Funktionsweise, Technologie und Ermittlung von Kryptowährungen. Ein Leitfaden für Schweizer Strafverfolgungsbehörden

Taria Bretscher

Taria Bretscher arbeitet seit August 2013 beim Bundesamt für Informatik und Telekommunikation (BIT). Seit 2016 ist sie die Compliance Managerin des Amtes und im Bereich Informatik-Sicherheit tätig. Zuvor arbeitete Sie im Bankensektor und in der Pharma-Branche. Sie hat den Bachelor in Betriebsökonomie und den Master in Economic Crime Investigation.

Kryptowährungen gewinnen immer mehr an Attraktivität und die Anzahl neuer Währungen nimmt stetig zu. Im Gegensatz zum heutigen Zahlungsverkehr wird das zentrale Geldinstitut ersetzt durch ein anonymes Netzwerk, das sogenannte Peer-to-Peer System. In einem dezentralen System gibt es keine zentrale Instanz mehr, welche das verfügbare Vermögen und die Korrektheit von Zahlungen überprüft. Um das Vertrauen in Transaktionen ohne Intermediär trotzdem sicher zu stellen, braucht es einen Mechanismus, der die Integrität der Transaktionen gewährleistet. Dieser Mechanismus wird mit der Blockchaintechnologie umgesetzt. Basierend darauf werden Transaktionen kryptografisch verschlüsselt, dezentral über das Peer-to-Peer System verifiziert und direkt zwischen Sender und Empfänger abgewickelt. Das Netzwerk prüft die Korrektheit der Transaktionen mittels einem Konsensalgorithmus und sobald eine Transaktion verifiziert wurde, wird sie in einem Block in der Blockchain abgelegt. Dort ist sie für jeden Netzwerkteilnehmer ersichtlich, nachweis- und praktisch unveränderbar.

Der Krypto-Boom, ausgelöst durch Bitcoin im Jahre 2009, motiviert weitere Unternehmungen Kryptowährungen zu schaffen, wovon sich viele durch sogenannte Initial Coin Offerings (ICO) finanzieren lassen. Neue Währungen können entweder auf neuen oder bestehenden opensource Blockchaintechnologien, wie beispielsweise Bitcoin oder Ethereum, aufgebaut und durch individuelle Änderungen am Code angepasst oder ergänzt werden. Diese unterschiedlichen Technologien je Währung entwickeln sich rasant weiter und vor allem der Privatsphäre wird vermehrt ein höherer Stellenwert gegeben. Der gewisse Grad an Anonymität wird auch für widerrechtliche Handlungen wie Geldwäscherei, Betrug, Bezahlung von illegalen Waren, etc. eingesetzt. Obwohl sämtliche Transaktionen unveränderbar und für jeden ersichtlich in der Blockchain abgelegt werden, ist es für die Strafverfolgungsbehörden eine Herausforderung, sich an die unterschiedlichen Funktionsweisen anzupassen oder die Verbindung zwischen der digitalen Welt und realen Personen herzustellen.

Ziel der Masterarbeit war es deshalb, einen Leitfaden für Ermittler der Schweizer Strafverfolgungsbehörden zu erstellen. Um in einem ersten Schritt die Bedürfnisse und den aktuellen Wissensstand der Schweizer Strafverfolgungsbehörden festzustellen, wurde eine Umfrage bei den Schweizer Polizeikorps, der Bundesanwaltschaft (BA) und dem Bundesamt für Polizei (fedpol) durchgeführt. Basierend darauf und auf Gesprächen mit Staatsanwälten und Polizeiangehörigen wurden in Form eines Leitfaden Lösungsansätze und Handlungsempfehlungen für die erfolgreiche Ermittlung und Sicherstellung von Kryptowährungen erarbeitet. Weiter wurden die verschiedenen Technologien, Funktionsweisen und Anwendungsgebiete (zB. im Darknet) von unterschiedlichen Kryptowährungen analysiert und mittels einer Übersicht für Schulungszwecke aufbereitet. Als weiterer wichtiger Aspekt wurden die rechtlichen Rahmenbedingungen, also die gesetzlichen Grundlagen, welche in der Schweiz vorhanden sind, auf deren Anwendbarkeit in Bezug auf Krypto-Assets untersucht.

Die Erfahrungswerte in der Ermittlung und Sicherstellung von Kryptowährungen sind bei den Schweizer Strafverfolgungsbehörden noch gering. Es bestehen keine standardisierten Prozesse und die rechtlichen Rahmenbedingungen im Umgang mit Kryptowährungen sind ungenügend respektive unklar. Obwohl Kryptowährungen in der Schweiz als Zahlungsmittel akzeptiert und vom Bundesrat als Vermögenswert definiert sind, handelt es sich bei Krypto-Assets nicht um staatliche Währungen. Dies führt dazu, dass in der Schweiz kein besonderer rechtlicher Schutz für virtuelle Währungen vorhanden ist. Betrachtet man jedoch die bestehende Gesetzgebung im Bereich des Strafrechts genauer, greift diese weitegehend bei Tatbeständen, welche das Vermögen schützen (Art. 137 ff. StGB). Straftatbestände wie Datendelikte der unbefugten Datenbeschaffung (Art. 143 StGB), der Datenbeschädigung (Art. 144bis StGB) oder der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) bieten sich zum Schutz an, da es sich bei Kryptowährungen um geldwerte Daten mit kryptografischer Verschlüsselung handelt. Hinzu kommt die

