenen angeordnet werden – nicht nur in den konkret nachverfolgten Coin. Das erweitert den Zugriff erheblich, macht die Maßnahme aber auch stärker angreifbar, wie der in Kapitel 2 dargestellte Fall des OLG Braunschweig zeigt: Fiel dort die Anknüpfungstat weg, fiel der auf ihr beruhende Vermögensarrest gleich mit.

§ 111f StPO regelt die praktische Vollziehung des Vermögensarrests. Bei beweglichen Sachen, Forderungen oder sonstigen Vermögensrechten erfolgt sie durch Pfändung. Bei Kryptowerten, die auf einer Handelsplattform (Exchange) gehalten werden, bedeutet dies in der Praxis regelmäßig eine Pfändung des Herausgabeanspruchs des Beschuldigten gegenüber der Börse als Drittschuldnerin – nicht eine unmittelbare technische Beschlagnahme der Blockchain-Adresse.

§ 111p StPO erlaubt zudem eine Notveräußerung sichergestellter Vermögenswerte bei drohendem erheblichem Wertverlust. Angesichts der Volatilität von Kryptowerten wird davon in der Praxis konsequent Gebrauch gemacht: An die Stelle des ursprünglichen Coins tritt dann der in Euro hinterlegte Verkaufserlös, der bis zur rechtskräftigen Einziehungsentscheidung verwahrt bleibt. Für ein forensisches Gutachten bedeutet das: Die identifizierte Kryptowährung und der später ausgekehrte Betrag können wirtschaftlich, nicht aber technisch identisch sein.

AKTUELLE RECHTSPRECHUNG — LG VERDEN, BESCHL. (2 QS 35/25)

Kryptowerte, die auf einem Börsenwallet gehalten wurden, wurden über einen Vermögensarrest in das bewegliche und unbewegliche Vermögen des Beschuldigten gesichert und anschließend durch Pfändung seiner Ansprüche gegen die Börse als Drittschuldnerin vollzogen. Das Gericht ordnete ausdrücklich an, dass nicht konkrete Bitcoins, sondern eine Kryptowährung im Wert von 7,41598504 Bitcoin einzuziehen sei – die Börse transferierte den Wert im Ergebnis in Form von Solana auf ein Behörden-Wallet.

Das Landgericht lehnte zugleich eine analoge Anwendung von § 111n StPO (vorläufige Herausgabe an Verletzte) auf Kryptowerte ab: Der Gesetzgeber habe die Vorschrift bewusst auf bewegliche Sachen beschränkt und die Auskehr von Forderungen und anderen Vermögenswerten dem Vollstreckungsrecht (§ 459h StPO) vorbehalten; an Kryptowerten könne zudem begrifflich kein Besitz im Sinne des BGB begründet werden. Vorläufig gesicherte Kryptowerte – und insbesondere ihre Surrogate – können damit weder unmittelbar noch analog nach § 111n StPO an Geschädigte herausgegeben werden.

ZURÜCK ZUM PRAXISBEISPIEL AUS KAPITEL 3

Auf das dort geschilderte HTX-Konto übertragen: Die Ermittlungsbehörden lassen das Konto nicht durch unmittelbaren Zugriff auf die Blockchain-Adresse „einfrieren", sondern erwirken einen Vermögensarrest nach § 111e StPO und vollziehen ihn durch Pfändung des Herausgabeanspruchs des Beschuldigten gegenüber HTX als Drittschuldnerin (§ 111f StPO) – technisch exakt der in der LG-Verden-Entscheidung beschriebene Weg.

14.3 Die Grenze der vorläufigen Herausgabe: § 111n StPO und Kryptowerte

Geschädigte fragen in der Praxis naheliegenderweise häufig zuerst, ob gesicherte Kryptowerte nicht bereits vor Abschluss des Straf- und Vollstreckungsverfahrens im Wege einer vorläufigen Besitzstandsregelung zurückgegeben werden können. § 111n StPO sieht eine solche vorläufige Herausgabe für bewegliche Sachen vor, deren Eigentumslage eindeutig ist. Wie die Entscheidung des LG Verden zeigt, greift diese Vorschrift bei Kryptowerten nach derzeitigem Stand der Rechtsprechung jedoch nicht – weder unmittelbar noch analog. Für die forensische Praxis folgt daraus eine wichtige Erwartungssteuerung gegenüber Geschädigten: Eine Rückführung gesicherter Kryptowerte ist regelmäßig erst nach rechtskräftigem Abschluss des Einziehungsverfahrens über § 459h StPO zu erwarten, nicht bereits während des Ermittlungs- oder Zwischenverfahrens. Für den Geschädigten aus dem Praxisbeispiel bedeutet dies konkret: Er kann die auf dem HTX-Konto gesicherten USDT nicht bereits während des laufenden Ermittlungsverfahrens beanspruchen, selbst wenn seine Berechtigung unstreitig erscheint.

14.4 Materiell-rechtliche Grundlage: §§ 73 ff. StGB

Die eigentliche Einziehungsentscheidung stützt sich materiell-rechtlich auf die §§ 73 ff. StGB:

- **§ 73 StGB – Einziehung von Taterträgen:** Gegenstände, die der Täter durch oder für die Tat erlangt hat, können eingezogen werden.
- **§ 73b StGB – Einziehung bei Drittbegünstigten:** Auch Vermögenswerte, die auf Wallets, Mixer oder Exchange-Konten Dritter gelangt sind, können eingezogen werden, wenn der Dritte ohne rechtlichen Grund bereichert wurde – forensisch relevant bei Layering über mehrere Wallets und Wechseldienste (vgl. Kapitel 4–9).
- **§ 73c StGB – Einziehung des Wertes von Taterträgen (Wertersatzeinziehung):** Ist die Einziehung des konkreten Gegenstands nicht mehr möglich – etwa weil die Kryptowerte bereits getauscht, über eine Bridge transferiert oder in Fiatgeld umgewandelt wurden –, tritt an ihre Stelle die Einziehung eines entsprechenden Geldbetrags.

