Behördenwallets: Digitale Geldbörsen für die Verwahrung von sichergestellten Kryptowährungen

Coin-O-Mat“: ein vom C4 entwickelter Automat, der direkt mit der Blockchain kommunizieren kann

Blockchain in der Strafverfolgung

Kriminelle nutzen zunehmend Kryptowährungen zur Verschleierung ihrer Geldflüsse. Im Cybercrime-Competence-Center (C4) des Bundeskriminalamts ist der Fachbereich „Blockchain“ für die Bekämpfung von Krypto-Kriminalität zuständig.

Kryptowährungen und die dahinterliegende Blockchain-Technologie haben in den vergangenen Jahren einen festen Platz in der digitalen Welt eingenommen – mit weitreichenden Auswirkungen auf Gesellschaft, Wirtschaft und Kriminalität. 2009 wurde der erste Vertreter der Kryptowährungen – der Bitcoin – eingeführt. Mit zunehmender Verbreitung nahm das Missbrauchspotenzial zu und die Zahl der Anzeigen begann sich zu häufen. Diesem Umstand trug das Bundeskriminalamt Rechnung und richtete im September 2017 im Referat 5.3.3 (Sonderermittlungen Cybercrime) in der Abteilung 5 den Fachbereich Blockchain ein. In diesem Fachbereich sind fünf Expertinnen und Experten tätig, die mit den Kollegen des Referats 7.2.1 Lagebild Betrug und Kryptoassets zusammenarbeiten.

Die Hauptaufgabe der Mitarbeiter des Fachbereichs liegt in der zentralen Erstellung und Verwaltung von Behördenwallets des Bundesministeriums für Inneres (BMI), digitaler Geldbörsen für die Verwahrung von sichergestellten Kryptowährungen. Zudem ist der Fachbereich bundesweite Ansprechstelle für Kolleginnen und Kollegen, die bei Ermittlungen mit kryptobezogenen Fragen konfrontiert sind. Das umfasst Transaktionsanalysen (Geldflussermittlungen), Unterstützung bei Hausdurchsuchungen und die technische Auswertung von Wallets. Dabei steht nicht nur der kriminalistische Aspekt im Vordergrund, sondern auch die Wissensvermittlung: Eine Tätigkeit besteht darin, sowohl behördenintern als auch behördenübergreifende Schulungen abzuhalten und sich mit anderen Bereichen zu vernetzen und auszutauschen – national und international. Zudem stellt der Fachbereich Tools zur Verfügung, die für Ermittlungen benötigt werden.

Pionierarbeit. Anfangs standen nur wenige Informationen sowie Tools zur Verfügung und die Ermittlungen basierten auf öffentlich zugänglichen Blockchain-Explorern. Komplexe Transaktionsmuster mussten händisch aufbereitet und visualisiert werden, um Kolleginnen und Kollegen, Staatsanwältinnen und Staatsanwälten ein besseres Verständnis für diese Thematik zu ermöglichen. Die Expertise entstand durch Eigeninitiative und das Engagement einzelner Beamtinnen und Beamten, die sich aus persönlichem Interesse in die Materie eingearbeitet hatten.

Die Blockchain ist eine Kette von Datenblöcken, die miteinander so verknüpft sind, dass jeder nachträgliche Eingriff erkennbar und lokalisierbar – und unmöglich wird. Alle Transaktionen (seit Anbeginn) sind darin gespeichert, dokumentiert und im Internet abrufbar. Die Blockchain ist ein digitales Kassabuch mit beliebig vielen Kopien.

