Bundesministerium
Inneres

Sicherheitsakademie

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis


Haslhofer, Bernhard

# Die Spur des digitalen Krypto-Geldes. Herausforderungen und Lösungsansätze für die Strafverfolgung

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2/2026), 76-86.

doi: 10.7396/2026_2_F

*Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:*

Haslhofer, Bernhard (2026). Die Spur des digitalen Krypto-Geldes. Herausforderungen und Lösungsansätze für die Strafverfolgung, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 76-86, Online: https://dx.doi.org/10.7396/2026_2_F.



Online publiziert: 7/2026

# Die Spur des digitalen Krypto-Geldes

## Herausforderungen und Lösungsansätze für die Strafverfolgung

**BERNHARD HASLHOFER,**
*leitet die Forschungsgruppe Digital Currency Ecosystems am Complexity Science Hub in Wien.*

Kryptowährungen wie Bitcoin sind zum bevorzugten Zahlungsmittel für Cybercrime-Aktivitäten geworden, etwa für Ransomware-Angriffe, Investmentbetrug oder den Handel mit Missbrauchsdarstellungen. Täterinnen und Täter nutzen die vermeintliche Anonymität digitaler Währungen, um Zahlungsströme zu verschleiern. Um diese Ströme nachzuverfolgen, hat sich das Follow-the-Money-Prinzip als zentrale Ermittlungsmethode etabliert. Forensische Werkzeuge sind bereits im Einsatz, doch es bestehen Weiterentwicklungspotenziale in vier Bereichen: einfache Werkzeuge für eine breitere Ermittlerbasis, frühzeitige Erkennung von Fallzusammenhängen zur Vermeidung von Doppelermittlungen, wissenschaftliche Validierung gängiger Analysemethoden für die gerichtliche Verwertbarkeit sowie datengetriebene Ansätze als Antwort auf die zunehmende Automatisierung auf Täterseite. Dieser Beitrag zeigt anhand unserer Erfahrungen aus der Zusammenarbeit mit bayerischen Strafverfolgungsbehörden diese Handlungsfelder auf, skizziert konkrete Lösungsansätze und diskutiert deren Grenzen.

### 1. EINLEITUNG

Die Veröffentlichung des Whitepapers unter dem Pseudonym Satoshi Nakamoto (vgl. Nakamoto 2008) markierte im Jahr 2009 den Beginn dezentraler digitaler Zahlungssysteme. Ursprünglich als technologisches Experiment einer kleinen Gruppe von Kryptografie-Enthusiastinnen und -Enthusiasten konzipiert, entwickelte sich diese Innovation innerhalb weniger Jahre zu einem globalen Phänomen, das sowohl die Finanzwelt als auch die Strafverfolgungsbehörden vor erhebliche Herausforderungen stellt.

Kryptowährungen ermöglichen den Transfer von Werten ohne klassische Finanzintermediäre wie Banken oder Zahlungsdienstleister. Alle Transaktionen werden in einer öffentlich einsehbaren, dezentralen Datenbank gespeichert, der Blockchain. Diese Transaktionen sind zwar transparent, erfolgen jedoch pseudonym: Wer hinter einer bestimmten Adresse steht, lässt sich nicht unmittelbar aus den Transaktionsdaten ablesen. Schon frühzeitige wissenschaftliche Arbeiten haben gezeigt, dass diese Pseudonymität keinen vollständigen Schutz bietet. Ron und Shamir (vgl. Ron/Shamir 2013) konnten durch eine quantitative Analyse des Bitcoin-Transaktionsgraphen nachweisen, dass sich wesentliche Strukturen des Zahlungsverkehrs rekonstruieren und einzelnen Entitäten zuordnen lassen. Trotzdem hat die Pseudonymität Kryptowährungen früh zu einem attraktiven Zahlungsmittel für kriminelle Aktivitäten gemacht.

Die ersten prominenten Fälle krimineller Nutzung standen im Zusammenhang mit Online-Marktplätzen für illegale Güter. Der 2011 gegründete und 2013 vom FBI geschlossene Marktplatz Silk Road gilt als Wegbereiter für den Einsatz von Bitcoin im Drogenhandel (vgl. Meiklejohn et al. 2013). Seither hat sich das Spektrum deutlich erweitert. Ransomware-Angriffe, bei denen Schadsoftware die Daten von Opfern verschlüsselt und sie nur gegen Zahlung eines Lösegelds in Kryptowährung freigibt, zählen inzwischen zu den folgenschwersten Cybercrime-Phänomenen. Allein 2024 beliefen sich die Gesamtzuflüsse an als illegal eingestufte Kryptowährungsadressen auf mindestens 40,9 Milliarden US-Dollar (vgl. Chainalysis 2025), wobei Ransomware, Betrug und Darknet-Handel die größten Kategorien darstellten.[1] Hinzu kommen Investmentbetrug, Erpressung, Geldwäsche sowie der Handel mit Darstellungen sexuellen Kindesmissbrauchs.

