Thesenpapier

Blockchain in der Öffentlichen Sicherheit

16. Oktober 2019

Zum Hintergrund des Thesenpapiers

Am 16.10.2019 haben die Bitkom Arbeitskreise Blockchain und Öffentliche Sicherheit im Rahmen der Sicherheitskooperation Cybercrime einen ersten „Public Security Blockchain Day“ veranstaltet. In diesem Workshop mit Vertretern der Sicherheitsbehörden und Digitalwirtschaft diskutierten die Teilnehmer Chancen und Risiken sowie mögliche Anwendungsfälle der Blockchain für Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Die Ergebnisse dieser Tagung bilden die Grundlage für das vorliegende Thesenpapier, das Anregungen für den Einsatz der Blockchain im Bereich der Öffentlichen Sicherheit liefern soll. In einem ersten Schritt werden Vorteile der Blockchain im Bereich des Crypto-Tracing diskutiert, also der Analyse von Blockchain-basierten Transaktionsdaten in der Finanzkriminalität. Daraufhin werden mögliche Blockchain Use Cases für Behörden der öffentlichen Sicherheit aufgezeigt.

1. Crypto-Tracing

Insbesondere im Bereich der Finanzkriminalität mit Kryptowährungen können sich Behörden der Öffentlichen Sicherheit einige Kerneigenschaften der Blockchain wie die Transparenz oder die Unveränderbarkeit zu Nutze machen. Über die Transparenz der Transaktionshistorie z.B. bei Bitcoin können Geldströme bestens nachvollzogen werden und dadurch Täter, Teilnehmer und Opfer häufig de-anonymisiert/de-pseudonymisiert und identifiziert werden. Dies ist für Ermittlungen krimineller Delikte wie Geldwäsche, Terrorismusfinanzierung, Erpressung, Drogen- oder Waffenhandel ein wertvoller Vorteil. Das Bundesfinanzministerium bewertet in der am 21. Oktober 2019 veröffentlichten ersten Nationalen Risikoanalyse die Geldwäschebedrohung von Kryptowerten mit mittel-niedrig. Zudem lägen keine Erkenntnisse vor, dass Kryptowerte in größerem Umfang für Terrorismusfinanzierung genutzt würden.[1]

Der mit Abstand größte Teil der kriminellen Handlungen mit Kryptowährungen findet nach wie vor in Bitcoin statt. Einfache Transaktionen zu bekannten Bitcoindienstleistern ermöglichen die Identifikation eines Täters. Anonymisierende Systeme und Privacy Coins wie Monero werden unter fortgeschrittenen Kriminellen beliebter und stellen Ermittler vor neue Herausforderungen.

[1] Vgl. Nationale Risikoanalyse des BMF: https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.pdf?__blob=publicationFile&v=7.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Patrick Hansen
Bereichsleiter Blockchain
T +49 30 27576-410
p.hansen@bitkom.org

Dr. Christian Weber
Referent Öffentliche Sicherheit & Verteidigung
T +49 30 27576-136
c.weber@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Auch mit Unterstützung von Machine Learning/AI können die zugrundeliegenden Datenmodelle für die Nachverfolgung von Geldströmen weiter verbessert werden. Die ständige Weiterentwicklung und Analyse neuer Zahlungsmethoden mit virtuellen Währungen ist notwendig, um das übliche Katz- und Mausspiel zugunsten des Ermittlers zu entscheiden. Eine wesentliche Voraussetzung um die Potenziale des „Crypto Tracing" durch Angehörige der BOS voll auszuschöpfen, ist das entsprechende Fachwissen, sowie der Zugang zu den relevanten Blockchain- und Identifikationsdaten. Hier braucht es eine umfassende Qualifizierung und Schulung der Mitarbeiter in den Sicherheitsbehörden sowie einen Ausbau der personellen und finanziellen Kapazitäten im Krypto-Bereich.

Die Unveränderbarkeit der Transaktionshistorie macht Blockchain-basierte Daten außerdem für die Indizien-, Beweis und Nachweisführung nutzbar. Die Bundesregierung kündigte in ihrer Blockchain Strategie aus dem September 2019 an, den Einsatz von Blockchain Technologien im Rahmen der Beweisführung zu prüfen. Dabei geht es insbesondere darum, wie die Blockchain-Daten zur Nachweisführung an Gerichte oder Prüfinstanzen übermittelt werden können und somit die rechtlich notwendige Verkehrstätigkeit gewährleistet bleibt. Zudem muss die Langzeitsicherheit der Daten und der kryptographischen Algorithmen gewährleistet sein. Der Bereich der Beweisführung bietet folglich großes Potenzial für Blockchain-Anwendungen.