hohe Volatilität von Kryptowährungen, was vor allem bei beschlagnahmten Vermögenswerten innert kurzer Zeit zu einer starken Wertverminderung oder -steigerung führen kann. Handlungsbedarf besteht demnach auch in der Anwendung der Schweizerischen Strafprozessordnung. Denn, wenn es um die Sicherstellung, Aufbewahrung und Verwertung von den sehr volatilen Coins geht, erscheint die Gesetzgebung noch sehr ungenau und die Handhabung in der Praxis je Fall und Behörde individuell gestaltet. Eine schweizweite Vorgabe, wie Krypto-Assets verwertet werden sollen, gibt es nicht. Auch ist nicht klar geregelt, wer die Verantwortung für allfällige Wertveränderungen tragen muss. Es liegt jedoch nahe, dass ein sofortiger Wechsel in CHF oder in eine andere Fiat-Währung die sinnvollste Variante darstellt und die Verwertung resp. Aufbewahrung der Staatsanwaltschaft obliegen soll. Der Wunsch nach einer strukturierten Vorgehensweise ist flächendeckend bei allen befragten Schweizer Behörden vorhanden. Um dies zu erreichen, bilden die Sensibilisierung aller Mitarbeitenden im Bereich Kryptowährungen, klare Abläufe sowie Verantwortlichkeiten zwischen den Polizeikorps und den jeweiligen Staatsanwaltschaften die Basis. Die im Leitfaden beschriebenen Anwendungsmöglichkeiten unterstützen die Strafverfolgungsbehörden deshalb, Vorgehensweisen standardisieren und Verantwortlichkeiten festlegen zu können.

Die Fähigkeit Adressen, Schlüssel und Walletsoftware erkennen und öffnen zu können, ist für die erfolgreiche Ermittlung von Krypto-Assets eine der wichtigsten Grundvoraussetzungen. Bereits die Identifikation von unterschiedlichen alphanummerischen Adressen oder Passphrases als mögliche Krypto-Adressen stellt bei den Schweizer Strafverfolgungsbehörden eine grosse Schwierigkeit dar oder löst Unsicherheiten aus. Trotzdem werden Schulungen noch sehr zurückhaltend angeboten oder sind spezifisch auf Bitcoin beschränkt. Ohne Sensibilisierung und regelmässiger Schulung der Mitarbeitenden ist die rechtzeitige Sicherstellung von Kryptowährungen gefährdet. Ausserdem können Vermögenswerte durch Drittpersonen innert Minuten an unbekannte Adressen wegtransferiert werden und sind somit für die Ermittler, zumindest vorübergehend, verloren. Die im Leitfaden ausgewiesene Übersicht unterstützt die Front, in Form von Beispielen, unterschiedliche Wallet-Arten und Adresskombinationen sowie deren Erkennungsmerkmale identifizieren zu können. Zudem werden die verschiedenen technischen Besonderheiten einzelner Kryptowährungen beleuchtet. Die erarbeitete Anleitung hilft weiter, dass Coins bereits von Live-Systemen vor Ort auf ein sicheres Wallet transferiert werden können und nicht erst im Labor. Auch das Wiederherstellen von Schlüsseln oder wie Hardwallets neu aufgesetzt werden können, wird thematisiert. Dies ist für Ermittler vor allem relevant, um an inkriminierte Vermögenswerte zu gelangen. Der Fokus liegt dabei auf den Währungen Bitcoin und Ethereum, wobei zum heutigen Zeitpunkt die meisten im Leitfaden beschriebenen Vorgehensweisen für einen Grossteil der im Markt angebotenen Kryptowährungen angewendet werden können.

Was die Zukunft im Bereich Blockchain und Kryptowährungen bringt, wird sich erst noch zeigen. Jedoch werden Kryptowährungen kaum vom Markt verschwinden. Viel mehr wird sich die zugrundeliegende Technik rasant weiterentwickeln, dem Nutzer neue Möglichkeiten bieten, dem Kriminellen neues Verschleierungspotential geben und Ermittler vor neue Herausforderungen stellen. Umso wichtiger ist es, dass die Strafverfolgungsbehörden ihr Knowhow stetig weiterentwickeln und mit der Technik und deren Möglichkeiten vertraut sind. Die Sensibilisierung ist von grösster Wichtigkeit, damit Kryptowährungen in Zukunft eine Selbstverständlichkeit darstellen und frühzeitig erkannt werden können.

Hochschule Luzern - Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Grafenauweg 10
Postfach 7344
CH-6302 Zug
+41 41 757 67 67
ifz@hslu.ch