Mit einer halben Million Euro[9] finanziert die EU-Kommission bereits Forschungen für das europäische Gesichtserkennungssystem. Unter Leitung des estnischen Justizministeriums prüfen polizeiliche Forensik-Abteilungen aus Finnland, Lettland, Schweden und den Niederlanden im Projekt TELEFI[10] (*Towards the European Level Exchange of Facial Images*) mögliche technische Verfahren. Mit einer nur 18-monatigen Laufzeit ist das Projekt vergleichsweise kurz, Ergebnisse sollen bereits im Sommer nächsten Jahres vorliegen.

Die grenzüberschreitende Abfrag
anschließend mit neuen EU-Prüf
gelt werden. Würde die Funktio
henden Vertrages umgesetzt, kö
ähnlichen Gesichtserkennungssystem“ erfolgen.

Quelle: https://netzpolitik.org/2019/europaeische-union-plant-europaweite-abfrage-von-gesichtsbildern/

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Anmerkungen

1 *http://dipbt.bundestag.de/dip21/btd/19/094/1909407.pdf*
2 *https://data.consilium.europa.eu/doc/document/ST-10550-2018-INIT/de/pdf*
3 *https://netzpolitik.org/2019/bka-testet-die-europaweite-vernetzung-von-polizeiakten/*
4 *https://netzpolitik.org/2018/gesichtserkennung-bei-der-bundespolizei-jede-achte-abfrage-ein-treffer/*
...termin-am-suedkreuz-die-...-beginnt/
...utsche-grossflughaefen-...er-kinder/
...soko-schwarzer-block-hamburger-
datenschutzbeauftragter-haelt-gesichtserkennung-fuer-rechtswidrig/
8 *https://netzpolitik.org/2018/gesichtserkennung-bka-will-auf-verbessertes-system-umstellen/*
9 *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/union-actions/docs/isfp-list-proposals-selected-for-funding-during-2018_en.pdf*
10 *https://www.telefi-project.eu/*
11 *http://www.cilip.de/*

Anna Biselli

Blockchain-Forensik: Wer steckt hinter einer Bitcoin-Zahlung?

Bitcoin ist eine anonyme Währung? Von wegen! Transaktionen kann jeder öffentlich einsehen. Auch wenn da erstmal nur lange Zeichenketten stehen: Es gibt Möglichkeiten zu erfahren, wer dahintersteckt. Wie, das haben wir uns von Forensiker Jakob Hasse erklären lassen.

Die einzelnen Glieder in der Blockchain mögen kryptisch wirken. Aber irgendjemand steckt dahinter CC-BY 2.0 Jinko Cruz

Ransomware verschlüsselt Dateien auf deinem Rechner, die Urheber fordern Lösegeld in Bitcoin. Jemand verschickt Erpressungsmails und hat dich angeblich beim Masturbieren gefilmt – und fordert Bitcoin. Auf Marktplätzen für illegale Drogen, Waffen oder Kreditkartendaten kann man vermeintlich anonym zahlen, natürlich mit Bitcoin.

Auf der anderen Seite stehen Meldungen, dass mit der Blockchain Verdächtige überführt[1] wurden. So im Fall der Administratoren der Darknet-Plattform Wall Street Market. Sie wollten sich mit den Bitcoins ihrer Kunden[2] aus dem Staub machen, aber begingen dann einen Fehler.

Jakob Hasse arbeitet bei der Dresdner Firma *dence*[3], die sich mit digitaler Forensik beschäftigt. Eines ihrer Spezialgebiete: Wie kann man Kryptowährungen wie Bitcoin nachverfolgen und vielleicht sogar herausfinden, wer hinter einer kryptischen Geldübertragung steht? Im Interview mit netzpolitik.org erklärt er, welche Informationen bei Blockchain-Transaktionen anfallen, was sie über die Nutzer verraten und was man beachten sollte, wenn man sich nicht gleich verraten will.

netzpolitik.org: *Wofür nutzt man Blockchain-Forensik?*

Jakob Hasse: Wir schauen uns größtenteils öffentlich verfügbare Daten an und schauen, was man daraus lernen kann. Das ist zum Beispiel interessant, wenn bei jemandem die Festplatte durch Ransomware verschlüsselt wurde und derjenige das Lösegeld gezahlt hat. Das Geld ist dann nicht gleich verschwunden, wie viele glauben.