2. Blockchain Use Cases für Behörden der öffentlichen Sicherheit

Der deutsche föderale Flickenteppich im Sicherheitsbereich mit zahlreichen Behörden auf unterschiedlichen Ebenen, gepaart mit den hohen Anforderungen an Datenaustausch und –integrität, scheint für Anwendungen der Blockchain Technologie für eine bessere behördenübergreifende Kooperation und Koordination wie gemacht. Der Blockchain Use Case im BAMF zur Verbesserung der Zusammenarbeit im Asylprozess könnte dafür als Vorbild dienen.[2]

Dabei sollte auf die Sicherheit von IT-Systemen weiterhin großer Wert gelegt werden, denn die Zusammenarbeit zwischen verschiedenen Einrichtungen erhöht die Komplexität und damit das Risiko für Sicherheitsvorfälle kontinuierlich. Die Blockchain Technologie kann hier einen Beitrag leisten, indem sie bspw. das manipulationssichere Logging von Zugriffen auf IT-Systeme (wer hat wann worauf zugegriffen) gewährleistet. Bei solchen Systemen, die heute auf zentralen Log-Servern betrieben werden und in nahezu jedem Unternehmen und jeder öffentlichen Einrichtung zu finden sind, lässt sich die Sicherheit durch blockchainbasiertes, manipulationssicheres Logging im Vergleich zu heutigen Systemen deutlich erhöhen.

[2] Vgl. http://www.bamf.de/DE/DasBAMF/BAMFdigital/Blockchain/blockchain.html.

Die Abbildung der Prozesse bei Straf- und Verfolgungsverfahren über eine Blockchain, wie z.B. Aktenführung, Asservatenführung, Sicherheitsüberprüfungen sowie jegliche Art von Registern, kann den Austausch und den Zugriff auf bestimmte Dokumente und Daten sowie auf Statusauskünfte seitens zahlreicher Behörden deutlich vereinfachen. Dies gilt natürlich auch und insbesondere auf europäischer Ebene, wo Abstimmung und Abläufe bei grenzüberschreitender Kriminalität noch großes Verbesserungspotenzial aufweisen. Für die European Blockchain Services Infrastructure, die im Frühjahr 2020 erste Use Cases wie Hochschulzertifikate auf einer öffentlichen europäischen Blockchain Infrastruktur testen möchte, wäre dies ein weiterer sinnvoller Anwendungsfall.

Nicht zuletzt sind für die Öffentliche Sicherheit auch die Potenziale der Blockchain Technologie in der Logistik bzw. Lieferkette ein denkbares nützliches Anwendungsfeld. Naheliegend erscheint das für sicherheitsrelevante Güter, zum Beispiel aus dem Bereich der Rüstung oder Chemie, deren Herstellung, Einsatz, und Verfügbarkeit dadurch transparent abgebildet werden könnte. Ggf. kann dies mit der Möglichkeit, diese Daten für das „Predictive Maintenance“ nutzbar zu machen, verbunden werden. Aber auch die eindeutige Zuordenbarkeit digitaler Fahraufträge bei der Bundeswehr, oder der Herkunftsnachweis bei Firmware in Behörden öffentlicher Sicherheit, wären mögliche Ansatzpunkte für einen sinnvollen Einsatz der Blockchain. Bei größeren, koordinierten Einsätzen von Sicherheitsbehörden oder Militär im internationalen Rahmen wäre die Technologie zudem zur Steuerung der Personal- und Einsatzkontingente denkbar.

Zusammenfassung und Ausblick

Dass Kriminelle heutzutage Blockchain-basierte Kryptowährungen nutzen, um sich illegale Waren zu kaufen, Geld zu waschen, oder Lösegeld zu fordern, ist hinlänglich bekannt. Unterschätzt wird bisher das Crypto-Tracing, also die Möglichkeiten für Sicherheitsbehörden, Blockchain-basierte Daten wie beispielsweise Bitcoin-Transaktionen auszuwerten und dadurch kriminelle Taten aufzudecken. Darüber hinaus kann die Blockchain- Technologie auch für eine ganze Reihe von Use Cases zur besseren behördenübergreifenden Kooperation oder im Bereich Logistik/Lieferkette für den Sicherheitsbereich interessant sein. Dazu finden sich in diesem Thesenpapier erste Ideen für exemplarische Anwendungsfelder der Blockchain Technologie, die auf dem „Public Security Blockchain Day“ diskutiert wurden. In diesem Sinne ist ein weiterer enger Austausch zwischen Sicherheitsbehörden und Technologie-Experten unabdingbar, um sowohl Anwendungspotenziale, als auch Kriminalitätspotenziale der Blockchain bzw. Kryptowährungen frühzeitig zu erkennen und zu nutzen. Der Bitkom möchte dafür unter anderem mit der Sicherheitskooperation Cybercrime eine Plattform bieten und den begonnen Dialog zwischen Digitalwirtschaft und Sicherheitsbehörden fortsetzen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.