Tools. Die technische Vielfalt und Komplexität der unterschiedlichen Blockchain-Systeme macht es unmöglich, ein Werkzeug für alle Ermittlungszwecke zu nutzen. Da Blockchains in der Regel öffentlich sind und auf transparenten, mathematisch definierten Strukturen beruhen, bietet sich die Möglichkeit, spezialisierte Werkzeuge zu entwickeln, die auf bestimmte Anforderungen zugeschnitten sind. In den Anfangsjahren entwickelten Bedienstete des Fachbereichs – in Zusammenarbeit mit Bediensteten innerhalb des C4 – Analyse- und Ermittlungs-Tools. Diese Entwicklungen machten Österreich zu einem Vorreiter auf dem Gebiet der Blockchain-Ermittlungen in Europa. Das Know-how sowie die Werkzeuge stießen und stoßen bis heute auf großes Interesse – sowohl bei internationalen Partnerbehörden als auch bei Organisationen wie Europol.

Behördenwallets. Ein Meilenstein bei der Strafverfolgung im Krypto-Bereich war die Einführung der Behördenwallets 2019. Diese wurden nicht nur von Mitarbeitern des Fachbereichs entwickelt, was eine Unabhängigkeit von Drittanbietern und damit eine höhere Sicherheit garantiert, sie folgen auch dem Prinzip „Not your keys, not

FOTOS: BETTINA FRÖHLICH

Kriminelle und Terrororganisationen nutzen zunehmend Kryptowährungen zur Verschleierung ihrer Geldflüsse

FOTO: FOTOMEK - STOCK.ADOBE.COM

your coins“. Wer die „Verfügungsmacht“ über Kryptowährungen haben möchte, der muss die benötigten Schlüssel (keys) selbst verwalten und darf diese nicht in die Hand anderer geben. Deshalb gelten Kryptowährungen erst dann als sichergestellt, wenn sie auf ein Behördenwallet transferiert worden sind. Bisher wurden mehr als 1.000 Wallets erstellt und ein ähnlicher Vorrat steht nach Bedarf 24/7 zur Verfügung. Im Normalfall wird für jeden Fall sowie für jede Kryptowährung ein eigenes Behördenwallet verwendet. Dadurch kann es zu keinen Vermengungen kommen und es gibt eine klare Trennung zwischen den einzelnen Fällen.

Seit der Einführung der Behördenwallets wurden Kryptowährungen im Gesamtwert von mehreren Millionen Euro sichergestellt. Etwa eine Million Euro wurden davon in Geld umgewandelt und auf Konten der Justiz überwiesen. Ebenso viel wurde an Opfer oder ehemalige Beschuldigte rückübertragen.

Kriminelle Organisationen. Mit der zunehmenden gesellschaftlichen Akzeptanz und Nutzung von Kryptowährungen steigt ihre Relevanz für die Kriminalitätsbekämpfung. Die Möglichkeit, Vermögenswerte schnell und grenzüberschreitend zu transferieren, macht Kryptowährungen attraktiv für Kriminelle – sei es im Betrug, Drogenhandel oder Geldwäsche. Im Vergleich mit den vergangenen Jahren hat die Zahl der Ermittlungen im Zusammenhang mit Kryptowährungen zugenommen.

Einerseits sind das Wissen und die Handhabung in der Gesellschaft angekommen und andererseits ist der schnelle internationale Transfer von Vermögenswerten für kriminelle Organisation sehr verlockend. Daher werden mittlerweile Ermittlungen, die im Zusammenhang mit Kryptwährungen stehen, von mehreren Polizeidienststellen in ganz Österreich aus geführt und nicht mehr nur zentral im Bundeskriminalamt.

ICO-Exit-Scam. Zwischen Dezember 2017 und Februar 2018 gaben Betrüger vor, eine neue Kryptowährung bzw. Token zu veröffentlichen, der hohe Gewinne versprach. Es sollen zehn Millionen Token zum Verkauf angeboten worden sein, die ausschließlich durch Zahlungen über Bitcoin und Ethereum zu erwerben waren. Nachdem 8.000 Personen weltweit in diesen Token investierten, löschten die Verdächtigen ihre Webseite und sämtliche Social-Media-Kanäle und flüchteten mit den Einlagen ihrer Opfer.