Bitcoin kann man nachverfolgen, alle Transaktionen sind öffentlich. Oft wird gesagt, Bitcoin sei ein anonymes Zahlungssystem. Das stimmt aber nicht: Es ist ein pseudonymes System mit einem öffentlichen Transaktionsverzeichnis. Wir wissen aber erstmal nicht, welches Pseudonym zu welcher realen Person gehört und können diesen Link nicht einfach herstellen. Dafür versuchen wir, Anhaltspunkte zu finden.

Woher kommt das Geld und wo geht es hin?

netzpolitik.org: *Welche Informationen sind denn öffentlich, wenn ich etwas mit einer Kryptowährung bezahle?*

Jakob Hasse: Das kommt auf das Währungssystem an. Wenn wir über Bitcoin reden, sind die Vorgängertransaktionen und -adressen sichtbar. Das heißt: Woher kommt das Geld, das du in dieser Transaktion nutzen möchtest?

Das Geld, das du nutzt, musst du außerdem öffentlich signieren. Mit dieser Art Unterschrift beweist du, dass du der Eigentümer dieses Geldes bist. Außerdem sind die Blockchain-Adressen sichtbar, an die du das Geld senden möchtest. Sie sind wie öffentliche Schlüssel.

netzpolitik.org: *Kann ich auch erfahren, wann eine Transaktion getätigt wurde?*

Jakob Hasse: Ja, über die Blöcke. In einem Block werden viele Transaktionen zusammengefasst, er ist wie eine riesige Liste. Da sind auch Zusatzdaten drin: ein Zeitstempel und die Verbindungen zu den vorhergehenden Blöcken zum Beispiel.

Die Transaktionen in einem Block werden überprüft. Man prüft einerseits, dass kein Geld doppelt ausgegeben wurde. Andererseits, dass die Transaktionen valide sind: Dass es keine Fehler gegen die Regeln gibt, die man sich für das Blockchain-System selbst gegeben hat. Bei Bitcoin heißt das zum Beispiel: Der Miner bekommt ein bisschen von dem Geld ab, dafür dass er die Transaktion in die Liste schreibt.

Anhaltspunkte via Google-Suche

netzpolitik.org: *Welche Informationen wertet ihr bei der Blockchain-Forensik aus?*

Jakob Hasse: Das Interessante sind die Daten in den Transaktionen: Woher kommt das Geld und wohin soll es gehen? Bei einer Ransomware-Zahlung schaut man etwa, wo das Geld entlanggeht und ob es Punkte gibt, die man irgendwoher kennt. Es kann beispielsweise sein, dass jemand das Geld an eine bekannte Website spendet.

Wenn diese Website ihre Bitcoin-Adresse veröffentlicht, besteht schonmal eine Verbindung zwischen der Transaktion und einer realen Person, beziehungsweise einer Seite. Das lässt sich einfach mit einer Google-Suche herausfinden. Manchmal ergeben sich daraus Anhaltspunkte, wer hinter einer Transaktion steckt.