Die bestehenden Normen der §§ 73 ff. StGB und der flankierenden StPO-Vorschriften bieten nach überwiegender Einschätzung genug Flexibilität, um Kryptowerte einzuziehen oder ersatzweise ihren Wert abzuschöpfen; die Besonderheiten der Volatilität werden dabei über die Notveräußerung nach § 111p StPO aufgefangen, ohne das Grundprinzip der vollständigen Abschöpfung aufzugeben. Nach unserer Erfahrung liegt die eigentliche gutachterliche Herausforderung dabei selten in der Frage, ob überhaupt eingezogen werden kann, sondern darin, entlang welcher Wallets, Swaps und Bridges sich der wirtschaftliche Wert lückenlos bis zur richtigen Einziehungsgrundlage zurückverfolgen lässt.

14.5 Die Auskehr an Geschädigte: §§ 459h, 459k, 111l StPO

Die für Geschädigte entscheidende Vorschrift liegt im Vollstreckungsrecht: **§ 459h StPO**. Nach Absatz 1 wird ein eingezogener Gegenstand demjenigen zurückübertragen, dem ein Anspruch auf Rückgewähr des Taterlangten aus der Tat erwachsen ist. Wurde – wie bei Kryptowerten nach Notveräußerung oder Wertersatzeinziehung häufig der Fall – stattdessen ein Geldbetrag eingezogen, wird nach Absatz 2 der Verwertungserlös an den Verletzten ausgekehrt.

Das Verfahren dazu regelt **§ 459k StPO**: Der Verletzte muss seinen Anspruch binnen sechs Monaten nach Mitteilung der Rechtskraft der Einziehungsanordnung bei der Vollstreckungsbehörde anmelden. Ergibt sich die Berechtigung ohne weiteres aus der Einziehungsanordnung, erfolgt die Auskehr unmittelbar; andernfalls bedarf es einer gerichtlichen Zulassung, in der auch der frühere Beschuldigte anzuhören ist. Bereits im Ermittlungsverfahren informiert die Staatsanwaltschaft die Geschädigten nach **§ 111l StPO** über die Vollziehung einer Sicherstellung oder eines Vermögensarrests und über die bestehenden Entschädigungsmöglichkeiten – eine Herausgabe vor Rechtskraft kommt dabei, wie in Kapitel 14.3 dargestellt, praktisch nicht in Betracht.

Für Geschädigte bedeutet dies in der Praxis: Wer am Ende an einer Auskehr beteiligt werden will, muss seinen Schaden konkret beziffern, seine Verletzteneigenschaft belegen und Zahlungsnachweise geordnet bereithalten – und die Sechs-Monats-Frist des § 459k StPO im Blick behalten.

ZURÜCK ZUM PRAXISBEISPIEL AUS KAPITEL 3: DIE KURSFRAGE

Damit lässt sich auch die zweite, eingangs aufgeworfene Frage des Praxisbeispiels beantworten: Wurden die auf dem HTX-Konto gesicherten USDT nach § 111p StPO notveräußert, erhält der Geschädigte nach § 459h Abs. 2 StPO den Euro-Gegenwert des Verwertungserlöses – nicht den zwischenzeitlichen Euro-Gegenwert von 2,0 BTC zum Zeitpunkt der Auskehr. Nach Auffassung der Finanz Forensik GmbH ist genau diese Differenz zwischen dem wirtschaftlichen Wert im Zeitpunkt der Tat, im Zeitpunkt der Sicherung und im Zeitpunkt der Auskehr ein Punkt, den ein forensisches Gutachten explizit beziffern und offenlegen sollte – nicht zuletzt, um Geschädigte realistisch auf das vorzubereiten, was sie am Ende tatsächlich erhalten.

14.6 Alternativweg: Adhäsionsverfahren, §§ 403 ff. StPO

Unabhängig von Einziehung und Auskehr können Geschädigte ihre zivilrechtlichen Ansprüche über das Adhäsionsverfahren (§§ 403 ff. StPO) bereits im Strafprozess titulieren lassen, statt einen gesonderten Zivilprozess zu führen. Das Adhäsionsverfahren ersetzt die Einziehung nicht, kann aber parallel dazu einen vollstreckbaren Titel schaffen, der – etwa bei nicht restlos abgeschöpftem Vermögen – für die weitere Zwangsvollstreckung genutzt werden kann.

14.7 Ausblick: die EU-Vermögensabschöpfungsrichtlinie

Auf europäischer Ebene verpflichtet die Richtlinie (EU) 2024/1260 die Mitgliedstaaten, wirksame Rückgabemechanismen für Geschädigte zu schaffen, damit diese einen direkten Anspruch auf Herausgabe oder Entschädigung aus eingezogenen Vermögenswerten erhalten. Die vollständige Umsetzung in Deutschland steht noch aus. Bereits jetzt können Geschädigte ergänzend über § 73e StGB sowie über zivilrechtliche Ansprüche nach §§ 823, 826 BGB vorgehen. Für die forensische Praxis ist absehbar, dass sich die Position von Geschädigten mit fortschreitender Umsetzung der Richtlinie strukturell verbessern wird – Gutachten sollten diese Entwicklung im Blick behalten.

