Kapitel 3 – Technische Auswertungs- und Ermittlungsmöglichkeiten bei Blockchain-Systemen

Die Blockchain-Technologie ist vor allem aus dem Zusammenhang mit Kryptowährungen und deren Verwendung für illegale Aktivitäten bekannt. Denn da es keine zentrale Verwaltungsstelle gibt und die Nutzer nur unter den Pseudonymen der *public keys* miteinander agieren und diese einer Person nicht unmittelbar zugeordnet werden können[261], gelten Kryptowährungen als anonymes Zahlungsmittel.[262] Aus diesem Grund sind sie für illegale Aktivitäten besonders beliebt.[263] So geht eine aktuelle Studie davon aus, dass 46% der Bitcoin-Transaktionen im Zusammenhang mit illegalen Aktivitäten stehen.[264] Hierbei werden Kryptowährungen insbesondere eingesetzt, um Zahlungen zu illegalen Zwecken – wie etwa dem Kauf von Drogen oder Waffen oder zum Empfang von Erpressungszahlungen[265] – abzuwickeln oder um Geld zu waschen.[266]

Aus diesem Grund besteht ein hohes Interesse daran, illegale Aktivitäten, die im Zusammenhang mit Kryptowährungen oder Blockchains[267] stehen, aufzuklären. Dieses Interesse haben einerseits die Strafverfolgungsbehörden,[268] andererseits aber auch private Stellen/Personen, entweder, wenn sie

261 *Boehm/Pesch*, MMR 2014, 75 (76); *Safferling/Rückert*, MMR 2015, 788 (791); *Krause*, NJW 2018, 678 (679).

262 *Reid/Harrigan*, SPSN 2013, 197 (200f.); *Koshy/Koshy/McDaniel*, FC2014, LNCS 8437, 469 (469); *Krause*, NJW 2018, 678 (679).

263 *Safferling/Rückert*, MMR 2015, 788 (791); *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (1).

264 *Foley/Karlsen/Putnins*, RFS 2019, 1798 (1798).

265 *Safferling/Rückert*, MMR 2015, 788 (789). Ein Beispiel für eine Erpressung ist etwa Fall der Cyberattacke „WannaCry", bei der insgesamt 240.000 Computer gehackt und verschlüsselt wurden, bis eine Zahlung auf bestimmten Bitcoin-Adressen eingegangen waren, vgl. hierzu *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 22.

266 *Safferling/Rückert*, MMR 2015, 788 (789).

267 Siehe hierzu etwa bestimmte *Smart Contracts,* die auf der Ethereum-Blockchain abgelegt werden und als Schneeballsysteme einzuordnen sind, vgl. *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37575).

268 Vgl. insoweit das vom BMBF geförderte Forschungsprojekt BITCRIME und dessen Abschlussbericht: *Böhme/Grzywotz/Pesch/Rückert/Safferling*, Prävention von Straftaten mit Bitcoins und Alt-Coins, Handlungsempfehlung zur Regulierung virtueller

bereits Opfer von Straftaten geworden sind und eine Aufklärung durch die Strafverfolgungsbehörden nicht ausreichend gewährleistet werden kann, oder – und vor allem – bevor sie in Crowdfunding-Projekte investieren, um deren Rechtschaffenheit vorab prüfen zu lassen.[269]

Welche Möglichkeiten es gibt, um illegale Aktivitäten im Zusammenhang mit Blockchains aufzudecken und zu verfolgen, wird im Folgenden dargestellt. Dabei wird danach differenziert, auf welcher Datengrundlage die Ermittlungen basieren, da die rechtliche Bewertung unter anderem davon abhängen wird.[270]

Denn derartige Ermittlungen können zunächst am Transaktionsregister der Blockchain ansetzen,[271] da dieses – wie bereits dargestellt[272] – öffentlich einsehbar ist und alle Transaktionen seit Beginn der jeweiligen Blockchain enthält. Insoweit ist es möglich, die Transaktionen der Blockchain auszuwerten und hierdurch bspw. zu verfolgen, wohin Zahlungen im Zusammenhang mit illegalen Aktivitäten geflossen sind. Oder die Transaktionen können systematisch dahingehend ausgewertet werden, ob es Transaktionsmuster gibt, die auf illegale Aktivitäten, wie Geldwäsche oder Betrug, hindeuten (hierzu im Einzelnen unter A.).

Ein weiterer Auswertungsansatz können die technischen Eigenschaften des *Peer-to-Peer-Netzwerks* zwischen den *nodes* sein, denn hieraus können etwa die IP-Adressen einzelner Bitcoin-Adressen ermittelt werden (hierzu im Einzelnen unter B.).

Kryptowährungen. Vgl. hierzu außerdem das EU-Forschungsprojekt TITANIUM, https://www.titanium-project.eu (letzter Abruf: 20 Dezember 2021).

269 So hat sich auch in Deutschland bereits ein Markt für derartige Untersuchungen entwickelt, vgl. insoweit die Dienste des in München ansässigen Anbieters https://www.immutableinsight.com (letzter Abruf: 20. Dezember 2021).