Anderes Beispiel: Wir haben öfter Fälle, wo Privatpersonen sehr hohe Summen verloren haben. Die Personen haben dann virtuelle Währungen genutzt, zum Beispiel zur Spekulation, und durch Betrug wie Phishing irgendwie ihre Coins „verloren". Dann ist die Frage: Wie ist das überhaupt passiert? Kann man Hinweise finden, um das Geld wiederzubekommen?

netzpolitik.org: *Virtuelle Währungen sind gerade auf Darknet-Marktplätzen verbreitet. Wie realistisch ist es denn, dass man bei Käufen auf solchen Marktplätzen unerkannt bleiben kann?*

Jakob Hasse: Auf Darknet-Marktplätzen sind virtuelle Währungen sehr beliebt, weil sie verschiedene Privacy-Charakteristiken haben. Bitcoin hat aber keine starken Privacy-Garantien, da man jeden Schritt einer Transaktion auf der Blockchain nachvollziehen kann. Man kann sehen, was mit dem Geld passiert und welche Pseudonyme damit Kontakt haben.

Das geht bei Bitcoin sogar noch besser als mit Bargeld. Wenn man Bargeld an eine andere Person zahlt, hinterlässt man höchstens durch die physische Anwesenheit Spuren.

Ich sollte mir überlegen, wie ich mein Geld einsetze. Wenn ich viel Wert darauf lege, dass meine Zahlung privat bleibt und keine Bezüge entstehen, sollte ich nur an jemanden überweisen, der nicht öffentlich bekannt ist. Wenn ich die Coins nur an meine Freunde schicke, ist das schon mal ein Vorteil. Sobald ich aber einem Dienstleister Geld schicke – beispielsweise Exchange-Börsen wie Coinbase – ist das erkennbar.

Anderer Coin, andere Eigenschaften

netzpolitik.org: *Ist das bei anderen Coins anders als bei Bitcoin?*

Jakob Hasse: Andere Krypto-Währungen wie Monero haben viel stärkere Privacy-Garantien. Auch sie bieten über kryptografische Verfahren die Garantie, dass das Geld nicht doppelt ausgegeben wurde. Ich kann beweisen, dass ich der Eigentümer bin. Aber wenn man das Geld verschickt, ist nicht mehr sichtbar, wo es herkommt. Wenn man sich bei Monero nur die Blockchain-Daten anschaut, kann man fast nichts tun.

netzpolitik.org: *Gibt es noch andere Spuren als die Transaktionshistorie, die einen bei virtuellen Währungen verraten können?*

Jakob Hasse: Die Blockchain selbst ist eine Datenbank. Zu dieser Datenbank gehört immer noch ein Netzwerk, in dem sich Teilnehmer miteinander unterhalten und Transaktionen verbreiten. Dieses Netzwerk und die Datenströme sind bei Bitcoin unverschlüsselt. Wenn ich also fürchte, dass meine Leitung überwacht wird, sollte ich VPN-Dienstleister oder Tor einsetzen, um meine Transaktionen zu senden. Sonst könnte dieser Datenstrom mit mir in Verbindung gebracht werden.

Es gibt Erweiterungen, die diesen Nachteil bei Bitcoin verbessern. Eine Variante ist, dass der Client Informationen nicht gleich an alle sendet, sondern erstmal nur an eine ausgewählte Kette – ähnlich wie beim Onion-Routing für Tor[4]. Erst später wird die Transaktion an alle gesendet.

Eine andere Methode sind sogenannte Coin-Join-Techniken[5], die zum Beispiel der Wasabi-Client[6] umsetzt. Da werden Techniken eingesetzt, um die Verbindung „Woher und wohin?" zu trennen. Bei Coin Joins findet sich üblicherweise eine Gruppe von Leuten zusammen, die ihre Coins zur Verfügung stellen und gemeinsam Transaktionen auslösen. Alles soll so möglichst gleich aussehen.

Innerhalb dieser Gruppe von Personen ist nicht mehr eindeutig nachvollziehbar, ob eine Verbindung zwischen Geldeingang und -ausgang besteht oder wo zwischen den Personen das Geld geflossen ist. Letztlich sorgt das trotzdem nur für Anonymität für die Personengruppe, die sich da zusammenfindet. Umso größer die Gruppe, desto mehr „Anonymität".