Von Dezember 2022 bis März 2024 gelang es den Ermittlerinnen und Ermittlern des C4 unter der Leitung der Wirtschafts- und Korruptionsstaatsanwaltschaft den Zahlungsverlauf zu analysieren und Beweismittel sicherzustellen und auszuwerten. Dabei kam zum Vorschein, dass es sich bei den Tätern um eine vorwiegend aus Österreich agierende Gruppe handelte. Die Beweise führten durch ganz Österreich und nach Tschechien, Thailand und Zypern.

In Zusammenarbeit mit der europäischen Justizbehörde Eurojust kooperierten mehrere Staatsanwaltschaften der betroffenen Länder, um europäische Haftbefehle gegen die Tatverdächtigen zu erwirken. Im Herbst 2023 kam es schließlich zu einem „Action-Day“, bei dem in Linz, Graz, Prag und Zypern in einer koordinierten Aktion mit dem Einsatzkommando Cobra, den tschechischen und zypriotischen Be-

Causa „EXW Wallet“: Acht Personen wurden angeklagt, die mit einem „Krypto-Pyramidenspiel“ 40.000 Opfer um mehr als 14 Millionen Euro gebracht haben

hörden sowie einem IT-Fachexperten von Europol mehrere Hausdurchsuchungen, Sicherstellungen und drei Festnahmen erfolgten. In Linz und Zypern wurden ein 38-jähriger und ein 29-jähriger Österreicher und in Prag ein 34-jähriger Tscheche festgenommen. Im weiteren Verlauf der Ermittlungen wurden bis Anfang 2025 drei weitere Österreicher im Alter von 36 und 40 Jahren in Graz, Linz und Spielfeld festgenommen. Insgesamt wurden 750.000 Euro in diversen Währungen, zwei Fahrzeuge und eine Immobilie im Wert von knapp 1,4 Millionen Euro sichergestellt. Der Gesamtschaden beläuft sich auf sechs Millionen Euro.

Wissenstransfer und Vernetzung. Aufgrund des hohen Spezialisierungsgrades und der ständigen Weiterentwicklung der Blockchain-Technologie sind der Wissenstransfer und die Vernetzung zwischen Ermittlerinnen und Ermittlern wichtig. Mittlerweile stehen nationale und internationale Aus- und Weiterbildungen mit Schwerpunkt Kryptowährungen zur Verfügung, wobei das Angebot Entwicklungspotenzial aufweist.

Das persönliche Interesse und die Eigeninitiative der Bediensteten tragen dazu bei, dass sie sich auch außerhalb ihrer regulären Aufgaben kontinuierlich Wissen in diesem Fachbereich aneignen. Daher ist es umso wichtiger, dass regelmäßige Veranstaltungen stattfinden, bei denen Beamtinnen und Beamte aus den unterschiedlichsten Bereichen, die mit Ermittlungen im Krypto-Bereich betraut sind, zusammenkommen, sich vernetzen und sich über Erfahrungen und Erkenntnisse austauschen. Eines dieser Treffen ist das „Blockchain-Meeting“, zu dem der Fachbereich Blockchain regelmäßig einlädt.

BK-Token. Der Umgang mit Kryptowährungen und der dahinterliegenden Blockchain-Technologie erfordert nicht nur fundiertes Wissen, sondern vor allem praktische Erfahrung – insbesondere, wenn es darum geht, Transaktionen nachzuvollziehen und digitale Spuren auszuwerten. Da viele Polizeibedienstete bisher kaum praktische Berührungspunkte mit digitalen Vermögenswerten oder „Smart Contracts“ hatten, entwickelte das C4 ein Übungsszenario, das im Jänner 2020 präsentiert wurde. Smart Contracts sind computergestützte Programme auf der Blockchain, die automatisch bestimmte Abläufe ausführen, sobald festgelegte Bedingungen erfüllt sind.