Das Prinzip „Follow the Money", also die Spur des Geldes vom Opfer zur Täterin oder zum Täter zu verfolgen und umgekehrt, hat sich als eine der wirksamsten Ermittlungsmethoden gegen Finanzkriminalität bewährt. In der traditionellen Finanzwelt geschieht dies über Kontenauskünfte und die Zusammenarbeit mit Banken. Bei Kryptowährungen eröffnet die Transparenz der Blockchain neue Möglichkeiten, denn jede Transaktion ist öffentlich einsehbar und dauerhaft gespeichert. Die Pseudonymität der Adressen bleibt dabei jedoch eine Hürde, da die Zuordnung zu realen Personen oder Organisationen zusätzliche Ermittlungsschritte erfordert.

Seit einigen Jahren haben sich spezialisierte Werkzeuge und Methoden für die Kryptowährungsforensik herausgebildet. Kommerzielle Anbieter haben Plattformen geschaffen, mit denen Ermittlerinnen und Ermittler Transaktionsflüsse visualisieren, Adressen clustern und bekannten Entitäten wie Kryptowährungsbörsen, Darknet-Marktplätzen oder Betrugsfällen zuordnen können. Diese Werkzeuge haben wesentlich zur Aufklärung bedeutender Fälle beigetragen, beispielsweise bei der Rückverfolgung gestohlener Kryptowährungswerte im Milliardenbereich oder bei der Identifizierung von Betreiberinnen und Betreibern großer Darknet-Marktplätze.

Das Feld entwickelt sich jedoch rasant weiter. Tätergruppen agieren global vernetzt, automatisiert und technisch versiert. Generative Methoden der künstlichen Intelligenz (KI) ermöglichen es kriminellen Akteurinnen und Akteuren, neue Angriffsvektoren rasch umzusetzen und Verschleierungstechniken weiterzuentwickeln. Besonders herausfordernd sind Privacy Coins wie Monero oder Zcash, die im Unterschied zu Bitcoin erweiterte kryptografische Verfahren einsetzen, um Transaktionsbeträge sowie Absende- und Empfangsadressen zu verschleiern. Möser u.a. (vgl. Möser et al. 2018) haben gezeigt, dass die Anonymitätsgarantien von Monero in der Praxis zwar nicht absolut sind, die forensische Analyse jedoch erheblich erschwert wird, da herkömmliche Heuristiken wie das Adress-Clustering hier nicht greifen. Dezentrale Finanzprotokolle, bekannt als Decentralized Finance (DeFi), erzeugen zusätzlich komplexe Transaktionsketten über mehrere Blockchains hinweg, die mit herkömmlichen Methoden kaum noch nachvollziehbar sind (vgl. Auer et al. 2023).

Auf regulatorischer Seite zeichnen sich Entwicklungen ab, die der Strafverfolgung neue Ansatzpunkte eröffnen können. Die Markets in Crypto-Assets Regulation (MiCAR) der Europäischen Union (vgl. Europäisches Parlament/Rat der Europäischen Union 2023), seit Ende 2024 voll-

ständig in Kraft, etabliert erstmals einen umfassenden Regulierungsrahmen für Kryptowährungsdienstleister in der EU, einschließlich Zulassungspflichten und Anforderungen an die Geldwäscheprävention. Die Travel Rule, die auf Empfehlungen der Financial Action Task Force (FATF) zurückgeht, verpflichtet Kryptowährungsdienstleister zudem, bei Transfers ab einem bestimmten Schwellenwert Informationen über die Auftraggeberin oder den Auftraggeber sowie die Begünstigte oder den Begünstigten zu erheben und weiterzuleiten.[2] Diese Instrumente können die Ermittlungsarbeit erleichtern, indem sie die Identifizierung der beteiligten Personen vereinfachen. Ob sie in der Praxis wirksam sind, wird sich erst zeigen, wenn sie flächendeckend um- und durchgesetzt werden.

Strafverfolgungsbehörden stehen vor der Herausforderung, mit den technologischen Entwicklungen Schritt zu halten, ihre Methoden und Werkzeuge kontinuierlich weiterzuentwickeln und diese auf ein solides wissenschaftliches Fundament zu stellen. Aufbauend auf Erfahrungen aus der Zusammenarbeit mit bayerischen Strafverfolgungsbehörden werden in diesem Beitrag vier zentrale Handlungsfelder identifiziert und für jedes konkrete Lösungsansätze vorgestellt: die Verfügbarkeit von Werkzeugen, das Erkennen von Fallzusammenhängen, die Verlässlichkeit eingesetzter Methoden sowie die Automatisierung und ein netzwerkzentrierter Ermittlungsansatz.

## 2. VERFÜGBARKEIT VON WERKZEUGEN

Internationale Leitfäden wie die INTERPOL Guidelines on the Darknet and Cryptocurrencies (vgl. INTERPOL 2020) oder das OSZE Handbook for Dealing with Virtual Currencies in Criminal Proceedings (vgl. OSCE 2022) belegen, dass die Strafverfolgung die Relevanz von Kryptowährungen erkannt hat. Kryptowährungskriminalität ist längst kein Nischenphänomen mehr. Mit der wachsenden Verbreitung von Kryptowährungen unter der Bevölkerung steigt die Wahrscheinlichkeit, dass Ermittlerinnen und Ermittler auch in allgemeinen Strafverfahren auf Kryptowährungsadressen, Wallet-Dateien oder Transaktionsnachweise stoßen. Das betrifft spezialisierte Cybercrime-Einheiten ebenso wie Ermittlerinnen und Ermittler in Bereichen wie dem allgemeinen Betrug, der Drogenkriminalität oder der Vermögensabschöpfung.