14.8 Konsequenz für digitale Vermögensforensik-Gutachten

Nach Auffassung der Finanz Forensik GmbH sollte die folgende Prüfliste künftig ebenso selbstverständlicher Bestandteil eines Blockchain-Gutachtens sein wie die Wallet-Attribution selbst. Ein Gutachten, das die Eigentumslage von Kryptowerten für Geschädigte belastbar einordnen soll, sollte künftig regelmäßig auch dokumentieren:

- ob und in welchem Umfang eine Sicherstellung oder ein Vermögensarrest nach §§ 111b, 111e StPO erfolgt ist oder rechtlich in Betracht käme,
- wie die Vollziehung nach § 111f StPO technisch umsetzbar ist – insbesondere bei Exchange-gehaltenen Werten als Pfändung gegenüber der Börse als Drittschuldnerin,

- ob eine Notveräußerung nach § 111p StPO wegen Volatilität nahegelegen hätte oder erfolgt ist, und welche Folgen dies für die Identität des gesicherten Werts hat,
- dass eine vorläufige Herausgabe nach § 111n StPO bei Kryptowerten nach aktueller Rechtsprechung ausscheidet,
- welche Einziehungsgrundlage – § 73, § 73b oder § 73c StGB – im konkreten Fall einschlägig ist,
- wie der Auskehrweg nach §§ 459h, 459k StPO für die konkreten Geschädigten aussieht, einschließlich der Anmeldefrist von sechs Monaten,
- ob ein Adhäsionsverfahren (§§ 403 ff. StPO) als ergänzender Weg zur Titulierung in Betracht kommt.

Erst mit dieser Ergänzung wird aus einer technischen Transaktionsanalyse eine belastbare Grundlage für die Frage, die Geschädigte tatsächlich interessiert: Bekomme ich etwas zurück – und wann?

15 Eigentumsrechte müssen künftig Bestandteil forensischer Gutachten werden

Die Blockchain beantwortet nicht, wem Vermögenswerte gehören, ob Eigentum wirksam übertragen wurde, welche Ansprüche fortbestehen oder welche Rechte Geschädigte besitzen – und, wie Kapitel 14 gezeigt hat, auch nicht, ob und wie diese Rechte strafprozessual durchsetzbar sind. Diese Bewertung muss künftig Bestandteil moderner Blockchain-Gutachten werden. Dazu gehören unter anderem

- zivilrechtliche Eigentumsfragen,
- Besitz- und Verfügungsrechte,
- Verwahrung,
- Treuhandverhältnisse,
- Insolvenzrecht,
- Erbrecht,
- internationales Privatrecht,
- regulatorische Vorgaben,
- strafprozessuale Vermögenssicherung und Einziehung (§§ 111b ff. StPO, §§ 73 ff. StGB, § 459h StPO),
- wirtschaftliche Betrachtungsweise.

AKTUELLE RECHTSPRECHUNG — VOLLSTRECKUNG UND INSOLVENZ IN DEUTSCHLAND

Dass Eigentumsfragen längst keine akademische Übung mehr sind, zeigt die Praxis der Zwangsvollstreckung: Das OLG Köln entschied mit Beschluss vom 26.06.2024 (Az. 11 W 15/24), dass Kryptowerte grundsätzlich pfändbar sind – unabhängig davon, ob sie auf einer Börse oder in einer privaten Wallet gehalten werden – und dass Schuldner im Rahmen zumutbarer Mitwirkungspflichten auch technische Hilfe Dritter in Anspruch nehmen müssen, um die Herausgabe zu ermöglichen. Bereits zuvor hatten das OLG Düsseldorf (Beschl. v. 19.01.2021 – 7 W 44/20) und das LG Heilbronn (Beschl. v. 03.03.2021 – Sa 8 O 368/20) die Übertragung von Kryptowerten als vertretbare Handlung eingeordnet, deren Vollstreckung nach § 887 ZPO erfolgt.

Auch der Gesetzgeber hat reagiert: Mit dem am 27.12.2024 verkündeten Finanzmarktdigitalisierungsgesetz (FinmadiG) und dem Kryptomärkteaufsichtsgesetz (KMAG), die auf dem bereits 2023 in Kraft getretenen Zukunftsfinanzierungsgesetz (ZuFinG) aufbauen, gilt seit dem Jahreswechsel 2024/2025 ein eigenes Sonderinsolvenzrecht für Kryptowerte: Nach § 46i Abs. 1 KWG fallen Kryptowerte und kryptografische Schlüssel im Grundsatz nicht in die Insolvenzmasse eines Kryptoverwahrers, sondern gelten als dem Anleger zugeordnet.

16 Die digitale Vermögensforensik als eigenständige Disziplin

Die Anforderungen an Sachverständige verändern sich grundlegend. Die klassische Blockchain-Analyse beantwortet künftig nur noch einen Teil der relevanten Fragestellungen. Hinzukommen müssen insbesondere

- Blockchain-Analyse
- Wallet-Attribution
- OSINT-Recherche
- Smart-Contract- und Protokollanalyse

- wirtschaftliche Analyse
- Dokumentenforensik
- Vertragsanalyse
- regulatorische Bewertung (MiCA, KWG, KMAG)
- zivilrechtliche Einordnung
- strafrechtliche Bewertung einschließlich Vermögensabschöpfung und Einziehung
- Bewertung möglicher Eigentumswechsel
- Analyse von Cross-Chain-Sachverhalten
- Einordnung von Asset-Transformationen und RWA-Tokenisierungen
- Bewertung internationaler Zuständigkeiten

Erst das Zusammenspiel dieser Disziplinen ermöglicht eine vollständige Rekonstruktion komplexer Kryptowährungssachverhalte. Unsere praktische Erfahrung aus einer Vielzahl forensischer Untersuchungen zeigt, dass Auftraggeber diese Bandbreite zu Beginn eines Mandats regelmäßig unterschätzen – und erst im Verlauf des Verfahrens erkennen, dass eine reine Transaktionsanalyse ihr eigentliches Ziel, die Rückführung von Vermögenswerten, nicht erreicht.

