Post-Bitcoin Kryptowährungen: Zwischen Vertraulichkeit privater Finanzdaten und Bekämpfung globaler Cyber-Kriminalität

Das AIT Austrian Institute of Technology und die Universität Innsbruck hatten am 19. Oktober 2018, namhafte internationale WissenschaftlerInnen aus Deutschland, Österreich, Großbritannien und auch aus den USA zum „Symposium on Post-Bitcoin Cryptocurrencies“ (https://www.ait.ac.at/postbitcoin-symposium/) in die Arena 21 des Wiener Museumsquartiers geladen, um ausgehend von jüngsten technologischen Entwicklungen bei Kryptowährungen in Ergänzung und funktionaler Erweiterung zu Bitcoin die anstehenden Herausforderungen in den Bereichen Rechtssicherheit, Datenschutz, Regulierung und auch Strafverfolgung zu diskutieren.

Wien, 26. November 2018: In den 10 Jahren seit der Geburtsstunde der Kryptowährung Bitcoin, welche die als Blockchain bekannte Distributed Ledger-Technologie benutzt, ist viel passiert: steigende Transaktionsvolumina, eine zunehmende Verbreitung von Bitcoin-Bankomaten, neue Finanzierungsformen wie DAOs (Decentralized Autonomous Organizations) und ICOs (Initial Coin Offerings) als Mischform aus IPO und Crowdfunding. Außerdem entstanden neue Kryptowährungen wie Ether, Zcash oder Monero, welche die Funktionalität von Bitcoin in Richtungen wie erhöhter Schutz der Privatsphäre und dezentralisierte Computing-Plattformen erweiterten.

„Die Post Bitcoin-Kryptowährungen verdanken sich dem Umstand, dass viele der Anfangsversprechen der virtuellen Urwährung Bitcoin, wie zum Beispiel Dezentralisierung oder Anonymität nach nur einem Jahrzehnt ernüchternden Realitäten gewichen sind. Heute ist es möglich, Zahlungsströme zu verfolgen (Tracking) und es zeigen sich deutliche Zentralisierungstendenzen sowohl bei Mining-Diensten also bei virtuellen Krypto-Wechselstuben, den sogenannten Exchanges“, erklärte Dr. Bernhard Haslhofer vom AIT, das Co-Veranstalter des international ausgerichteten Symposiums war.

Die spektakulären Hacks von Mount Gox bis DAOs, diverse Ransomware-Angriffe, das Aufkommen von Schneeballsystemen (z. B. Optioment) mit betrügerischen Absichten und zuletzt auch ICO-Betrug im großen Stil haben nicht nur das Image der Kryptowährungen beschädigt und damit ihre schnellere Verbreitung für „bona-fide“-Transaktionen verhindert, sondern auch den Bedarf an gezielter Regulierung im Spannungsfeld von Datenschutz und Risikominimierung gegenüber illegalen Aktivitäten ins öffentliche Bewusstsein gerückt.

Für Prof. Dr. Rainer Böhme, vom Institut für Informatik der Universität Innsbruck, ebenfalls Co-Veranstalter des Symposiums, ist dieser Spagat nur möglich, wenn Gesetzgeber und Regulierungsbehörden der Geschwindigkeit und Komplexität der jüngsten Technologieentwicklungen Rechnung tragen. „Ein Defizit aus Rechtssicherheit gepaart mit

viel Euphorie – teils befeuert durch medienwirksame Experimente von namhaften Institutionen – hat viele ahnungslose Nutzer in unseriöse Geschäftspraktiken verwickelt. Diese Fehlentwicklungen muss der Gesetzgeber schnell beenden.“, so Prof. Böhme.

Anonymität, Schutz persönlicher Daten und Zahlungsverfolgung am Prüfstand von Zcash, Monero und Etherum

Prof. Sarah Meiklejohn PhD vom University College London ist seit vielen Jahren eine anerkannte Expertin für Blockchain-Forensik. Durch algorithmisches Zusammenführen von Adressen und dem manuellen Sammeln von „Ground Truth“-Daten durch Teilnahme an Transaktionen, ist es gelungen, die Silk Road und Mt. Gox-Vorkommnisse zu enthüllen.