Ein Vergleich mit dem polizeilichen Alltag macht das Problem greifbar: Heute ist es selbstverständlich, dass Ermittlerinnen und Ermittler ein Autokennzeichen in einer Datenbank abfragen oder eine Kontoauskunft zu einer internationalen Bankkontonummer (IBAN) einholen. Diese Routineabfragen erfordern kein Expertenwissen. Genauso sollte es in Zukunft möglich sein, grundlegende Aufgaben der Kryptowährungsforensik ohne Spezialausbildung zu erledigen: eine Kryptowährungsadresse abfragen, die zugehörige Börse identifizieren und einfache Zahlungsströme nachverfolgen.

Die derzeitige Situation steht diesem Ziel entgegen. Die am Markt verfügbaren forensischen Werkzeuge sind hochspezialisiert und teuer. Hinzu kommen kostenintensive Schulungen, die in der Regel von den Herstellern selbst durchgeführt werden. In der Praxis haben deshalb nur wenige Spezialistinnen und Spezialisten Zugang zu diesen Werkzeugen. Die Folge ist ein Engpass: Die Zahl der Fälle mit Kryptowährungsbezug steigt stetig, doch die Kapazität für deren forensische Aufarbeitung bleibt begrenzt.

Ein naheliegender Lösungsansatz besteht darin, die bestehenden Spezialwerkzeuge um einfachere und kostengünstigere

Alternativen zu ergänzen. Diese brauchen nicht den vollen Funktionsumfang abzudecken, sondern sollen grundlegende Ermittlungsschritte ermöglichen: eine Kryptowährungsadresse abfragen, sie bekannten Diensten zuordnen, einfache Zahlungsflüsse darstellen und die Ergebnisse für die Akte dokumentieren. Solche niedrigschwelligen Werkzeuge sollen die kommerziellen Speziallösungen nicht ersetzen. Für komplexe Fälle, etwa die Rückverfolgung von Geldern über mehrere Blockchains oder die Analyse verschleierter Transaktionsketten, bleiben spezialisierte Werkzeuge mit umfassenden Attribution-Datenbanken notwendig.

Erfahrungen aus der Praxis zeigen, dass viele Fälle mit Kryptowährungsbezug keine hochspezialisierten Werkzeuge erfordern. Häufig reicht es aus, eine vom Opfer gemeldete Kryptowährungsadresse abzufragen, den zugehörigen Dienst, beispielsweise eine Kryptowährungsbörse, zu identifizieren und dort eine Auskunft einzuholen. Dieses Vorgehen ähnelt der klassischen Kontoabfrage im Bankenwesen und kann von Ermittlerinnen und Ermittlern durchgeführt werden, sofern geeignete Werkzeuge zur Verfügung stehen.

Die breitere Verfügbarkeit solcher Werkzeuge hat neben der Entlastung der Spezialistinnen und Spezialisten einen weiteren Effekt: Sie fördert die Verbreitung von Wissen innerhalb der Ermittlungsbehörden. Regelmäßige Anwendung einfacher Kryptowährungsabfragen ermöglicht den Aufbau eines Grundverständnisses für die Funktionsweise dieser Technologie und erleichtert die Einschätzung, wann ein Fall an Spezialistinnen und Spezialisten übergeben werden sollte. Dieser Wissenstransfer stärkt die langfristige Handlungsfähigkeit der Strafverfolgungsbehörden.

Die Entwicklung solcher niedrigschwelligen Werkzeuge sollte sich an den tatsächlichen Bedürfnissen der Ermittlungspraxis orientieren und in enger Zusammenarbeit mit den Strafverfolgungsbehörden erfolgen. Open-Source-Ansätze können einen wichtigen Beitrag leisten, da sie die Kosten senken und zugleich Transparenz sowie Nachvollziehbarkeit der eingesetzten Methoden gewährleisten. Ohne diese Transparenz ist die gerichtliche Verwertbarkeit der Ergebnisse oft nicht gegeben. Open-Source-Lösungen bringen jedoch eigene Herausforderungen mit sich: Langfristige Pflege und Weiterentwicklung erfordern institutionelle Verankerung und kontinuierliche Ressourcen. Zudem können sie die umfangreichen Attribution-Datenbanken kommerzieller Anbieter, die auf jahrelanger Datensammlung und proprietären Quellen basieren, nicht ohne Weiteres ersetzen. Eine realistische Strategie sollte daher beide Ansätze kombinieren.

## 3. ERKENNEN VON FALLZUSAMMENHÄNGEN

Cybercrime-Akteurinnen und -Akteure agieren global und hochvernetzt. Ein einzelner Ransomware-Angriff kann Hunderte von Opfern in verschiedenen Ländern betreffen, eine Betrugsmasche kann gleichzeitig in mehreren Bundesländern oder Staaten Schaden anrichten. Die Strafverfolgung hingegen ist nach wie vor überwiegend lokal organisiert. Zuständigkeiten folgen territorialen Grenzen, und die Zusammenarbeit über Ländergrenzen hinweg, ob innerstaatlich zwischen Bundesländern oder international zwischen Staaten, ist oft aufwändig.