270 Siehe für eine abweichende Differenzierung *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (1f.), die zwischen dem sog. *Clustering* und *Attribution Tagging* differenzieren. Hintergrund dieser abweichenden Differenzierung dürfte sein, dass die Autoren sich mit der Trefferwahrscheinlichkeit der dargestellten Auswertungsmöglichkeiten und deren Beweiswert im Strafverfahren auseinandersetzen.

271 Vgl. hierzu etwa *Safferling/Rückert*, MMR 2015, 788 (791).

272 Siehe hierzu oben unter Kap. 2, A.IV. m.w.N.

Darüber hinaus können die Blockchain-Daten, etwaige Auswertungsergebnisse und Daten aus dem Netzwerk mit Daten verknüpft werden, die anderweitig verfügbar sind[273] (hierzu im Einzelnen unter C.).

Zu beachten ist, dass die folgenden Auswertungs- und Ermittlungsmöglichkeiten auf Grund des schnellen technischen Wandels nicht abschließend sind. Außerdem beziehen sich die bisher entwickelten Auswertungsmöglichkeiten vorwiegend auf Bitcoin und können nicht zwangsläufig bei allen anderen Blockchain-Systemen angewendet werden. Die nachfolgenden Ausführungen dienen insoweit nur zur Darstellung, welche Auswertungen und Ermittlungen grundsätzlich möglich sind und wie diese technisch ablaufen.

A. Auswertung der Blockchain-Daten

Die unmittelbaren Blockchain-Daten können in verschiedener Art und Weise ausgewertet werden. So ist es zunächst möglich, mehrere Bitcoin-Adressen, die mit hoher Wahrscheinlichkeit von einer einzelnen Person oder Organisation kontrolliert werden, einem sog. *Entitäts-Cluster* zuzuordnen – sog. *Entitäts-Clustering*[274] (hierzu unter I.).

Außerdem kann etwa das typische Transaktionsverhalten innerhalb von Blockchains ermittelt werden, um Anomalien aufzudecken, die auf kriminelle Aktivitäten hindeuten können (hierzu unter II.).

Soweit darüber hinaus Informationen über die Hintergründe für ein bestimmtes Transaktionsverhalten bekannt sind (bspw., wenn eine bestimmte Transaktion bekanntermaßen im Zusammenhang mit Erpressungssoftware stand), kann dieses bekannte Transaktionsverhalten zunächst ausgewertet werden, um nach ähnlichen oder abweichenden Mustern innerhalb der Blockchain-Daten zu suchen (hierzu unter III.).

273 Etwa dadurch, dass ein Nutzer seine Bitcoin-Adresse in einem Forum selbst öffentlich preisgibt, indem er sie als Signatur verwendet, vgl. hierzu insbesondere *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1 (3f.).

274 Der technische Begriff des *Clusterings* beschreibt Algorithmen, die zum Aufdecken von Ähnlichkeitsstrukturen in großen Datensätzen verwendet werden. Insoweit ist die Verwendung des Begriffs im hier benutzten Kontext nicht vollständig korrekt, wird aber im Folgenden verwendet, da die Entwickler derartiger *Clustering*-Methoden im Blockchain-Kontext diese jeweils als *Clustering* bezeichnen.

I. Entitäts-Clustering

Eine der ersten, und die wohl am häufigsten zitierte, Möglichkeit[275] der Blockchain-Auswertungen ist das sog. *Clustering.*

Clustering ist in Informatik und Statistik zunächst einmal ein Verfahren zur Gruppierung von Daten mit ähnlichen Eigenschaften. Im Bereich des *Entitäts-Clusterings* ist es das Ziel, mehrere, verschiedene Bitcoin-Adressen zu einer sog. *Entität* zu gruppieren.[276]

Entität ist dabei eine Person oder Organisation, die eine oder mehrere Bitcoin-Adressen kontrolliert oder kontrollieren kann.[277] Zu beachten ist, dass das *Entitäts-Clustering* auf Grund von technischen Besonderheiten im Software-Protokoll bisher fast ausschließlich bei Bitcoin Anwendung findet. Entsprechende Anwendungen bei anderen Blockchains sind aktuell in Entwicklung, aber noch nicht ausgereift.[278]

Beim *Entitäts-Clustering* werden die folgenden Methoden (im Einzelnen unter 1. – 3.) unterschieden, wobei das sog. *Multi-Input-Clustering* (hierzu unter 1.) als das erfolgversprechendste im Bitcoin-Kontext gilt.[279]

1. Multi-Input-Clustering

Das sog. *Multi-Input-Clustering* beruht darauf, dass die Bitcoin-Nutzer Nutzer mehrere, verschiedene Bitcoin-Adressen haben – dies wird sogar zum Schutz der Privatsphäre von *Satoshi Nakamoto* empfohlen.[280] Aus diesem Grund haben Nutzer häufig mehrere, unterschiedliche Bitcoin-Adressen, auf denen sie jeweils Bitcoin (im Folgenden wird für die Bezeichnung

275 Siehe etwa: *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (132); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Pham/Lee*, arXiv:1611.03941 [cs.LG] 2016, 1 (1); *Monamo/Marivate/Twala*, ISSA2016, 129 (130); *Pesch/Böhme*, DuD 2017, 93 (95); *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (1f.).