In ihrer Präsentation in Wien zeigte sie, wie bei Zcash Transaktionen innerhalb eines geschützten Bereichs kryptografisch maskiert werden, bei Ein- und Auszahlungen sowie außerhalb dieses Bereichs aber sichtbar bleiben und somit deanonymisiert werden können. Da nur sehr wenige Zahlungsflüsse durch den geschützten Bereich laufen, bleibt zu bezweifeln, ob Zcash in der Praxis eine Verbesserung der Anonymität bringt.

Bei der Kryptowährung Monero gibt es grundsätzlich drei Verbesserungen gegenüber Bitcoin wie Malte Möser, derzeit Doktorand an der Princeton University in den USA ausführte. Erstens generiert Monero für jede Transaktion automatisch neue Adressen (ähnlich Kontonummern), zweitens werden die Transaktionsbeträge verdeckt und drittens kann der Ursprung einer Transaktion nicht eindeutig rückverfolgt werden. Die Wirksamkeit des gesamten Monero-Systems setzt jedoch eine entsprechende Sorgfalt bei der Ausführung von Transaktionen voraus. Seine Forschungsarbeiten zeigten, dass Anfang 2017 immerhin noch 80 % aller Transaktionen nachzuvollziehen waren – ein Problem, das in neueren Versionen von Monero mittlerweile gelöst zu sein scheint.

Zwischen und Bitcoin und Ether, der Währung der „Ethereum“-Plattform, existieren zentrale Unterschiede betreffend der Nachverfolgung von Zahlungsflüssen. Während bei Bitcoin der „Transaktionsgraph“ der Schlüssel zum Tracking ist, ist es bei Ether in viel höherem Maße der „Adressgraph“. Grund dafür ist, dass Ethereum in der Funktionsweise Bankkonten ähnlicher ist als digitale Münzen. Eine Besonderheit ist, dass diese Konten durch Computerprogramme automatisch verwaltet werden können. Damit lassen sich Unter-Kryptowährungen (sog. Token-Systeme) realisieren, von denen derzeit über 200.000 auf der Ethereum-Blockchain gespeichert sind. Die 600 am meisten genutzten sind mit 28 Milliarden Euro höher bewertet als die ihnen zugrundeliegende Plattform. Die Schwierigkeit der Verfolgung von Zahlungsflüssen in Ethereum liegt darin, dass die Ether-Flüsse bei isolierter Betrachtung nur ein unvollständiges Bild ergeben und daher alle Token-Systeme (Transaktionen, Adressen und Einheiten) untersucht werden müssten. Die automatische Erkennung des Token-Zwecks ist dabei eine offene Forschungsfrage, die mit ähnlichen Methoden wie die Klassifizierung von Schadsoftware gelöst werden könnte. Michael Fröwis,

Doktorand an der Universität Innsbruck in conclusio: „Ether-Zahlungsströme sind einfach zu verfolgen, aber die Token-Systeme, die darauf aufbauen, sind technisch anders konzipiert." Derzeit fehlen Werkzeuge für eine Analyse. Nur wenn Token-Entwickler den ERC20-Standard korrekt umsetzen, können Wertbewegungen in Handarbeit nachverfolgt werden.

Terrorismusbekämpfung, rechtliche Transparenz und Ökoystem-Regulierung
Drei weitere hochkarätige Vortragende beleuchteten das Metathema des Symposiums aus Sicht möglicher kooperativer Lösungen bei der Bekämpfung des internationalen Terrorismus, aus Perspektive der Chancen-Risiken-Abwägung bei der rechtlichen Umsetzung von Transparenz für Kryptowährungen und der Regulierung des Ökosystems für Kryptowährungen.

Daniel G. Arce, Professor of Economics an der University of Texas in Dallas, befasste sich in seinem Vortrag mit der Frage, wie Erfolge in der koordinierten Terrorismusbekämpfung auch dafür adaptiert werden können, den Einsatz von Kryptowährungen für Geldwäsche und Terrorismusfinanzierung mit Mitteln der Strafverfolgung zu adressieren.