Um diesen anspruchsvollen Bereich anschaulich und praxisnah zu vermitteln, entwickelten Expertinnen und Experten des C4 einen Token auf Basis einer Blockchain – den „BK-Token“. Dieser Token basiert auf einem Smart Contract und wurde gezielt an die Bedürfnisse polizeilicher Schulungen angepasst. In vier unterschiedlichen Schwierigkeitsstufen werden verschiedene Übungsszenarien durchlaufen, die unter anderem die Einrichtung eines Wallets, die Berechnung und Berücksichtigung von Transaktionsgebühren sowie die eigentliche Durchführung einer Transaktion beinhalten. Ziel ist es, Schritt für Schritt ein tiefgehendes Verständnis für die technischen Abläufe und Ermittlungsansätze im Zusammenhang mit Kryptowährungen zu vermitteln.

„Coin-O-Mat“. Ein besonderes Highlight des Schulungskonzepts ist der „Coin-O-Mat“ – ein Automat, der mit dem Smart Contract interagieren kann und dadurch mit der Blockchain kommuniziert. Wird eine Übung korrekt abgeschlossen, also ein Wallet eingerichtet, ein BK-Token erfolgreich übertragen und alle erforderlichen Bedingungen erfüllt, gibt der Automat zur Bestätigung eine geprägte Münze aus. Dieser Lerneffekt hilft, die abstrakte Technologie hinter Blockchain und Kryptowährungen anschaulich zu machen. Diese Erfahrung soll dazu beitragen, die digitale Kompetenz in der Polizei zu stärken und so die Effizienz bei der Aufklärung von Cybercrime-Delikten zu erhöhen.

Blockchain-Konferenz. Diese innovative Herangehensweise des Fachbereichs stieß auf internationales Interesse. Im Rahmen eines EU-geförderten Projekts organisierte der Fachbereich Blockchain 2020 eine Blockchain-Konferenz für den deutschsprachigen Raum. Über 220 Teilnehmerinnen und Teilnehmer aus Polizei, Justiz und Privatwirtschaft nahmen daran teil. Auch hier kam der Coin-O-Mat zum Einsatz und vermittelte den internationalen Gästen auf kreative und praxisnahe Weise das Funktionieren von Kryptowährungen.

Neben dieser Konferenz war der Fachbereich auch an weiteren internationalen Projekten beteiligt, etwa im Rahmen eines EU-Twinning-Projekts mit Bosnien und Herzegowina, einem Cybercrime-Workshop in Montenegro sowie einem bilateralen Aktionsplan mit Marokko. Dabei geht es nicht nur um die Vermittlung von technischem Know-how, sondern auch um den Aufbau nachhaltiger Strukturen zur grenzüberschreitenden Bekämpfung von Cybercrime.

250.000 Euro Schaden. 2023 verlor ein Geschädigter aufgrund eines Rip-Deals 250.000 Euro in Kryptowährungen. Rip-Deal-Betrüger gaukeln ihren Opfern ein Geldtauschgeschäft vor, in-

FOTO: GERT EGGENBERGER / APA / PICTUREDESK.COM

Die Blockchain ist eine Kette von Datenblöcken, die miteinander so verknüpft sind, dass jeder nachträgliche Eingriff sofort erkennbar und lokalisierbar wird

dem sie echtes Geld gegen Falschgeld tauschen. Nach der Anzeige in einer Polizeiinspektion in Wien, kontaktierte der zuständige Sachbearbeiter des Landeskriminalamts Wien Kollegen des C4 des Bundeskriminalamtes und ersuchte um Unterstützung in diesem Fall. Der Geschädigte gab an, dass ihm im Zuge eines vermeintlichen Investments rund 140 Ethereum (entsprach rund 250.000 Euro) betrügerisch herausgelockt worden waren.