276 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (127); *Pesch/Böhme*, DuD 2017, 93 (95).

277 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (132); *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (3).

278 Vgl. etwa *Chan/Olmsted*, ICITST 2017, 498, die ein erstes Graphen-Modell entwickelt haben, um Transaktionen in der Ethereum-Blockchain nachzuvollziehen.

279 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

280 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 6., und die Empfehlung auf: https://bitcoin.org/de/schuetzen-sie-ihre-privatsphaere (letzter Abruf: 20. Dezember 2021).

der Einheit eines Bitcoin die Abkürzung „BTC“ verwendet) in unterschiedlicher Höhe empfangen haben. Will nun ein Nutzer eine Summe an BTC an eine andere Bitcoin-Adresse transferieren, deren Höhe er nur erreicht, wenn er sein Vermögen von verschiedenen Bitcoin-Adressen kombiniert, muss er von mehreren Bitcoin-Adressen, entsprechende Transaktionen weiterleiten.[281] Dabei haben dann aber unterschiedliche Absendeadressen den gleichen Empfänger.[282]

Als Beispiel:

Hat Nutzer A 20 verschiedene Bitcoin-Adressen A_1-A_{20}, die jeweils eine Transaktion mit 1 BTC erhalten haben und will Nutzer A an Nutzer B, insgesamt 2 BTC transferieren, muss er insgesamt zwei seiner empfangenen Transaktionen weiterleiten. Absendeadressen sind dann etwa A_1 und A_2, Empfangsadresse ist nur B_1. Die Absendeadressen werden als sog. *Inputs,* die Empfangsadressen als sog. *Outputs* bezeichnet. Wenn nun eine Transaktion erstellt werden soll, bei der mehrere *Inputs* kombiniert werden müssen, um eine bestimmte Höhe an BTC zu erreichen, wird regelmäßig eine einheitliche Transaktionsnachricht erstellt, in der als *Inputs* die beiden Bitcoin-Adressen A_1 und A_2 enthalten sind, als *Output* B_1.

Da der Absender dieser Transaktion über beide *private keys* – den für A_1 und A_2 – verfügen muss, um die Transaktionsnachricht zu signieren[283], kann man annehmen, dass zumindest eine Beziehung zwischen A_1 und A_2 besteht – wenn nicht sogar die gleiche Person oder Organisation hinter beiden Adressen steht.[284]

Dementsprechend ist es möglich, die Transaktionsdaten der Blockchain nach Transaktionen mit mehreren *Inputs* bei gleichem *Output* zu durchsuchen. So ist es im Beispiel möglich die Adressen A_1 und A_2 einer *Entität* zuzuordnen.[285] Wenn nun Nutzer A von den Adressen A_2 und A_3 jeweils 1

281 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC ‘13 2013, 127 (133); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

282 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC ‘13 2013, 127 (133); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

283 Siehe hierzu oben unter Kap.2, A.II.2.

284 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC ‘13 2013, 127 (133); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

285 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2f.).

BTC an die Adresse des Nutzers C transferiert, können auch die Adressen A_2 und A_3 der *Entität* des A zugeordnet werden.[286]

Die dieser Auswertung zugrundeliegende Annahme, dass bei mehreren *Inputs* einer Transaktion diese einer gemeinsamen *Entität* zugeordnet werden können, beruht insbesondere auch darauf, dass Nutzer von Bitcoin zur Verwaltung ihrer BTC und Bitcoin-Adressen häufig sog. *Wallets* verwenden. Dies können entweder sog. *Software-Wallets* sein oder *Online-Wallet-Anbieter*. Diese *Software-Wallets* oder *Online-Wallet-Anbieter* erleichtern die Verwaltung für die Nutzer, indem sie sowohl die Bitcoin-Adressen als auch die dazugehörigen *private keys* speichern und die Transaktionsnachrichten teilweise automatisch erstellen.[287] Bei der Erstellung der Transaktionsnachrichten verknüpft die Software dann automatisch mehrere Bitcoin-Adressen als absendende Adressen.[288]

Auf dieser Grundlage können durch die Transaktionsdaten der Blockchain mehrere Bitcoin-Adressen zu einer *Entität geclustert* werden.[289]

2. Change- und Shadow-Clustering

Zwei weitere *Entitäts-Clustering*-Methoden, die sich ebenfalls Besonderheiten der Verwendung und technische Eigenheiten von Bitcoin zu Nutze machen, sind die sog. *Change- und Shadow-Clustering*-Methoden.[290]