Da es sich sowohl bei Terrorismus als auch bei Kryptowährungen um grenzenlose Phänomene handelt und gerade Terroristen oft mit gefälschten Identitätspapieren in ihre Operationsgebiete einreisen, bildet die Interpol-Datenbank „Stolen and Lost Travel Documents" (SLTDs), bekannt als MIND/FIND, in die jedes teilnehmende Land ihre Daten einspeist und auch entscheidet, welches Land die Daten einsehen darf, einen guten Ausgangspunkt für verbesserte Terrorabwehr. Obwohl diese Datenbank nicht spezifisch für Terrorbekämpfung konzipiert wurde, liegt der Nutzen ihrer Verwendung klar auf der Hand. In den USA würde bereits eine Trefferquote von 0,29 % für terroristische Straftaten das gesamte MIND/FIND-Budget rechtfertigen. In allen teilnehmenden Ländern zusammen führte der Einsatz der Datenbank zu einem Rückgang des internationalen Terrors um 30 %.

Der zweite wichtige Kernpunkt ist die verstärkte Berücksichtigung der Empfehlungen der FATF (Financial Activities Task Force), eines internationalen Netzwerkes für die Peer-Review von Compliance-Anforderungen, für die Erkennung von Terrorismusfinanzierung und Geldwäsche-Aktivitäten, insbesondere aber die prompte Meldepflicht von Finanzorganisationen über verdächtige Transaktionen und die Bereitstellung von akkuraten Informationen über den Ausgangspunkt von Finanzflüssen und Meldungen zur Identifizierung von Zahlern.

„Die Transparenz von Kryptowährungen hat Implikationen für den Datenschutz, für kriminalpolizeiliche Untersuchungen und nicht zuletzt für die Regulierung", so die Schlussfolgerung von Dr. Paulina Jo Pesch vom KIT (Karlsruher Institut für Technologie). Dabei geht es in Summe um die zentrale „Abwägung zwischen der Privatsphäre der Nutzer und den Möglichkeiten für Ermittler und Aufsichtsbehörden.

In ihrem Diskussionsbeitrag nahm sie die grundlegenden Charakteristika von Kryptowährungen wie die dezentrale Abwicklung von Online-Transaktionen in einem Peer-to-peer Netzwerk, die Möglichkeit, jederzeit Adressen (Accounts) im System zu kreieren, die Verifizierung von Transaktionen durch die Systemteilnehmer selbst und die Einspeisung von Transaktionen in ein verteiltes, öffentliches und größtenteils unveränderbares Register, in dem die gesamte Transaktionsgeschichte abgespeichert ist, zum Ausgangspunkt für die Frage, was in der Blockchain sichtbar und was unsichtbar bleibt: Adressen und transferierte Beträge, die Summe der Transaktionen aller Adressen und durch Adressen-Clustering die eventuelle Zuordnung von Zahlungsflüssen an eine Systemeinheit können ausgelesen werden, nicht aber die Identitäten der Adressinhaber.

Da öffentliche Blockchain-Daten jedenfalls teilweise personenbezogen sind, da die Adressen als Pseudonyme ihren Inhabern häufig mit Zusatzinformationen zugeordnet werden können, fielen diese Daten vielfach unter den rechtlichen Geltungsbereich der seit diesem Jahr in Europa anzuwendenden DSGVO (Datenschutzgrundverordnung). Konfliktpotenzial gibt es in vielfacher Hinsicht: die Daten in der Blockchain sind transparent, die Datenverarbeitung durch die für die Einhaltung der DSGVO verantwortlichen Netzwerkteilnehmer ist es nicht. Weil diese weitgehend unbekannt sind und Einzelne geringen Einfluss auf die Datenverarbeitung haben, können Betroffenenrechte nach der DSGVO nicht ausgeübt werden. Die Löschung oder Berichtigung einzelner Einträge in der Blockchain ist wegen deren Unveränderbarkeit ohnehin unmöglich; vorgeschlagene Lösungsansätze sind bislang unzureichend erforscht. Die für die Überprüfung neuer Einträge durch die Netzwerkteilnehmer nötige Transparenz der Daten in der Blockchain steht im Spannungsverhältnis zum Prinzip der Datensparsamkeit. Es ergibt sich der Befund, dass öffentliche Blockchains mit erheblichen Risiken für den Datenschutz verbunden sind, die DSGVO die Datenverarbeitung in dezentralen Blockchains aber unzureichend abdeckt.