17 Der digitale Vermögensforensiker der Zukunft – ein neues Berufsbild

Die vorstehenden Kapitel zeigen in ihrer Summe, dass sich hinter der technischen Weiterentwicklung von Blockchains, Wechseldiensten, Smart Contracts, NFT und tokenisierten realen Vermögenswerten faktisch ein neues Berufsbild abzeichnet. Wer künftig belastbare, gerichtsfeste Gutachten zu digitalen Vermögenswerten erstellen will, benötigt fundierte Kenntnisse in einer ungewöhnlich breiten Kombination von Disziplinen:

- Informatik,
- Kryptografie,
- Blockchain-Technologie,
- Wirtschaft und Bilanzierung,
- Zivilrecht,
- Strafrecht einschließlich Vermögensabschöpfungsrecht,
- Insolvenzrecht,
- internationales Privatrecht,
- Geldwäscheprävention,
- Aufsichtsrecht (MiCA, KWG, KMAG),
- Beweisrecht.

In der Praxis ist diese Kombination heute die Ausnahme. Die meisten Marktteilnehmer kommen entweder aus einer rein technischen Richtung – etwa der IT-Sicherheit oder Softwareentwicklung – oder aus einer klassisch juristischen oder betriebswirtschaftlichen Richtung, ohne die jeweils andere Seite in der Tiefe zu beherrschen. Genau diese Lücke führt in der Praxis regelmäßig zu Gutachten, die entweder technisch beeindruckend, aber rechtlich unvollständig sind – oder rechtlich sauber argumentieren, ohne die zugrunde liegenden technischen Vorgänge tatsächlich verstanden zu haben.

Für Gerichte, Staatsanwaltschaften, Insolvenzverwalter und Rechtsanwälte wird es deshalb zunehmend wichtig, bei der Auswahl von Sachverständigen gezielt danach zu fragen, ob beide Seiten – die technische und die rechtlich-wirtschaftliche – tatsächlich in einer Person oder zumindest in einem eng abgestimmten Team abgedeckt werden. Langfristig erscheint es naheliegend, dass sich für dieses Anforderungsprofil – ähnlich wie bei anderen etablierten Sachverständigenbereichen – eigenständige Qualifikationswege, Fortbildungen oder Zertifizierungen herausbilden werden. Dieser Beitrag versteht sich

auch als Beitrag zu dieser Diskussion: Die digitale Vermögensforensik sollte nicht länger als Erweiterung der IT-Forensik oder als Unterkapitel des Wirtschaftsstrafrechts behandelt werden, sondern als eigenständiges, interdisziplinäres Berufsbild anerkannt und entsprechend ausgebildet werden.

Nach Auffassung der Finanz Forensik GmbH wird sich dieses Berufsbild in den kommenden Jahren nicht nur herausbilden, sondern zu einer eigenständigen Sachverständigendisziplin verfestigen müssen – aus denselben Gründen, aus denen sich zuvor etwa die IT-Forensik oder die Bau- und Immobilienbewertung als eigenständige Sachverständigenbereiche etabliert haben: An ihrem Ergebnis hängen regelmäßig gerichtliche Entscheidungen, die ohne eine solche Spezialisierung auf unsicherer Grundlage getroffen würden.

18 Aktuelle Rechtsprechung im Überblick: Wo Theorie und Praxis bereits aufeinandertreffen

Die vorstehenden Kapitel beschreiben eine strukturelle Herausforderung. Wie akut diese Herausforderung bereits ist, zeigt ein Blick auf die Rechtsprechung und Regulierung der vergangenen Jahre in Deutschland, im Vereinigten Königreich und in den USA. Die folgenden Entscheidungen und Regelungen wurden für diesen Beitrag ausgewertet.

18.1 Deutschland: Strafrecht – wenn technischer Zugriff nicht gleich Diebstahl ist

Die bereits in Kapitel 2 vorgestellte Entscheidung des OLG Braunschweig (Beschl. v. 18.09.2024 – 1 Ws 185/24) ist die bislang deutlichste obergerichtliche Aussage dazu, dass technische Verfügungsgewalt über Kryptowerte und die strafrechtliche Bewertung einer Vermögensverschiebung auseinanderfallen können. Der Senat verneinte Diebstahl, Ausspähen von Daten, Computerbetrug und Datenveränderung gleichermaßen und ordnete den Vorgang als reine – zivilrechtlich zu bewertende – Vertragsverletzung ein.

18.2 Deutschland: Vermögenssicherung, Einziehung und Auskehr an Geschädigte bei Kryptowerten

Wie in Kapitel 14 ausführlich dargestellt, konkretisiert die aktuelle Rechtsprechung zunehmend, wie die strafprozessuale Sicherung und Einziehung von Kryptowerten praktisch abläuft. Das LG Verden (Beschl., 2 Qs 35/25) bestätigte, dass ein Vermögensarrest (§ 111e StPO) und dessen Vollziehung durch Pfändung des Herausgabeanspruchs gegen die Börse (§ 111f StPO) auch bei Exchange-gehaltenen Kryptowerten funktioniert, lehnte zugleich aber eine analoge Anwendung von § 111n StPO auf die vorläufige Herausgabe an Geschädigte ab. Die tatsächliche Auskehr richtet sich damit auch bei Kryptowerten nach dem allgemeinen Vollstreckungsrecht der §§ 459h, 459k StPO und setzt eine rechtskräftige Einziehungsentscheidung voraus.

18.3 Deutschland: Zwangsvollstreckung und Pfändbarkeit von Kryptowerten

Das OLG Köln (Beschl. v. 26.06.2024 – 11 W 15/24) bestätigte, dass Kryptowerte pfändbar sind und Schuldner im Rahmen zumutbarer Mitwirkungshandlungen an der Herausgabe mitwirken müssen. Das OLG Düsseldorf (Beschl. v. 19.01.2021 – 7 W 44/20) und das LG Heilbronn (Beschl. v. 03.03.2021 – Sa 8 O 368/20) hatten die Übertragung von Kryptowerten bereits zuvor als vertretbare Handlung im Sinne des § 887 ZPO eingeordnet. Diese Verfahren betreffen die zivilrechtliche Zwangsvollstreckung und sind von der strafprozessualen Vermögenssicherung nach Kapitel 14 rechtlich zu unterscheiden, obwohl beide auf dieselbe technische Herausforderung – den Zugriff auf fremdverwahrte Kryptowerte – treffen.