Dieses Missverhältnis zeigt sich bei Kryptowährungsermittlungen besonders deutlich. In der Praxis erstattet ein Opfer seine Anzeige bei der örtlich zuständigen Polizeidienststelle. Werden dabei Kryptowährungsadressen oder Transaktionsnachweise vorgelegt, beginnen die Ermittlungen lokal. Weitere Opfer desselben Betrugs oder derselben Ransomware-

Kampagne erstatten derweil bei anderen Dienststellen Anzeige. So entstehen parallel laufende, voneinander isolierte Ermittlungsverfahren.

Die Folgen: Ermittlungsressourcen werden mehrfach gebunden, ohne Mehrwert zu erzielen. Erkenntnisse aus einem Verfahren stehen anderen Verfahren zum selben Phänomen nicht zur Verfügung. Die Gesamtdimension eines kriminellen Netzwerks bleibt unerkannt, weil jede Dienststelle nur einen Ausschnitt sieht. Und die Chancen auf erfolgreiche Strafverfolgung sinken, weil Beweismittel nicht gebündelt und Maßnahmen nicht koordiniert werden. Das betrifft auch die Vermögensabschöpfung: Ohne Kenntnis der Gesamtdimension einer kriminellen Kampagne bleiben Sicherstellungsansprüche auf Teilbeträge beschränkt, obwohl die zugrunde liegenden Kryptowährungswerte möglicherweise identifizierbar und auffindbar wären.

Einen Ausweg bietet die frühzeitige Erkennung von Fallzusammenhängen auf Basis gemeinsam genutzter Kryptowährungsadressen. Die Grundidee ist einfach: Taucht dieselbe Kryptowährungsadresse in zwei oder mehr unabhängigen Ermittlungsverfahren auf, besteht ein potenzieller Zusammenhang. Dieser kann darauf hindeuten, dass dieselbe Täterin oder derselbe Täter hinter mehreren Straftaten steht, dass die Fälle Teil einer größeren kriminellen Kampagne sind oder dass eine gemeinsame Infrastruktur genutzt wird.

Eine in Kooperation mit der bayerischen Zentralstelle Cybercrime durchgeführte Studie (vgl. Haslhofer et al. 2023) hat das Potenzial dieses Ansatzes belegt. Kryptowährungsadressen aus einer Vielzahl von Ermittlungsverfahren wurden systematisch abgeglichen. Dabei zeigte sich, dass ein erheblicher Anteil der untersuchten Verfahren über gemeinsame Adressen miteinander in Verbindung stand. Viele dieser Zusammenhänge waren den zuständigen Ermittlerinnen und Ermittlern zuvor nicht bekannt gewesen.

Praktisch erfordert dieser Ansatz die zentrale oder zumindest koordinierte Erfassung von Kryptowährungsadressen in laufenden Ermittlungsverfahren. Sobald eine Ermittlerin oder ein Ermittler eine Adresse in einem neuen Verfahren erfasst, wird automatisch geprüft, ob sie bereits in einem anderen Verfahren bekannt ist. Bei einer Übereinstimmung werden die beteiligten Dienststellen benachrichtigt, sodass eine Abstimmung und gegebenenfalls eine Zusammenführung der Verfahren erfolgen können. Die Staatsanwaltschaft sollte von Beginn an eingebunden sein, da die Zusammenführung von Verfahren eine staatsanwaltschaftliche Entscheidung erfordert und eine frühzeitige Koordination die Verfahrenssteuerung erleichtert.

Konzeptionell ist dieser Mechanismus vergleichbar mit bestehenden kriminalistischen Datenbanken, etwa zur Erfassung von DNA-Spuren oder Fingerabdrücken.[3] Wie bei diesen etablierten Instrumenten liegt der Schlüssel zum Erfolg in der konsequenten und frühzeitigen Erfassung der relevanten Daten, also der Kryptowährungsadressen, sowie in der organisatorischen Verankerung des Abgleichprozesses in den bestehenden Ermittlungsabläufen.

Eine systematische Fallverknüpfung vermeidet Doppelarbeit, doch ihr Nutzen reicht über diese hinaus. Wenn Erkenntnisse aus verschiedenen Verfahren zusammenfließen, entsteht ein umfassenderes Bild der kriminellen Aktivitäten. Das kann Ermittlungen beschleunigen, die Beweislage verbessern und die Wahrscheinlichkeit einer erfolgreichen Strafverfolgung sowie der Vermögensabschöpfung erhöhen. Die aggregierte Betrachtung ermöglicht zudem eine realistischere Einschätzung der Schadensdimension, was für die Priorisierung von Verfahren und die Zuweisung von Ressourcen relevant ist.

## 4. VERLÄSSLICHKEIT EINGESETZTER METHODEN

Die forensische Analyse von Kryptowährungstransaktionen stützt sich auf Methoden, die in den vergangenen Jahren in Wissenschaft und Praxis entwickelt worden sind. Am weitesten verbreitet ist das Adress-Clustering: Dabei werden mehrere Kryptowährungsadressen, die vermutlich derselben Entität angehören, automatisiert zu einer Gruppe zusammengefasst. Die zugrunde liegende Annahme lautet, dass Adressen, die gemeinsam als Eingabe (Input) einer Transaktion verwendet werden, mit hoher Wahrscheinlichkeit von derselben Person oder Organisation kontrolliert werden. Diese als Common-Input-Ownership-Heuristik bezeichnete Methode wird in nahezu allen kommerziellen und akademischen Analysewerkzeugen eingesetzt (vgl. Ron/Shamir 2013; Meiklejohn et al. 2013).