Rechtsunsicherheit besteht bei der kriminaltechnischen Untersuchung von Blockchaindaten z. B. im Zusammenhang mit Online-Drogenhandel oder Erpressungen mit Ransomware. Allgemeine Rechtsgrundlagen erlauben den Strafverfolgungsbehörden das Tracking von Transaktionsflüssen, die Identifikation von Adressinhabern oder das Clustering von Adressen, die wahrscheinlich demselben Inhaber zuzuordnen sind, nur in gewissem Umfang. Ermittlungen, mit denen intensive Eingriffe in Grundrechte Betroffener einhergehen, bedürfen spezieller Rechtsgrundlagen, an denen es bislang fehlt. Im Einzelnen ungeklärt ist bislang, was sich auf die bestehenden Rechtsgrundlagen stützen lässt. Offen ist, inwieweit die Schaffung neuer Rechtsgrundlagen notwendig und rechtspolitisch wünschenswert ist.

In Bezug auf die Regulierung stellte Dr. Paulina Jo Posch schließlich fest, dass die Anti-Geldwäsche-Richtlinie (EU) 2018/843 mit ihren inzwischen auch für Exchanges und Wallet-Provider geltenden Identifikations- (KYC), Überwachungs- und Meldepflichten viele Schwächen aufweist. Insbesondere im Bereich von Kryptowährungen sind die Pflichten leicht zu umgehen und gefährden den Datenschutz. Effektiver lassen sich Kryptowährungen mit

Transaktions-Sperrlisten regulieren, die Intermediären die Annahme von Cryptocoins aus gelisteten Transaktionen verbietet. Durch die Nachverfolgbarkeit von Transaktionen in der Blockchain lässt sich die Regulierung nicht durch Nachfolgetransaktionen umgehen. Der Ansatz ist geeignet, Kriminalität mit Kryptowährungen zu verhindern, wenn durch Straftaten erlangte Cryptocoins nicht mehr oder nur noch zu einem geringeren Preis eingetauscht werden können. Dies funktioniert aber nur bei einer internationalen Umsetzung.

Angesichts der genannten Risiken und Chancen transparenter Blockchains stellt sich die Frage, so Dr. Paulina Jo Pesch, inwieweit anonymere Kryptowährungen möglich und wünschenswert sind. Intransparentere Systeme machen es zwar Strafverfolgern und Regulierern schwerer, schützen personenbezogene Daten der Nutzer aber auch vor anderen Akteuren.

Den Abschluss des dichten Vortragsprogramms beim eintägigen Symposium bildete der Auftritt von Prof. Ross Anderson, Fellow of the Royal Society und Fellow of the Royal Academy of Engineering, von der Cambridge University zum Thema „Regulating the Real Cryptocurrency Ecosystem“.

Zu Beginn seines Vortrages erläuterte Prof. Anderson die aktuelle Regulierungssituation, wie die seit 2013 geltenden FinCEN (Financial Crimes Enforcement Network) Bestimmungen mit der Registrierungspflicht für Exchanges als „money service businesses“ oder die EU Directive PE CONS, die seit heuer versucht, Wallet Hosting Service Provider ebenfalls zu regulieren.

Danach berichtete er über Ergebnisse seiner Bitcoin-Untersuchung von den Anfängen bis heute auf Basis von 56 Diebstahls-Berichten, aus deren Analyse er den Schluss zog, dass die FIFO (First in-First out)-Methodik für das Tracking von UTXOs (Unspent transaction Output), also von Transaktionen, die als Input für neue Transaktionen verwendet werden sowie für die Analyse von Bitcoin Mixes oder Bintcoin Laundries (Geldwäsche) der „haircut tainting“-Methode überlegen ist. Das Forscherteam hat den FIFO-Ansatz im März dieses Jahres veröffentlicht und taintchain.org als öffentlichen Dienst etabliert.