Wie oben dargestellt, werden im Bitcoin-System nur Transaktionen weitergeleitet.[291] Wichtig hieran ist, dass Transaktionen nur als Ganzes weitergeleitet werden können – sie können aber mehrere *Outputs* haben.[292] Da der Empfänger von BTC selten eine Transaktion in voller Höhe erhalten soll, werden häufig zwei *Outputs* definiert – einerseits der Empfänger, dem BTC tatsächlich transferiert werden sollen und eine weitere Bitcoin-Adresse, die den verbleibenden Teil – also das Wechselgeld / *Change* – erhalten

286 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2f.).
287 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5.
288 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5.
289 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (132f.).
290 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (37).
291 Vgl. hierzu oben unter Kap.2, A.II.7 m.w.N.
292 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.

soll.[293] Die sog. *Change-Adresse* ist dann die Adresse, an die das Wechselgeld transferiert wird.[294]

Hat also eine Transaktion mehrere *Outputs* kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass einer der beiden *Outputs* zur Entität des Absenders der Transaktion gehört.[295]

So kann das oben bereits erwähnte Beispiel wie folgt erweitert werden:

Wenn Nutzer A von seiner Adresse A_1 eine Transaktion an die Adressen B_1 und A_4 erstellt, kann man annehmen, dass die *Entität* hinter A_1 entweder auch über B_1 oder A_4 verfügen kann.[296] Transferiert nun die Bitcoin-Adresse A_1 häufiger BTC an die Bitcoin-Adresse A_4 und eine jeweils variierende Bitcoin-Adresse, kann man annehmen, dass A_1 und A_4 zu derselben Entität gehören.[297] So ist es möglich, mit Hilfe des sog. *Change-Clusterings*, die Adressen A_1 und A_4 der Entität des A zuzuordnen.

Die *Change-Clustering*-Methode kann wiederum auf Grund einer technischen Besonderheit der *Online- und Software-Wallets* um eine weitere Auswertungsmöglichkeit erweitert werden. Denn diese erzeugen für den Empfang von Wechselgeldtransaktionen regelmäßig jeweils neue Bitcoin-Adressen, die dem alleinigen Zweck dienen bei einer bestimmten Transaktion das Wechselgeld zu empfangen.[298] Der Nutzer bekommt hiervon teilweise gar nicht erst etwas mit. Diese Wechselgeld-Adressen, die nur zum einmaligen Empfang von Wechselgeld verwendet werden, werden als sog. *Shadow-Adressen* bezeichnet.[299]

Dementsprechend ist es zusätzlich möglich, die Blockchain-Daten nach entsprechenden Transaktionen zu durchsuchen, deren Empfänger Bitcoin-

293 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133).

294 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.

295 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133).

296 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (43).

297 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (43).

298 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5f.

299 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5f.

Adressen sind, die nur dem einmaligen Empfang von Transaktionen dienen – dies ist das sog. *Shadow-Clustering*.[300]

3. Behavioural Clustering

Eine dritte *Entitäts-Clustering*-Methode ist das sog. *Behavioural Clustering*, dessen Erfolgsaussichten bisher allerdings noch nicht ausreichend geklärt sind. Beim *Behavioural Clustering* werden die Blockchain-Daten nach Mustern in Form von zeitlichen Abläufen und Strukturen der Transaktionen durchsucht.[301] Hierdurch sollen Transaktionen mit ähnlichen Mustern gefunden werden, um diese einer *Entität* zuordnen zu können.[302] Hintergrund dieser Methode ist die Annahme, dass Bitcoin-*Wallets* mit einem herkömmlichen Bankkonto vergleichbar sind und insoweit nach Verhaltensmustern der dahinterstehenden natürlichen Personen durchsucht werden können.[303]

4. Probleme der Entitäts-Clustering-Methoden

Problematisch an den soeben dargestellten Methoden des *Entitäts-Clusterings* ist, dass sie jeweils immer auf Annahmen beruhen, wie Transaktionen typischerweise ablaufen.[304] Dabei kann der typische Ablauf von Transaktionen sowohl einen technischen als auch einen persönlichen Hintergrund haben.[305]

Problematisch ist dies deshalb, weil sich der typische Ablauf von Transaktionen ändern kann und die Annahmen insoweit nicht allgemeingültig sind – insbesondere vor dem Hintergrund, dass sich das typische Transaktionsverhalten gerade auch wegen der entwickelten Auswertungsmöglichkeiten ändert.[306]

---

300 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133f.); *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5f.

301 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500).

302 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500).

303 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500).

304 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (3).

305 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (3).