In der Praxis hat sich die Methode bewährt: Sie ermöglicht es, aus der Vielzahl einzelner Adressen auf der Blockchain zusammenhängende Wallet-Strukturen zu rekonstruieren und die Aktivitäten einer Entität über viele Transaktionen hinweg nachzuvollziehen. In Kombination mit Attribution-Tags, also der Zuordnung von Adress-Clustern zu bekannten Diensten wie Kryptowährungsbörsen, Darknet-Marktplätzen oder Zahlungsdienstleistern, entsteht ein wirksames Instrument zur Nachverfolgung von Zahlungsflüssen.

Doch wie verlässlich sind diese Methoden tatsächlich? Haslhofer u.a. (vgl. Haslhofer et al. 2020) haben die Herausforderungen des Adress-Clusterings systematisch untersucht. Sie zeigen, dass die Common-Input-Ownership-Heuristik auf Annahmen beruht, die in der Praxis nicht immer zutreffen. CoinJoin-Transaktionen, bei denen mehrere Nutzerinnen und Nutzer ihre Transaktionen bewusst zusammenführen, um die Nachverfolgbarkeit zu erschweren, können zum Beispiel zu fehlerhaften Clustern führen: Adressen verschiedener Personen werden dann fälschlicherweise einer einzigen Entität zugeordnet (vgl. ebd.). CoinJoin-Verfahren haben sich zudem deutlich weiterentwickelt. Moderne Implementierungen erzeugen Transaktionen, die sich zunehmend schwerer von regulären Transaktionen unterscheiden lassen, was die Zuverlässigkeit automatisierter Clustering-Verfahren weiter beeinträchtigt.

Kappos u.a. (vgl. Kappos et al. 2018) haben in einer empirischen Evaluierung gezeigt, dass unterschiedliche Clustering-Heuristiken zu teils stark voneinander abweichenden Ergebnissen führen und die Genauigkeit stark vom jeweiligen Anwendungskontext abhängt. Bislang ist die Genauigkeit dieser Methoden nicht systematisch und wissenschaftlich fundiert nachgewiesen. Es fehlen umfassende Ground-Truth-Datensätze, anhand derer sich die Fehlerraten, sowohl falsch positive als auch falsch negative Zuordnungen, zuverlässig quantifizieren ließen. Für Ermittlerinnen und Ermittler, die sich auf die Ergebnisse eines Clustering-Algorithmus stützen, bedeutet das: Sie können die Genauigkeit dieser Ergebnisse nicht beziffern.

Aus rechtlicher Sicht ist das problematisch. Beweismittel haben in einem Strafverfahren bestimmten Qualitätsanforderungen zu genügen. Die Methodik, mit der ein Beweismittel gewonnen wurde, sollte nachvollziehbar und in ihrer Aussagekraft einschätzbar sein. Ist die Fehlerrate einer Methode unbekannt, stellen Verteidigerinnen und Verteidiger sie zu Recht in Frage. In einigen Jurisdiktionen haben Gerichte bereits begonnen, die Ergebnisse von Blockchain-Analysen kritisch zu hinterfragen, insbesondere wenn sie nicht durch unabhängige Beweismittel gestützt werden. Auch gewinnt die Frage an Bedeu-

tung, ob und wann eine Sachverständige oder ein Sachverständiger für die Interpretation von Blockchain-Analysen hinzugezogen werden sollte, da die technische Komplexität die unmittelbare richterliche Beweiswürdigung erschwert.

Das Adress-Clustering sollte daher als Ermittlungsansatz verstanden werden, der Indizien liefert, nicht als eigenständiges Beweismittel. Seine Ergebnisse können Ermittlungsrichtungen aufzeigen und dabei helfen, relevante Adressen und Transaktionen zu identifizieren. Sie bedürfen jedoch stets der Absicherung durch weitere, unabhängig überprüfbare Erkenntnisse. Stattdessen empfiehlt sich ein Ansatz, der die Spur des Geldes konsequent an konkrete, überprüfbare Fakten bindet. Konkret heißt das: Der Fluss von Kryptowährungswerten wird anhand konkreter Adressen und der zwischen ihnen stattfindenden Transaktionen dokumentiert. Jede einzelne Transaktion ist in der Blockchain nachprüfbar gespeichert und kann unabhängig voneinander verifiziert werden.

Der entscheidende Vorteil dieses faktenbasierten Ansatzes liegt in der Reproduzierbarkeit. Eine Gutachterin oder ein Gutachter, eine Richterin oder ein Richter, eine Verteidigerin oder ein Verteidiger kann die dargestellte Transaktionskette unabhängig nachvollziehen, indem sie beziehungsweise er die entsprechenden Transaktionen in der Blockchain nachschlägt. Bei Clustering-Ergebnissen ist das anders: Ihre Reproduktion erfordert Kenntnis des verwendeten Algorithmus, der eingesetzten Heuristiken und der zugrunde liegenden Daten. Kommerzielle Werkzeuge behandeln diese Informationen häufig als Geschäftsgeheimnis.