Danach kam er auf sein eigentliches Kernthema der heutigen echten Beschaffenheit des Bitcoin-Ökosystems zu sprechen. Für Prof. Anderson markieren die Bitcoin Exchanges ein Schatten-Banksystem, dass vortäuscht, ein Goldhändler-System zu sein. Vor dem Hintergrund steigender Raten für schnelle und billige „off-chain“-Transaktionen während der letzten beiden Jahre (Coinbase in den USA und im UK, Binance in China) agieren die Bitcoin-Exchanges als e-money-Provider ohne die nach EU-Gesetzgebung erforderlichen Lizenzen, d.h. als unregulierte Bezahldienste.

Als am dringendsten erforderlich hält er, dass die EU-Regierungen Exchanges, die off-chain payments anbieten, nach der E-Money Directive regulieren, inklusive der Tokens. Und

zweitens müssten die Beziehungen zwischen Exchanges und ihren Kunden nach der „2nd Payment Directive“ (PSD2) reguliert werden. Im Grunde heißt dies nichts anderes, als einfach schon bestehendes Recht zur Anwendung zu bringen. Es gibt aber auch Lichtblicke. Wenn künftig Smart Contracts auf Rechnungen für den Währungstausch (FIAT gegen Bitcoin) Anwendung finden mit einer zentralen Bank als Absicherung, dann könnte das Ökoystem seinen Weg in die richtige Richtung nehmen.

Die Kontrolle von Verschlüsselung wäre hingegen der falsche Regulierungsansatz für das Ökosystem der Kryptowährungen, weil Encryption die sichere Abwicklung von Peer-to-peer-Zahlungen technologisch hervorragend unterstützen kann. Es geht nur darum, durch Anwendung und Adaptierung bestehender gesetzlicher Grundlagen für den Zahlungsverkehr im Netz Aktivitäten betrügerischer, weil vorgetäuschter Banksysteme auszuhebeln und zu unterbinden.

Mit einem Umweltschutzgedanken entließ Prof. Anderson die Delegierten: Da das Mining von Kryptowährungen heute einen Energieaufwand von rund 7GW, das entspricht in etwa dem Energiebedarf von Israel, erfordert, sollten die europäischen Regierungen zumindest eine Carbon-Steuer in Höhe von 33,- € per Tonne CO^2 zur Anwendung bringen wie sie im EU-Schema für den Emissionshandel verankert ist.

Symposium großer Erfolg – Appell zu politischem Gestaltungswillen

Dr. Bernhard Haslhofer vom AIT gab sich in seinen Schlussworten überzeugt, dass diese intensive öffentliche Diskussion über Kryptowährungen jetzt zum richtigen Zeitpunkt geführt wird. Die internationale Exzellenz der SprecherInnen hat dafür gesorgt, dass WissenschaftlerInnen, Regulierungsverantwortliche und Brancheninsider zahlreich den Weg nach Wien gefunden haben. Mit rund 130 TeilnehmerInnen war die Location „Arena 21“ sehr dicht besetzt.

Die Planung einer Tagungs-Agenda mit den Schwerpunkten „Kryptowährungen nach Bitcoin“ war möglich, weil sowohl AIT als auch die Universität Innsbruck sich seit mehreren Jahren wissenschaftlich intensiv mit dem Thema Kryptowährungen und Blockchain auseinandersetzen und mittlerweile auch auf europäischer Ebene, z.B.: im EU-Projekt TITANIUM, die Themenführerschaft übernehmen konnten.

Die wissenschaftlich fundierten Erkenntnisse des Symposiums können für die zukünftigen Gestaltungs- und Regulierungsbestrebungen genutzt werden und zeigen, dass intensive, erfolgreiche und international gut vernetzte Forschung auch globale Akzente setzen kann.

Rückfragehinweis:

Mag. (FH) Michael Mürling
Marketing and Communications
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43 (0)50550-4126 | M +43 (0)664 2351747
michael.muerling@ait.ac.at | www.ait.ac.at

Follow us on:
Facebook | LinkedIn | Twitter