306 So enthalten etwa die technischen Darstellungen der *Clustering* Methoden teilweise auch Empfehlungen, wie das Bitcoin-Protokoll angepasst werden kann, damit die

So gehen beispielsweise *Androulaki/ Karame/ Roeschlin/ Scherer/ Capkun*[307] beim *Change-Clustering* noch davon aus, dass Transaktionen, die mehrere *Outputs* haben, häufig darauf hindeuten, dass eine der beiden *Outputs* eine *Change*-Adresse ist, da Transaktionen mit mehreren Empfängern, bei denen alle *Outputs* gleichberechtigte Empfänger sind, sehr selten sind.[308]

Gerade diese Annahme wird bereits von *Meiklejohn/ Pomarole/ Jordan/ Levchenko/ McCoy/ Voelker/ Savage* dahingehend kritisiert, dass derartige Transaktionen mittlerweile keine Seltenheit mehr seien, da etwa sog. *Mining-Pools*[309] ihre Ausschüttungen in dieser Weise vornehmen würden.[310]

Ähnliches gilt für die *Multi-Input-Clustering*-Methode. Denn um die Transaktionsverläufe zu verschleiern und *Entitäts-Clustering*-Methoden zu verhindern, gibt es sog. *Mixing-Services* – wie etwa den bekanntesten *CoinJoin*.[311] Vereinfacht erstellen hierbei mehrere unterschiedliche Nutzer gemeinsam eine Transaktionsnachricht, in der sie ihre BTCs jeweils untereinander weiterversenden.[312] Hierdurch wird die Annahme des *Multi-Input-Clusterings* durchbrochen, dass bei einer Transaktion, die von mehreren unterschiedlichen Bitcoin-Adressen signiert wird, alle absendenden Adressen einer einheitlichen Entität zugeordnet werden können.[313]

Um derartige *CoinJoin*-Transaktionen identifizieren zu können, ist mittlerweile aber wiederum eine neue Auswertungsmethode entwickelt worden.[314] Diese Auswertungsmethode beruht nun auf der Eigenheit der *Coin-*

---

jeweils dargestellte Auswertung nicht mehr möglich ist, vgl. hierzu etwa *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (47ff.).

307 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42).

308 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133).

309 *Mining-Pools* sind *Full-nodes*, die sich zum Fortschreiben der Blockchain zusammenschließen, um durch die so erhöhte Rechenkapazität eine höhere Ausschüttung an Bitcoin zu erreichen. Siehe hierzu ausführlich m.w.N. *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 48; *Hofert*, Regulierung der Blockchains, S. 150f.

310 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133). Ähnlich auch *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 6f., der insbesondere darauf abstellt, dass die Erfolgswahrscheinlichkeit immer auch davon abhängt, wie die verwendete Wallet technisch funktioniert.

311 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 7.

312 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 7.

313 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 7.

314 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3f.); *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2f.).

Join-Transaktionen. Denn bei den *CoinJoin*-Transaktionen haben viele verschiedene Transaktionen die gleiche *In-* und *Output* Höhe und laufen ungefähr zu einer ähnlichen Zeit habe.[315] Auch diese Transaktionen weisen insoweit Besonderheiten auf, nach denen die Blockchain-Daten durchsucht werden können.[316]

5. Zwischenergebnis

Festzuhalten bleibt, dass es möglich ist, mehrere verschiedene Bitcoin-Adressen einer Person oder Organisation zuordnen zu können, indem die unmittelbaren Blockchain-Daten ausgewertet werden. Die jeweiligen Methoden nutzen dabei Eigenschaften von typischem Transaktionsverhalten aus. Dabei verändert sich zwar das Verständnis davon, wodurch sich typisches Transaktionsverhalten auszeichnet, diese Grundannahmen können aber von den technischen Auswertungsmethoden jeweils entsprechend angepasst werden.

II. Aufdecken von bestimmtem Transaktionsverhalten

Ähnlich funktioniert auch das Aufdecken von bestimmtem Transaktionsverhalten. Auch in diesem Kontext werden die Blockchain-Daten nach bestimmten Transaktionsmustern ausgewertet, die etwa auf Geldwäsche oder andere illegale Aktivitäten hindeuten (können).

So haben zum Beispiel *Hirshman/ Huang/ Macke* einen Algorithmus entwickelt, der auf maschinellem Lernen basiert und zunächst die Transaktionsdaten der Blockchain nach typischem und auffälligem Transaktionsverhalten analysiert.[317] In diesem Zusammenhang war etwa ein auffälliges Transaktionsverhalten, dass große Summen BTC, die anfänglich nur einer Bitcoin-Adresse zugeordnet waren, in einem ersten Schritt auf viele einzelne Bitcoin-Adressen verteilt werden und anschließend über viele Umwege wieder zu einer einzelnen Bitcoin-Adresse zusammengeführt wurden.[318]

315 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3f.).
316 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (5).
317 *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 1 (1).
318 *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 1 (2).

Ein derartiges Transaktionsverhalten lässt den Rückschluss auf Geldwäsche zu.[319]

Ein ähnliches Ziel verfolgten *Pham/ Lee*, die ebenfalls die Transaktionsdaten der Blockchain nach auffälligen Transaktionen durchsuchten, da diese in herkömmlichen Finanzsystemen regelmäßig auf illegale Aktivitäten hindeuteten.[320]

Ein Problem dieser Methoden ist häufig, dass sie nur die Daten innerhalb der Blockchain auswerten und insoweit nicht vergleichen können, was typisches (bzw. typischerweise legales) und was auffälliges (bzw. typischerweise illegales) Transaktionsverhalten ist.[321]

III. Vergleich mit bekanntem Transaktionsverhalten

Dieses Problem kann überwunden werden, wenn die Hintergründe von einzelnen Bitcoin-Adressen/-Entitäten, Transaktionen oder Transaktionsmustern bekannt sind und diese bekannten Muster dann mit anderem Transaktionsverhalten verglichen werden können.