Clustering-Methoden haben dennoch ihren Stellenwert für die Ermittlungsarbeit. Sie eignen sich gut zur Hypothesengenerierung und helfen Ermittlerinnen und Ermittlern, relevante Zusammenhänge zu erkennen, denen anschließend mit faktenbasierten Methoden nachgegangen wird. Die Unterscheidung zwischen hypothesengenerierenden Werkzeugen und beweissichernden Methoden bleibt dabei grundlegend für die Integrität der forensischen Arbeit.

## 5. AUTOMATISIERUNG UND NETZWERKZENTRIERTER ANSATZ

Professionelle Tätergruppen im Bereich der Cyberkriminalität arbeiten heute weitgehend automatisiert. Geldwäschenetzwerke erstrecken sich über eine Vielzahl von Blockchains und setzen komplexe Transaktionsketten ein, um die Herkunft kriminell erlangten Geldes zu verschleiern. Automatisierte Systeme verschieben Kryptowährungswerte über Dutzende oder Hunderte von Zwischenadressen, teilen Beträge auf und führen sie wieder zusammen, konvertieren zwischen verschiedenen Kryptowährungen und schleusen Gelder über dezentrale Börsen, Mixer-Dienste und Cross-Chain-Bridges. Skripte und Bots steuern diese Infrastrukturen rund um die Uhr.

Auf der Gegenseite verfolgen Ermittlerinnen und Ermittler die Spur des Geldes nach wie vor weitgehend manuell. Sie arbeiten Transaktionsketten Glied für Glied ab, dokumentieren jeden einzelnen Hop und versuchen, den Gesamtfluss nachzuvollziehen. Das führt zu einem wachsenden Skalierungsproblem: Während Tätergruppen innerhalb kürzester Zeit Tausende von Transaktionen durchführen, kann die forensische Analyse einer einzigen komplexen Transaktionskette Tage oder Wochen dauern.

Paquet-Clouston u.a. haben am Beispiel von Sextortion-Kampagnen im Bitcoin-Ökosystem gezeigt, wie automatisierte kriminelle Infrastrukturen funktionie-

ren. Massenhaft versandte Erpressungs-E-Mails wurden mit Bitcoin-Zahlungsadressen verknüpft, und die resultierenden Zahlungsströme wurden analysiert. Selbst vermeintlich einfache kriminelle Kampagnen umfassten dabei eine Vielzahl von Adressen und Transaktionen, deren manuelle Analyse an praktische Grenzen stieß (vgl. Paquet-Clouston et al. 2019).

Zum Skalierungsproblem kommt ein weiteres hinzu: die isolierte Betrachtung einzelner Datenpunkte. Kryptowährungsadressen werden in der Regel individuell analysiert, ohne den umfassenden Kontext zu berücksichtigen. Verschiedene Akteurinnen und Akteure oder Plattformen können jedoch über eine gemeinsame Infrastruktur miteinander verbunden sein. Ein Mixer-Dienst wird beispielsweise von mehreren Tätergruppen genutzt; eine Kryptowährungsbörse dient als gemeinsamer Knotenpunkt für verschiedene kriminelle Netzwerke. Bei isolierter Betrachtung einzelner Adressen bleiben solche Zusammenhänge leicht verborgen.

Die Antwort liegt im Übergang von der rein manuellen, werkzeugzentrierten Analyse hin zu einem datengetriebenen, netzwerkzentrierten Ermittlungsansatz. Beim werkzeugzentrierten Ansatz bestimmt die Funktionalität des eingesetzten Werkzeugs die Grenzen der Analyse. Beim datengetriebenen Ansatz stehen hingegen die Verfügbarkeit und die Verknüpfung der relevanten Daten im Vordergrund.

Konkret bedeutet das: Blockchain-Daten stehen über die Eingabe in spezialisierte Analysewerkzeuge hinaus als Datenbasis für analytische Auswertungen mit gängigen Data-Science-Methoden zur Verfügung. Werden beispielsweise bei einer Hausdurchsuchung Tausende von Kryptowährungsadressen sichergestellt, etwa aus Wallet-Dateien, Kontoauszügen von Kryptowährungsbörsen oder Kommunikationsprotokollen, lassen sich diese mit datengetriebenen Ansätzen effizient auswerten.

Sein volles Potenzial entfaltet der Ansatz, wenn Adress- und Transaktionsdaten in Netzwerke überführt werden. Adressen oder Entitäten bilden die Knoten, Transaktionen die Verbindungen. Auf solche Netzwerkstrukturen lassen sich etablierte Methoden der Netzwerkanalyse anwenden: Zentrale Knoten weisen auf wichtige Akteurinnen und Akteure sowie auf Infrastrukturkomponenten hin. Gemeinschaftsstrukturen helfen, zusammengehörige Gruppen von Adressen zu identifizieren. Die Analyse von Zahlungsflüssen zeichnet den Weg der Gelder durch das Netzwerk nach und identifiziert auch für die Vermögensabschöpfung relevante Endpunkte, etwa Kryptowährungsbörsen, an denen eine Sicherstellungsanordnung erwirkt werden kann.