18.4 Deutschland: Kryptowerte in der Insolvenz des Verwahrers

Mit dem Finanzmarktdigitalisierungsgesetz (FinmadiG, verkündet am 27.12.2024) und dem Kryptomärkteaufsichtsgesetz (KMAG), die auf dem ZuFinG (2023) aufbauen, existiert seit dem Jahreswechsel 2024/2025 ein eigenständiges Sonderinsolvenzrecht: Nach § 46i Abs. 1 KWG fallen Kryptowerte und kryptografische Schlüssel im Grundsatz nicht in die Insolvenzmasse eines Kryptoverwahrers.

18.5 Deutschland und EU: MiCA, CASP-Lizenzpflicht und Travel Rule

Seit Ende 2024 gilt in der EU mit MiCA ein einheitliches Aufsichtsregime für Kryptowerte-Dienstleister (CASP); die europäische Geldtransferverordnung (Travel Rule) verpflichtet CASPs seit dem 30.12.2024 grundsätzlich ohne Bagatellgrenze zur Erhebung und Weitergabe von Transferdaten. Das deutsche eWpG (seit 2021) und die europäische DLT-Pilotregelung bilden den regulatorischen Rahmen für tokenisierte Wertpapiere und andere RWA. Auf EU-Ebene verpflichtet zudem die Richtlinie (EU) 2024/1260 die Mitgliedstaaten perspektivisch zu wirksameren Rückgabemechanismen für Geschädigte (vgl. Kapitel 14.7); ihre Umsetzung in deutsches Recht steht noch aus.

18.6 Vereinigtes Königreich: Digitale Assets als eigene Eigentumskategorie

Der Court of Appeal entschied in Tulip Trading Ltd v Bitcoin Association for BSV & Ors [2024] EWCA Civ 83, dass digitale Vermögenswerte eine „dritte Kategorie" von Personal Property bilden. Im Fall D'Aloia v Persons Unknown Category A & Ors [2024] EWHC 2342 (Ch) vom 12.09.2024 stellte der High Court fest, dass USDT eigentumsfähig und einem Constructive Trust zugänglich ist. In Osbourne v Persons Unknown & Ors [2022] EWHC 1021 (Comm) und [2023] EWHC 340 (KB) wurden erstmals NFT als eigentumsfähige, gerichtlich schützbare Vermögensgegenstände behandelt. Am 2. Dezember 2025 erhielt der Property (Digital Assets etc) Act 2025 die Royal Assent und verankerte die von den Gerichten entwickelte „dritte Kategorie" gesetzlich.

18.7 USA: Vertragliche Bedingungen, DAOs und Smart Contracts

Das US-Insolvenzgericht im Fall Celsius Network entschied am 04.01.2023, dass Kryptowerte aus „Earn"-Konten aufgrund einer vertraglichen Transfer-of-Title-Klausel Eigentum der Plattform und damit Teil der Insolvenzmasse wurden. Im Verfahren CFTC v. Ooki DAO (Default Judgment v. 08.06.2023) wurde eine DAO erstmals als haftungsfähige „Person" eingeordnet. In Van Loon v. Department of the Treasury (Fifth Circuit, 26.11.2024) entschied das Gericht, dass unveränderliche Smart Contracts keine sanktionierbare „Property" darstellen – eine Entscheidung, die zeigt, wie ungeklärt die rechtliche Einordnung von Programmcode noch ist.

18.8 Rechtsprechungslücke: Swaps, Bridges und Cross-Chain-Sachverhalte

RECHTSPRECHUNGSLÜCKE

Auffällig ist, dass zu den in den Kapiteln 4 bis 9 beschriebenen Konstellationen – insbesondere zur Frage, ob ein Coin-Swap, ein Cross-Chain-Bridge-Vorgang oder eine Asset-Transformation einen rechtlichen Eigentumswechsel oder lediglich eine wirtschaftliche Umwandlung darstellt – nach derzeitigem Rechercheergebnis noch keine veröffentlichte höchst- oder obergerichtliche Rechtsprechung vorliegt. Dies ist keine Randnotiz, sondern der eigentliche Kern der in diesem Beitrag beschriebenen Herausforderung: Gerade die technisch komplexesten und in der Praxis inzwischen alltäglichen Vorgänge sind rechtlich am wenigsten geklärt. Dieselbe Lücke zeigt sich bei der strafprozessualen Vermögenssicherung: Ob und wie ein Vermögensarrest einen Coin-Swap oder eine Bridge-Transaktion „durchgreift", ist – anders als die in Kapitel 14 dargestellte Grundstruktur – höchstrichterlich ebenfalls noch nicht geklärt.