1. Betrugs-Transaktionen

So ist es etwa möglich, die Bitcoin-Blockchain nach Transaktionen zu durchsuchen, die im Zusammenhang mit Betrug stehen.[322]

Hierzu wertet ein sog. *Classifier* zunächst das typische Transaktionsverhalten von Transaktionen aus, die bekanntermaßen im Zusammenhang mit Betrug standen.[323] Der *Classifier* ermittelt auf dieser Grundlage dann Eigenschaften von typischem betrügerischem Transaktionsverhalten.[324] In einem zweiten Schritt durchsucht dann dieser *Classifier* die Blockchain-Daten nach Transaktionsmustern, die ähnliche Eigenschaften aufweisen.[325]

---

319 *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 1 (5).
320 *Pham/Lee*, arXiv:1611.03941 [cs.LG] 2016, 1 (1).
321 *Pham/Lee*, arXiv:1611.03941 [cs.LG] 2016, 1 (1).
322 *Monamo/Marivate/Twala*, ISSA 2016, 129 (129).
323 *Monamo/Marivate/Twala*, ISSA 2016, 129 (130f.). Ein *Classifier* ist ein Algorithmus, der typische Eigenschaften in einem Datensatz ermittelt.
324 *Monamo/Marivate/Twala*, ISSA 2016, 129 (130f.).
325 *Monamo/Marivate/Twala*, ISSA 2016, 129 (131).

Ein ähnliches Verfahren wurde auch verwendet, um bei der Ethereum-Blockchain betrügerische *Wallets* und Transaktionen zu ermitteln.[326] Hierzu wurden ebenfalls verschiedene *Classifier* eingesetzt, die in einem ersten Schritt das Transaktionsverhalten von bekannten[327] betrügerischen *Wallets* und Transaktionen auswerteten.[328] In einem zweiten Schritt wurde die Ethereum-Blockchain wiederum nach Transaktionsverhalten durchsucht, das den so ermittelten Eigenschaften ähnlich war.[329]

2. Transaktionen bei Schneeballsystemen

Ein ähnliches Modell entwarfen *Chen/ Zheng/ Ngai/ Zheng/ Zhou*[330], die eine Auswertungsmöglichkeit der Ethereum-Blockchain entwickelten, um Schneeballsysteme aufzudecken.

Da die Etherum-Blockchain – wie oben dargestellt[331] – nicht nur eine Kryptowährung ist, sondern eine entwicklungsoffene Blockchain, die gerade auch für die Entwicklung und Abwicklung von *Smart Contracts* genutzt werden kann, werden auf der Ethereum-Blockchain u.a. auch *Smart Contracts* von Schneeballsystemen abgelegt.[332] Diese laufen dann ähnlich wie herkömmliche Schneeballsysteme ab – nur automatisiert.[333]

Ziel der Methode von *Chen/ Zheng/ Ngai/ Zheng/ Zhou* war es, derartige *Smart Contracts* aufzudecken.[334] Hierzu wurden zunächst die Programmcodes von *Smart Contracts* ausgewertet, soweit diese verfügbar waren.[335] So konnte ermittelt werden, welche *Smart Contracts* nach einem Schneeball-

326 *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (1).
327 Die Grundlage der „bekannten", betrügerischen *Wallets* und Transaktionen waren die Angaben von https://etherscan.io (letzter Abruf: 20. Dezember 2021), die u.a. Informationen zu einzelnen Ethereum-Adressen bzw. Ethereum-Wallets bereitstellen. Unklar ist in diesem Zusammenhang allerdings, auf welcher Grundlage diese Angaben basieren. Vgl. *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (4).
328 *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (5ff.).
329 *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (6ff.).
330 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37575ff.).
331 Vgl. hierzu oben unter Kap.2, C.II.2.
332 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37576)., die als Beispiel etwa den *Smart Contract* Rubixi benennen.
333 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37579)., die auch beispielhaft den Programmcode eines Schneeballsystems abbilden und darstellen.
334 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37575).
335 Es konnten nur solche Programmcodes ausgewertet werden, die öffentliche verfügbar waren, da eben nicht alle Programmcodes sog. *Open-Source-Codes* sind. Vgl. hierzu *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37579f.).

system funktionieren.[336] Typischerweise legt etwa ein Schneeballsystem-Programmcode die Bedingung fest, dass Beträge an diejenigen ausgezahlt werden, die zuerst einen Betrag an den *Smart Contract* transferieren.[337]