Dieser Ansatz ermöglicht zudem, die Spur des Geldes automatisiert zu verfolgen. Anstatt eine Transaktionskette manuell nachzuverfolgen, zeichnen Algorithmen den Fluss von Kryptowährungswerten über beliebig viele Zwischenschritte automatisch nach. Ermittlerinnen und Ermittler können die Ergebnisse anschließend überprüfen und für die Dokumentation aufbereiten.

Ein datengetriebener Ansatz lässt sich nur durch Zugang zu relevanten Rohdaten und entsprechenden automatisierten Analysemethoden umsetzen. Das spricht für interdisziplinäre Teams, in denen Ermittlerinnen und Ermittler mit Datenanalystinnen und Datenanalysten zusammenarbeiten. Fachkräfte mit Data-Science-Kompetenz zu gewinnen und zu halten, ist für den öffentlichen Dienst eine Herausforderung, denn die Konkurrenz mit der Privatwirtschaft um diese Qualifikationsprofile ist groß. Ebenso spricht vieles für offene Datenformate und Schnittstellen, die eine flexible Analyse

mit verschiedenen Werkzeugen ermöglichen, statt die Ermittlungsarbeit an ein einzelnes proprietäres Werkzeug zu binden.

Der netzwerkzentrische Ansatz bietet auch einen praktischen Vorteil: Er skaliert. Während die manuelle Analyse linear mit dem Datenumfang wächst, verarbeiten datengetriebene Methoden auch große Datenmengen effizient. Angesichts des fortwährend wachsenden Volumens von Kryptowährungstransaktionen wird das immer wichtiger.

Ein Beispiel aus der Praxis verdeutlicht den Nutzen: Bei der Sicherstellung einer Wallet-Datei mit mehreren Tausend Kryptowährungsadressen wäre eine manuelle Analyse jeder einzelnen Adresse kaum durchführbar. Mit einem datengetriebenen Ansatz lassen sich diese Adressen automatisiert in eine Netzwerkstruktur überführen, in der die Beziehungen zwischen den Adressen, die Transaktionsvolumina und die zeitlichen Muster unmittelbar sichtbar werden. Auffällige Muster, etwa die regelmäßige Weiterleitung von Geldern an eine bestimmte Kryptowährungsbörse oder die Nutzung eines Mixer-Dienstes, lassen sich so innerhalb kurzer Zeit erkennen. Die Ermittlerin oder der Ermittler kann sich dann gezielt auf die relevanten Transaktionsketten konzentrieren und diese im Detail dokumentieren.

## 6. ZUSAMMENFASSUNG UND AUSBLICK

Kryptowährungen haben sich als Zahlungsmittel für kriminelle Aktivitäten etabliert. Die Strafverfolgungsbehörden verfügen über erste Werkzeuge und Methoden zur Analyse von Blockchain-Transaktionen, stehen jedoch vor vier miteinander verbundenen Herausforderungen.

Das Grundproblem ist der Zugang: Solange forensische Werkzeuge teuer und hochspezialisiert bleiben, erreichen Kryptowährungshinweise die richtigen Stellen oft zu spät oder gar nicht. Einfachere, kostengünstigere Lösungen für grundlegende Ermittlungsschritte würden die Spezialistinnen und Spezialisten entlasten und zugleich die Voraussetzungen für das zweite Handlungsfeld schaffen: die frühzeitige Erkennung von Fallzusammenhängen. Denn erst wenn Kryptowährungsadressen breit erfasst und systematisch abgeglichen werden, lassen sich parallele Ermittlungen zu denselben Tätergruppen identifizieren und Verfahren zusammenführen. Die bayerische Pilotstudie belegt das Potenzial dieses Ansatzes (vgl. Haslhofer et al. 2023).

Gleichzeitig muss die Verlässlichkeit der eingesetzten Methoden kritisch bewertet werden. Verfahren wie das Adress-Clustering liefern wertvolle Ermittlungshinweise, eignen sich jedoch nicht als eigenständige Beweismittel, sondern als Indizien. Gerichtlich verwertbar werden Ergebnisse erst durch faktenbasierte Dokumentation anhand konkreter, in der Blockchain nachprüfbarer Transaktionen (vgl. Haslhofer et al. 2020). Um der Automatisierung und Vernetzung auf Täterseite zu begegnen, empfiehlt sich schließlich ein datengetriebener, netzwerkzentrierter Ermittlungsansatz, der die manuelle Verfolgung einzelner Transaktionsketten durch automatisierte Analysemethoden ergänzt (vgl. Paquet-Clouston et al. 2019).

Diese Lösungsansätze sind nicht ohne Einschränkungen möglich. Sie erfordern Investitionen in die Entwicklung geeigneter Werkzeuge, in Dateninfrastrukturen für den Abgleich von Ermittlungsdaten, in die wissenschaftliche Validierung forensischer Methoden sowie in die Weiterqualifizierung von Ermittlerinnen und Ermittlern. Data-Science-Kapazitäten im öffentlichen Dienst aufzubauen, rechtliche Grundlagen für den behördenübergreifenden Datenabgleich zu schaffen und Open-Source-Werkzeuge langfristig zu

pflegen, sind Aufgaben, die über den rein technischen Bereich hinausreichen. Die enge Zusammenarbeit zwischen Strafverfolgungsbehörden, Staatsanwaltschaften, Wissenschaft und Technologieentwicklung ist daher unerlässlich.