18.9 Übersicht der zitierten Entscheidungen und Regelungen

LAND	GERICHT / RECHTSAKT, DATUM, AZ.	KERNAUSSAGE
Deutschland	OLG Braunschweig, Beschl. v. 18.09.2024 – 1 Ws 185/24	Unbefugte Token-Übertragung mittels bekannter Seedphrase erfüllt weder Diebstahl noch Ausspähen von Daten, Computerbetrug oder Datenveränderung; der darauf gestützte Vermögensarrest wurde aufgehoben.
Deutschland	LG Verden, Beschl. (2 Qs 35/25)	Vermögensarrest und Pfändung von Kryptowerten gegenüber der Börse als Drittschuldnerin zulässig; keine analoge Anwendung von § 111n StPO auf Kryptowerte – keine vorläufige Herausgabe an Geschädigte möglich.
Deutschland	§§ 111b, 111e, 111f, 111n, 111p, 459h, 459k StPO; §§ 73, 73b, 73c StGB	Gesetzlicher Rahmen der strafprozessualen Sicherung, Einziehung und Auskehr an Verletzte; auf Kryptowerte anwendbar, vertieft in Kapitel 14.
Deutschland	OLG Köln, Beschl. v. 26.06.2024 – 11 W 15/24	Kryptowerte sind pfändbar; Schuldner muss zumutbare Mitwirkung, ggf. mit technischer Hilfe Dritter, zur Herausgabe leisten.
Deutschland	OLG Düsseldorf, Beschl. v. 19.01.2021 – 7 W 44/20; LG Heilbronn, Beschl. v. 03.03.2021 – Sa 8 O 368/20	Übertragung von Kryptowerten ist vertretbare Handlung; Vollstreckung nach § 887 ZPO.
Deutschland	FinmadiG (27.12.2024) / KMAG, aufbauend auf ZuFinG (2023); § 46i Abs. 1 KWG	Kryptowerte und kryptografische Schlüssel fallen grundsätzlich nicht in die Insolvenzmasse des Kryptoverwahrers.
EU / Deutschland	MiCA (anwendbar seit 30.12.2024); EU-Geldtransferverordnung/Travel Rule (seit 30.12.2024); eWpG (seit 2021); DLT-Pilotregelung	CASP-Lizenzpflicht für Kryptodienstleister; Travel-Rule-Pflichten ohne Bagatellgrenze; Rechtsrahmen für tokenisierte Wertpapiere/RWA.
EU	Richtlinie (EU) 2024/1260 (Vermögensabschöpfungsrichtlinie)	Verpflichtet Mitgliedstaaten zu wirksameren Rückgabemechanismen für Geschädigte; Umsetzung in Deutschland steht noch aus.
UK	Tulip Trading Ltd v Bitcoin Association for BSV & Ors [2024] EWCA Civ 83	Digitale Assets bilden eine eigenständige dritte Kategorie von Personal Property.
UK	D'Aloia v Persons Unknown Category A & Ors [2024] EWHC 2342 (Ch), 12.09.2024	USDT ist eigentumsfähig und einem Constructive Trust zugänglich; Klage im Einzelfall an fehlendem Tracing-Nachweis gescheitert.
UK	Osbourne v Persons Unknown & Ors [2022] EWHC 1021 (Comm); [2023] EWHC 340 (KB)	NFT werden erstmals als eigentumsfähige, gerichtlich schützbare Vermögensgegenstände behandelt.
UK	Property (Digital Assets etc) Act 2025, in Kraft seit 02.12.2025	Gesetzliche Verankerung digitaler Assets als dritte Kategorie von Personal Property.
USA	In re Celsius Network LLC, U.S. Bankruptcy Court S.D.N.Y., Entsch. v. 04.01.2023	Kryptowerte in Kundenkonten wurden aufgrund vertraglicher Transfer-of-Title-Klausel Eigentum der Plattform und Teil der Insolvenzmasse.
USA	CFTC v. Ooki DAO, N.D. Cal., Default Judgment v. 08.06.2023	Eine DAO wird erstmals als haftungsfähige „Person" nach dem Commodity Exchange Act eingeordnet.
USA	Van Loon v. Department of the Treasury, 5th Cir., Entsch. v. 26.11.2024	Unveränderliche Smart Contracts sind keine sanktionierbare „Property"; OFAC überschritt seine Befugnisse.

Übersicht der ausgewerteten Entscheidungen und Regelungen (DE · UK · USA). *Stand der Recherche: Juli 2026. Aktenzeichen und Fundstellen sind vor einer Verwendung im Einzelfall zu verifizieren.*

19 Konsequenz für die Praxis: Interdisziplinäre Zusammenarbeit statt Einzeldisziplinen

Die in diesem Beitrag dargestellten Entwicklungen führen zu einer grundlegenden Konsequenz für die praktische Aufarbeitung komplexer Kryptosachverhalte. Während die Blockchain-Analyse traditionell überwiegend als technische Disziplin verstanden wurde, überschneiden sich die heute relevanten Fragestellungen zunehmend mit dem Zivilrecht, Strafrecht – einschließlich Vermögensabschöpfung und Einziehung –, Insolvenzrecht, Aufsichtsrecht sowie internationalen Rechtsordnungen.

Ein technischer Blockchain-Forensiker kann regelmäßig rekonstruieren,

- welchen Weg Vermögenswerte genommen haben,
- welche Wallets beteiligt waren,
- welche Dienstleister genutzt wurden,
- welche Smart Contracts aufgerufen wurden,
- welche Asset-Transformationen stattgefunden haben.

Die rechtliche Bewertung dieser Erkenntnisse erfordert hingegen regelmäßig die Prüfung unter anderem,

- ob Eigentumsrechte entstanden oder untergegangen sind,
- welche Herausgabeansprüche bestehen,
- ob und wie eine strafprozessuale Sicherung, Einziehung und Auskehr an Geschädigte erfolgen kann,
- welche Rechtsordnung Anwendung findet,
- welche regulatorischen Vorgaben einschlägig sind,
- welche gerichtlichen Maßnahmen Erfolg versprechen,
- welche Beweisfragen sich in einem gerichtlichen Verfahren stellen.

Umgekehrt verfügt selbst ein hochspezialisierter Rechtsanwalt regelmäßig nicht über die technischen Möglichkeiten und Erfahrungen, komplexe Blockchain-Analysen, Smart-Contract-Auswertungen oder Cross-Chain-Transaktionen eigenständig gerichtsfest zu rekonstruieren. Die zunehmende Komplexität digitaler Vermögenswerte führt deshalb dazu, dass anspruchsvolle Verfahren künftig immer häufiger durch interdisziplinäre Teams bearbeitet werden dürften, in denen technische Sachverständige und spezialisierte Rechtsanwälte ihre jeweiligen Kompetenzen bündeln.