Anschließend wurde wiederum das Transaktionsverhalten der so ermittelten *Schneeball-Smart Contracts* ausgewertet – insbesondere konnte in diesem Fall das Transaktionsverhalten eines *Schneeball-Smart Contracts* mit einem *Nicht-Schneeball-Smart Contract* verglichen werden und so Unterschiede und Eigenschaften des typischen Transaktionsverhaltens ermittelt werden.[338] Auffällige Eigenschaften eines *Schneeball-Smart Contracts* waren etwa, die Rücküberweisung an Nutzer, die zuerst einen Betrag an den *Smart Contract* transferiert hatten, oder ein Ungleichgewicht von Zahlungsein- und -ausgängen.[339]

Die so ermittelten, typischen Eigenschaften der Transaktionen von *Schneeball-Smart Contracts* wurden dann wiederum in einen *Classifier* implementiert, damit dieser dann die Ethereum-Blockchain nach vergleichbarem Transaktionsverhalten durchsuchen konnte.[340]

Auf Grund dieser Methode konnten insgesamt 394 *Smart Contracts* der Ethereum-Blockchain ermittelt werden, deren Transaktionsverhalten auf ein Schneeballsystem hindeutet.[341]

3. Kategorisierung von Entitäten – Labelling

Eine weitere Auswertungsmöglichkeit ist das sog. *Labelling*. Ziel des *Labellings* ist es, Bitcoin-Entitäten danach zu kategorisieren, ob und welchen Service sie im Zusammenhang mit dem Bitcoin-System anbieten.[342]

Hierzu haben etwa *Zola/ Eguimendia/ Bruse/ Urrutia* ein stufenweises *Classifier*-Verfahren (im Folgenden als *CML* bezeichnet) entwickelt.[343] Das *CML*-Verfahren soll Bitcoin-Entitäten in eine der folgenden sechs Kategorien einordnen:

336 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37580f.).
337 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37581).
338 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37581f.).
339 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37580).
340 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37583ff.).
341 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37585).
342 Vgl. hierzu *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3497); *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1).
343 *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).

- Exchange-Services = Anbieter eines Wechsels von Fiat-Geld in Bitcoin und andersherum
- Services = Unternehmen, die Bitcoin als Zahlungsmittel entgegennehmen
- Gambling-Services = Glücksspielanbieter
- Mining-Pools[344] = Zusammenschlüsse von Rechnern, um Erträge beim Bitcoin-Mining zu steigern
- Mixing Services[345] = Anbieter, die Rückverfolgbarkeit von Transaktionen erschweren
- Marketplace = Warenhandelsplatz

Hierzu werden zunächst die Bitcoin-Adressen zu *Entitäten geclustert*.[346] Im Anschluss werten mehrere *Classifier* die Transaktionsdaten von insgesamt 311 Bitcoin-*Entitäten* aus, bei denen davon ausgegangen wird, dass sie einen dieser sechs Services anbieten. Grundlage der Annahme sind die Angaben von *„WalletExplorer"*[347]. Die *Classifier* ermitteln auf der Grundlage dieser Daten wiederum typische Eigenschaften der *Entitäten*, die einen der sechs Services anbieten.

Basierend auf den so ermittelten typischen Eigenschaften des Transaktionsverhaltens können nun die Blockchain-Daten nach vergleichbaren Mustern durchsucht werden, um so Bitcoin-*Entitäten* in eine der sechs genannten Kategorien einzuordnen. Dabei verspricht das Verfahren eine Treffer-Genauigkeit von bis zu 100%.[348]

Ein ähnliches Verfahren haben *Harlev/ Sun Yin/ Langenheldt/ Mukkamala/ Vatrapu*[349] entwickelt, mit dem Unterschied, dass die *Entitäten* in die folgenden, zusätzlichen Kategorien eingeordnet wurden[350]:

- Hosted-Wallet: Anbieter, die es Nutzern ermöglichen, Bitcoin zu nutzen, ohne selbst *node* des *Peer-to-Peer-Netzwerks* zu werden
- Merchant-Service: Zahlungsabwicklungsdienstleister, die etwa die Abwicklung von Bitcoin-Zahlungen für Online-Shops ermöglichen

344 Siehe hierzu bereits oben unter Kap. 3, A.I.
345 Siehe hierzu etwa die ausführliche Darstellung zum Mixing-Service *CoinJoin* unter Kap. 3, A.I.4. m.w.N.
346 *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (4f.). Siehe zum *Entitäten-Clustering* bereits ausführlich oben unter Kap. 3, A.I.
347 https://www.walletexplorer.com (letzter Abruf: 20. Dezember 2021).
348 *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (11).
349 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3497ff.).
350 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500f.).

- Tor-Market: Handelsplattformen, die nur über einen *Tor-Browser*[351] erreicht werden können und auf denen überwiegend illegale Güter gehandelt werden
- Ransomware: Abwicklung von (Erpressungs-)Zahlungen im Fall von Schadsoftware
- Other: *Entitäten,* die zwar identifiziert wurden, die aber keiner der genannten Kategorien entsprechen, bspw. die Spendenadresse von Wikileaks

Das *Labelling* kann insoweit insgesamt dazu verwendet werden, um die Hintergründe von Transaktionen und den mit ihnen verfolgten Zweck besser nachzuvollziehen.[352]

IV. Zwischenergebnis

Die in der Blockchain enthaltenen Transaktionsdaten bieten verschiedenste Ansatzpunkte zur Auswertung.