Da die Anzeige zeitnah zur Tatzeit erfolgte, konnten die Ermittlungen rasch aufgenommen werden. Diese ergaben, dass die entwendeten Ethereum zu einem Krypto-Dienstleister mit Firmensitz auf den Seychellen transferiert wurden. Aufgrund der zügigen Ermittlungen konnte die Kryptowährung rechtzeitig eingefroren werden, bevor sie von den Tätern in Sicherheit gebracht werden konnte. Der Fall ist jedoch noch nicht abgeschlossen und es wird noch an der Rückgabe der Ethereum an den Geschädigten gearbeitet.

Vereitelter Auftragsmord. Unter dem Pseudonym „Sunnyboy“ veröffentlichte ein 53-jähriger IT-Experte zwischen Ende Februar und Anfang April 2023 auf einer Darknet-Plattform seine kriminellen Absichten. Sein Auftrag: Die 45-jährige Ex-Partnerin sollte von einem Auto überfahren werden und die Tat wie einen Unfall erscheinen lassen. Der Mann stellte dafür detaillierte Informationen, darunter Fotos, die Wohnadresse sowie den Tagesablauf der Frau, zur Verfügung. Mehrere potenzielle Dienstleister meldeten sich auf die Anfrage und es kam zu einer Einigung: Für 9.000 Euro bzw. rund 10.000 Dollar in Bitcoins sollte der Mordauftrag ausgeführt werden.

Die Ermittlungen in Österreich begannen nach einem Hinweis aus Manchester, der vom britischen Inlandsgeheimdienst MI5 weitergegeben worden war. Experten des C4 des Bundeskriminalamtes und des Landeskriminalamts Niederösterreich nahmen Ermittlungen auf. Es stellte sich heraus, dass der Auftraggeber eine Vielzahl an kleinen Bitcoin-Beträgen über unterschiedliche Quellen erwarb – darunter Kryptobörsen, Gutscheinkäufe sowie Bitcoin-Automaten. Dadurch wurde versucht, die Spuren zu verschleiern, jedoch ohne Erfolg.

Die Transaktionen konnten ermittelt werden und führten zu einem Treuhandkonto auf der Darknet-Plattform, über das die Bezahlung des Auftragsmordes abgewickelt werden sollte. Ein Tag vor dem geplanten Mord wurde der Mann festgenommen. Angesichts der Beweislast gestand der Verdächtige schließlich. Das Gericht verurteilte ihn wegen versuchten Mordes als Bestimmungstäter zu 15 Jahren Haft.

Rechtliche Aspekte. In den vergangenen Jahren gab es nicht nur Fortschritte in der fachlichen Expertise der Kriminalpolizei und der Verfügbarkeit technischer Werkzeuge für Ermittlungen, sondern auch auf rechtlicher Ebene wurden wichtige Entwicklungen angestoßen. So hat die MiCA-Verordnung der EU von 2024 dafür gesorgt, dass sich Exchanger (Firmen, die den Handel mit Kryptowährungen anbieten) an gewisse Regelungen, wie etwa mehr Transparenz oder die Einhaltung von Sicherheitsstandards halten müssen, um Kundinnen und Kunden sowie Anlegerinnen und Anleger zu schützen. Damit wurde erstmals EU-weit eine einheitliche Aufsicht über den Kryptomarkt etabliert.

Eine für Österreich wichtige Gesetzesänderung gab es mit 1. Jänner 2025: Mit der Änderung der Strafprozessordnung wurde Opfern die Geltendmachung privatrechtlicher Ansprüche erleichtert. Kryptowährungen fallen nun unter den Begriff der „Vermögenswerte“. Diese Änderung war von enormer Bedeutung für die polizeiliche und justizielle Praxis, da sie für Klarheit sorgte, wie mit Kryptowährungen umzugehen ist – sei es bei Sicherstellungen, der Verwertung oder der Rückgabe an Geschädigte. *Romana Tofan*

FOTO: GERD PACHAUER, STOCK.ADOBE.COM