Der Blockchain-Forensiker beantwortet dabei in erster Linie die Frage: „Was ist technisch und wirtschaftlich geschehen?“ Der Rechtsanwalt beantwortet anschließend die Frage: „Welche rechtlichen Konsequenzen ergeben sich daraus – zivilrechtlich wie strafprozessual?“ Erst das Zusammenwirken beider Disziplinen ermöglicht regelmäßig eine belastbare Grundlage für gerichtliche Verfahren, Vermögensabschöpfung, Arrestmaßnahmen, Schadensersatzansprüche oder internationale Rechtshilfe. Aus der zunehmenden Komplexität digitaler Vermögenswerte folgt damit nicht nur das in Kapitel 17 beschriebene neue Berufsbild, sondern auch eine neue Form der Zusammenarbeit zwischen Sachverständigen und spezialisierten Rechtsanwälten: Belastbare Ergebnisse entstehen im Zusammenspiel technischer und juristischer Expertise – nicht durch eine einzelne, alle Fragestellungen abdeckende Instanz.

Damit ist die interdisziplinäre Zusammenarbeit jedoch nur die halbe Konsequenz. Nach Auffassung der Finanz Forensik GmbH reicht es nicht aus, technische Sachverständige und Rechtsanwälte in jedem Einzelfall neu zusammenzuführen – so, wie es die Kapitel 3, 7, 13 und 14 am durchgehenden Praxisbeispiel gezeigt haben, wo dieselbe Frage einmal on-chain (Kapitel 7), einmal aufsichtsrechtlich (Kapitel 13) und einmal strafprozessual (Kapitel 14) beantwortet werden musste, ohne dass eine der drei Antwor-

ten für sich genommen ausgereicht hätte. Ein Fall, der von der Blockchain bis zur Auskehr durchgehend nur einer einzigen Sachverständigenlogik folgt, ist im Ergebnis belastbarer als eine Kette getrennt beauftragter Einzelgutachten.

Wir sind daher der Auffassung, dass sich die digitale Vermögensforensik nicht auf eine Methode der Zusammenarbeit reduzieren lässt, sondern sich – mit eigenen Ausbildungswegen, eigenen Qualitätsstandards und einem eigenen Selbstverständnis, wie in Kapitel 17 skizziert – zu einer eigenständigen forensischen Sachverständigendisziplin entwickeln muss, die neben etablierten Bereichen wie der IT-Forensik oder der Bau- und Immobilienbewertung ihren festen Platz in Gerichtsverfahren, Insolvenzen und Ermittlungen einnimmt. Interdisziplinäre Zusammenarbeit ist dafür die Voraussetzung – die eigenständige Disziplin ist das Ziel. ■

Fazit

Die Blockchain beantwortet die Frage: „Was ist technisch passiert?“ Gerichte und Ermittlungsbehörden müssen jedoch zusätzlich wissen:

- Wem gehörten die Vermögenswerte?
- Haben sich Eigentumsrechte geändert?
- Welche rechtlichen Folgen ergeben sich aus den Transaktionen, Smart-Contract-Interaktionen oder RWA-Tokenisierungen?
- Welche Ansprüche bestehen weiterhin?
- Welche Bedeutung haben Swaps, Bridges, DeFi-Protokolle und Exchange-Dienstleister für die Vermögenszuordnung?
- Können gesicherte oder eingezogene Werte tatsächlich – und über welchen Weg – an die Geschädigten zurückfließen?

Die Zukunft der Blockchain-Forensik liegt deshalb nicht mehr ausschließlich in der technischen Analyse von Transaktionen. Sie entwickelt sich zunehmend zu einer interdisziplinären digitalen Vermögensforensik, die Informatik, Blockchain-Technologie, Zivilrecht, Strafrecht, Aufsichtsrecht und wirtschaftliche Bewertung miteinander verbindet – ergänzt um ein eigenständiges Verständnis von Smart Contracts, NFT, tokenisierten realen Vermögenswerten, der strafprozessualen Vermögenssicherung und Einziehung sowie der neuen europäischen Aufsichtsarchitektur rund um MiCA.

Nur ein solcher ganzheitlicher Ansatz ermöglicht künftig gerichtsfeste Gutachten, die nicht nur den Weg digitaler Vermögenswerte rekonstruieren, sondern deren rechtliche und wirtschaftliche Bedeutung nachvollziehbar einordnen – bis hin zu der für Geschädigte entscheidenden Frage, ob und wann sie tatsächlich etwas zurückerhalten. Die in Kapitel 18 dargestellte Rechtsprechung zeigt: Diese Entwicklung hat längst begonnen – von der deutschen Straf- und Vollstreckungsjustiz über die zivilrechtliche Vollstreckungspraxis bis hin zur gesetzlichen Neuordnung des Eigentumsrechts an digitalen Vermögenswerten im Vereinigten Königreich und der Haftung von DAOs in den USA. Die digitale Vermögensforensik ist damit keine Zukunftsvision mehr, sondern eine Disziplin, deren Grundzüge sich bereits heute in Gerichtsentscheidungen, Gesetzen und Marktentwicklungen abzeichnen.