Die technologische Entwicklung im Bereich der Kryptowährungen wird auch in den kommenden Jahren mit hoher Geschwindigkeit voranschreiten. Neue Blockchain-Architekturen, erweiterte Anonymisierungstechnologien wie die Weiterentwicklung von Privacy Coins sowie die fortschreitende Verschmelzung von klassischem und dezentralem Finanzwesen werden die forensische Analyse vor immer neue Herausforderungen stellen. Die regulatorischen Entwicklungen auf europäischer Ebene, insbesondere die MiCA-Verordnung und die Umsetzung der Travel Rule, werden neue Ermittlungsmöglichkeiten eröffnen, auch wenn die technischen Anforderungen weiter steigen.

Internationale Zusammenarbeit ist dabei zentral. Kryptowährungskriminalität ist ihrem Wesen nach grenzüberschreitend, und forensische Standards, Datenaustauschmechanismen und Ermittlungsmethoden sollten international abgestimmt werden. Initiativen auf europäischer Ebene, etwa im Rahmen von Europol und Eurojust, bieten hierfür einen wichtigen Rahmen, der durch nationale Maßnahmen ergänzt und in die Praxis umgesetzt werden sollte.

Nur wenn die Strafverfolgung ihre Methoden und Werkzeuge stetig weiterentwickelt und auf ein solides wissenschaftliches und technisches Fundament stellt, wird sie mit diesen Entwicklungen Schritt halten und den Missbrauch von Kryptowährungen wirksam bekämpfen können.

[1] *Die Zahl von 40,9 Mrd. US-Dollar umfasst Gesamtzuflüsse an als illegal identifizierte Adressen über alle Deliktskategorien hinweg, einschließlich Ransomware, Betrug, Darknet-Handel und Sanktionsverstöße. Chainalysis (vgl. Chainalysis 2025) weist darauf hin, dass die tatsächliche Summe höher liegen dürfte, da nicht alle illegalen Adressen identifiziert wurden.*

[2] *Die Travel Rule wurde von der FATF erstmals 2019 auf virtuelle Vermögenswerte ausgeweitet (Recommendation 16) und wird in der EU durch die Transfer of Funds Regulation (TFR) umgesetzt, die Kryptowährungsdienstleister zur Übermittlung von Angaben zu Auftraggeberin, Auftraggeber und Begünstigten verpflichtet.*

[3] *Die Analogie zu DNA- oder Fingerabdruckdatenbanken ist insofern begrenzt, als biometrische Merkmale unveränderlich sind, während Kryptowährungsadressen beliebig neu erzeugt werden können. Der Abgleich von Kryptowährungsadressen ermöglicht daher nur die Erkennung von Zusammenhängen auf Basis bereits bekannter Adressen, nicht die generelle Identifizierung einer Person.*

***Quellenangaben***

*Auer, Raphael et al. (2023). The Technology of Decentralized Finance (DeFi), Digital Finance (6), 55–95, Online: https://link.springer.com/article/10.1007/s42521-023-00088-8 (09.03.2026).*

*Chainalysis (2025). The 2025 Crypto Crime Report, Online: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ (09.03.2026).*

*Europäisches Parlament/Rat der Europäischen Union (2023). Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA), Amtsblatt der Europäischen Union, L 150, 9.6.2023, Online: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng (09.03.2026).*

*Haslhofer, Bernhard et al. (2020). Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations, Forensic Science International, Digital Investigation (33), Online: https://www.sciencedirect.com/science/article/pii/S1742287619302567 (09.03.2026).*

*Haslhofer, Bernhard et al. (2023). Increasing the Efficiency of Cryptoasset Investigations by Connecting the Cases, Online: https://arxiv.org/abs/2311.08205 (09.03.2026).*

*INTERPOL (2020). Guidelines on the Darknet and Cryptocurrencies, Lyon.*

*Kappos, George et al. (2018). An Empirical Analysis of Anonymity in Zcash, Proceedings of the 27th USENIX Security Symposium, 463–477.*

*Meiklejohn, Sarah et al. (2013). A Fistful of Bitcoins. Characterizing Payments Among Men with No Names, Proceedings of the Internet Measurement Conference (IMC 2013), 127–140.*

*Möser, Malte et al. (2018). An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, 2018 (3), 143–163.*

*Nakamoto, Satoshi (2008). Bitcoin. A Peer-to-Peer Electronic Cash System, Online: https://bitcoin.org/bitcoin.pdf (09.03.2026).*

*OSCE (2022). Handbook for Dealing with Virtual Currencies in Criminal Proceedings, Skopje, Online: https://www.osce.org/mission-to-skopje/522754 (09.03.2026).*

*Paquet-Clouston et al. (2019). Spams meet Cryptocurrencies. Sextortion in the Bitcoin Ecosystem, Proceedings of the ACM Conference on Advances in Financial Technologies (AFT 2019), 76–88.*

*Ron, Dorit/Shamir, Adi (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph, Proceedings of the 17th International Conference on Financial Cryptography and Data Security (FC 2013), 6–24.*