Der Übergang von digitaler zu analoger Währung

netzpolitik.org: *Wo gibt es noch zusätzliche Punkte, an denen beispielsweise die Polizei ansetzen kann?*

Jakob Hasse: Der Übergang in die analoge Welt ist der Punkt, wo Ermittler die einzige Greifbarkeit haben. Sonst ist eine Blockchain ein dezentrales System, es gibt keinen wirklichen Betreiber. Es gibt nur Individualpersonen und Unternehmen, die mitmachen oder teilnehmen. Unternehmen unterliegen einer Rechtsprechung, je nachdem in welchem Land sie sind und welche Gesetze es dort gibt.

Je nach Land müssen die Unternehmen sich unter anderem mit Geldwäscheprävention oder Terrorismusfinanzierung[7] auseinandersetzen. In der EU gibt es Vorschriften[8], an die sich Unternehmen halten müssen, die mit virtuellen Währungen hantieren.

Betreiber von Exchange-Börsen müssen beispielsweise wissen, wer ihre Kunden sind und Auszahlungsgrenzen einhalten. Das sind Elemente, die auch für traditionelle Konten gelten. Vorschriften sind je nach Land schon verschieden weit umgesetzt[9]. Manche Staaten sind relativ lax, was diese Vorschriften angeht, andere schon recht weit.

netzpolitik.org: *Wie sehr können sich eure Kunden auf eure Analysen verlassen?*

Jakob Hasse: Was wir mit Sicherheit sagen können: Wie sieht ein Zahlungsstrom aus? Was passiert in der Blockchain, wo gehen die Zahlungen entlang? Wenn Zusatzinformationen ins Spiel kommen, wenn etwa Adressen veröffentlich wurden und zugeordnet werden können: Diesen Link finden wir. Wenn bekannte Zahlungsdienstleister beteiligt sind, geben wir das mit an. Wir zeigen auch, wenn Transaktionen an bekannte Systeme gesendet werden, etwa ein Coin-Join-System.

Es geht bei uns aber nicht ausschließlich um Analysen. Eine unserer größten Aufgaben ist, die Techniken dahinter zu erklären – sei es Ermittlern oder Privatpersonen: Welche Eigenschaften hat ein Wasabi-Client? Welche Möglichkeiten und Beschränkungen gibt es? An welcher Stelle kann man keine Erkenntnisse mehr erzielen? Wo könnte man möglicherweise noch Zusatzinformationen herbekommen?

Quelle: https://netzpolitik.org/2019/blockchain-forensik-wer-steckt-hinter-einer-bitcoin-zahlung/

Anmerkungen

1 *https://www.heise.de/ct/artikel/Spurensicherung-Wie-die-Blockchain-Kriminelle-ueberfuehrt-4427702.html*
2 *https://www.sueddeutsche.de/digital/wall-street-market-darknet-verhaftung-administratoren-1.4437605*
3 *https://www.dence.de/de/products/multimedia_forensics*
4 *https://www.heise.de/ix/heft/Hinter-Schichten-2268444.html*
5 *https://en.bitcoin.it/wiki/CoinJoin*
6 *https://wasabiwallet.io/*
7 *https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html*
8 *https://news.bitcoin.com/how-eu-european-nations-regulate-cryptocurrency/*
9 *https://netzpolitik.org/2018/die-eu-kommission-moechte-kryptowaehrungen-regulieren-irgendwann-vielleicht/*

Anna Biselli

Auf einem Zettel steht, dass sie eigentlich Informatikerin ist. **Anna Biselli** war ab 2013 bei *netzpolitik.org* und ist nach einer Pause wieder als freie Autorin dabei. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund ums *BAMF* (Bundesamt für Migration und Flüchtlinge). Du erreichst sie unter *anna@netzpolitik.org* – am besten verschlüsselt [325C 6992 DCD3 1167 D9FA 9A57 1873 5033 A249 AE26]