Das Praxisbeispiel aus Kapitel 3 fasst diesen Weg exemplarisch zusammen: Aus 2,0 BTC, die ein Geschädigter im Glauben an einen Recovery-Dienst überwies, wurde über ChangeNOW und das Tron-Netzwerk ein USDT-Bestand auf einem HTX-Konto (Kapitel 7), aus dessen KYC- und Travel-Rule-Daten die für den Vermögensarrest nötigen Anknüpfungstatsachen stammten (Kapitel 13), der schließlich über § 111e StPO gesichert, über §§ 73 ff. StGB eingezogen und – mit den in Kapitel 14.5 beschriebenen

Einschränkungen und Fristen – über § 459h StPO an den Geschädigten ausgekehrt werden konnte. Nach Auffassung der Finanz Forensik GmbH liegt genau in dieser durchgängigen Kette – von der ersten on-chain-Beobachtung bis zur letzten Vollstreckungsvorschrift – der Maßstab, an dem sich digitale Vermögensforensik künftig messen lassen muss.

RECHTLICHER HINWEIS

Bei der rechtlichen Einordnung ist stets zu berücksichtigen, dass die Bewertung von Eigentumsübergängen, Herausgabeansprüchen, strafprozessualer Vermögenssicherung oder den Folgen eines Asset- oder Netzwerkwechsels, einer Smart-Contract-Interaktion oder einer RWA-Tokenisierung von der jeweils anwendbaren Rechtsordnung und den konkreten Umständen des Einzelfalls abhängt. Ein technischer Swap, Transfer oder Vertragsaufruf führt nicht automatisch zu einer bestimmten rechtlichen Folge; diese bedarf stets einer gesonderten juristischen Prüfung. Die in diesem Beitrag zitierte Rechtsprechung und Regulierung gibt den Stand zum Zeitpunkt der Veröffentlichung wieder und kann durch neuere Entwicklungen überholt werden.

QUELLENVERZEICHNIS (AUSWAHL)

DEUTSCHLAND

OLG Braunschweig, Beschl. v. 18.09.2024 – 1 Ws 185/24; Besprechung: Rechtsanwalt Jens Ferner, ferner-alsdorf.de, „OLG Braunschweig: Virtueller Diebstahl von Kryptowährungen straflos“ · LG Verden, Beschl. (2 Qs 35/25); Besprechung: Rechtsanwalt Jens Ferner, ferner-alsdorf.de, „Keine vorläufige Herausgabe von Kryptowerten nach § 111n StPO“, jurisPR-ITR 3/2026 · §§ 111b, 111e, 111f, 111n, 111p, 111l StPO (Sicherstellung, Vermögensarrest, Vollziehung, vorläufige Herausgabe, Notveräußerung, Mitteilung an Verletzte) · §§ 73, 73b, 73c, 73e StGB (Einziehung von Taterträgen, Einziehung bei Drittbegünstigten, Wertersatzeinziehung) · §§ 459h, 459k StPO (Entschädigung Verletzter, Verfahren bei Auskehrung des Verwertungserlöses) · §§ 403 ff. StPO (Adhäsionsverfahren) · OLG Köln, Beschl. v. 26.06.2024 – 11 W 15/24 · OLG Düsseldorf, Beschl. v. 19.01.2021 – 7 W 44/20; LG Heilbronn, Beschl. v. 03.03.2021 – Sa 8 O 368/20 · Finanzmarktdigitalisierungsgesetz (FinmadiG, verkündet 27.12.2024); Kryptomärkteaufsichtsgesetz (KMAG); Zukunftsfinanzierungsgesetz (ZuFinG, 2023); § 46i KWG.

EU & VEREINIGTES KÖNIGREICH

Verordnung (EU) 2023/1114 (MiCA), anwendbar seit 30.12.2024; Verordnung (EU) 2023/1113 (Geldtransferverordnung/Travel Rule); Richtlinie (EU) 2024/1260 (Vermögensabschöpfungsrichtlinie); Gesetz über elektronische Wertpapiere (eWpG, seit 2021); EU-DLT-Pilotregelung · Tulip Trading Ltd v Bitcoin Association for BSV & Ors [2024] EWCA Civ 83 · D'Aloia v Persons Unknown Category A & Ors [2024] EWHC 2342 (Ch), 12.09.2024 · Osbourne v Persons Unknown & Ors [2022] EWHC 1021 (Comm); [2023] EWHC 340 (KB) · Property (Digital Assets etc) Act 2025 (Royal Assent und Inkrafttreten: 02.12.2025).

USA & MARKTDATEN

In re Celsius Network LLC, U.S. Bankruptcy Court für den Südbezirk von New York, Entscheidung v. 04.01.2023 (Richter Martin Glenn) · CFTC v. Ooki DAO, U.S. District Court N.D. Cal., Default Judgment v. 08.06.2023 · Van Loon v. Department of the Treasury, U.S. Court of Appeals for the Fifth Circuit, Entsch. v. 26.11.2024 · Marktdaten Tokenized Real-World Assets / BlackRock BUIDL: branchenübliche Marktbeobachtungen, Stand Juni 2026.

ÜBER DEN AUTOR

David Lüdtke

Geschäftsführer · OSINT-Analyst & Krypto-Forensiker · Finanz Forensik GmbH

Gerichtsfeste Kryptotransaktionsanalysen, OSINT-gestützte Vermögensermittlung und gutachterliche Aufbereitung für Strafverteidiger, Insolvenzverwalter und Unternehmen. Zertifiziert als Crystal Expert (CECF · CEEI · CEUI). **Kontakt:** postfach@finanz-forensik.de · +49 6057 9189145 · www.finanz-forensik.de

Herausgeber: Finanz Forensik GmbH · Würzburger Str. 59, 63639 Flörsbachtal · HRB 100521, Amtsgericht Hanau · USt-IdNr. DE454473675 · Geschäftsführung: Lydia Bonhard-Lüdtke, David Lüdtke. Dieses Whitepaper dient der allgemeinen Information und gibt den Rechts- und Diskussionsstand Juli 2026 wieder; es stellt keine Rechts-, Steuer- oder Anlageberatung dar und begründet kein Mandatsverhältnis.

© 2026 Finanz Forensik GmbH — alle Rechte vorbehalten.