So können eine Vielzahl von Bitcoin-Adressen einer einzelnen *Entität* zugeordnet werden. Außerdem können die Transaktionen insgesamt nach typischem und auffälligem Transaktionsverhalten analysiert werden, bei denen bestimmte Auffälligkeiten auf illegale Aktivitäten hindeuten können. Derartige Auffälligkeiten können noch präziser ermittelt werden, wenn die Hintergründe von einzelnem Transaktionsverhalten bekannt sind, um diese als Vergleichsmaßstab heranzuziehen.

Die beschriebenen Auswertungsmöglichkeiten unterliegen allerdings einem ständigen Wandel – sowohl des Nutzerverhaltens als auch der technischen Gegebenheiten – sodass die dargestellten Auswertungsmöglichkeiten nicht abschließend oder allgemeingültig sind.

B. Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens

Zusätzliche Erkenntnisse – insbesondere über die Identitäten von Bitcoin-Adressen und -*Entitäten* – können sich durch die Auswertung des Netz-

351 Zur Funktionsweise des *Tor-Browsers*, der es für den Nutzer ermöglicht, seine IP-Adresse zu verschleiern, im Einzelnen unter Kap. 3, B.II.1.

352 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3497); *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1).

werkverhaltens und der Netzwerkverbindungen der Nutzer im Blockchain-Netzwerk ergeben. Denn, wie oben dargestellt[353], sind die *nodes* zu einem *Peer-to-Peer-Netzwerk* zusammengeschlossen, um eine unmittelbare Kommunikation untereinander zu ermöglichen.[354] Dieser unmittelbare Zusammenschluss bietet aber auch Auswertungsmöglichkeiten.

So können etwa die IP-Adressen einzelner Bitcoin-Adressen durch das Weiterleitungsverhalten von Transaktionsnachrichten im Netzwerk ermittelt werden (hierzu unter I.). Ebenso können die IP-Adressen sowohl durch Überwachung des Datenverkehrs (hierzu unter II.) als auch durch sog. *Bloom-Filter-Attacks* (hierzu unter III.) ermittelt werden.

I. Grundsatz – Auswertung der Verbreitung von Transaktionsnachrichten

Eine im Jahr 2011 entwickelte Möglichkeit, die IP-Adresse einer Bitcoin-Adresse zu ermitteln, bestand darin, sich mit allen *Full-nodes* des Bitcoin-Netzwerks gleichzeitig zu verbinden.[355] Da derjenige *node*, der eine Transaktionsnachricht erstellt und versendet, diese auch als erster ins Netzwerk versendet, konnte man davon ausgehen, dass die IP-Adresse des ersten Absenders auch die des Erstellers der Transaktionsnachricht ist.[356] Da der Absender einer Transaktionsnachricht diese auch entsprechend mit seinem *private key* signieren muss[357], konnte man annehmen, dass der Ersteller der Transaktionsnachricht auch der Inhaber der absendenden Bitcoin-Adresse war.[358] Diese Annahme muss mittlerweile nicht mehr unbedingt zutreffen. Denn auf Grund der vielzähligen kommerziellen *Online-Wallet-Anbieter* ist es für Bitcoin-Nutzer nicht mehr notwendig, selbst *node* des Bitcoin-Netzwerkes zu werden.[359]

353 Siehe hierzu oben unter Kap. 2, A.III.1.a) m.w.N.
354 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Hofert*, Regulierung der Blockchains, S. 17.
355 *Reid/Harrigan*, SPSN 2013, 197 (218); *Feld/Schönfeld/Werner*, PCS. 2014, 1121 (1122f.); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
356 *Reid/Harrigan*, SPSN 2013, 197 (218); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
357 Siehe hierzu ausführlich oben unter Kap. 2, A.II.2.
358 *Reid/Harrigan*, SPSN 2013, 197 (218); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
359 *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).

II. Das Tor-Netzwerk – IP-Adressen-Verschleierung und Auswertungsmöglichkeit

Um die soeben beschriebene Ermittlung von IP-Adressen zu verhindern, verwenden viele Bitcoin-Nutzer den sog. *Tor-Browser*, durch den IP-Adressen über das *Tor-Netzwerk* verschleiert werden können.[360]

Allerdings ist es unter bestimmten Umständen trotzdem möglich, IP-Adressen von Nutzern zu ermitteln, ebenso wie möglicherweise sogar deren Datenverkehr auszuwerten (hierzu sogleich unter 2., 3.). Hierzu werden technische Besonderheiten des Bitcoin-Netzwerk-Protokolls und des *Tor-Netzwerks* ausgenutzt. Deshalb ist zunächst ein grundsätzliches Verständnis der technischen Funktionsweise des *Tor-Netzwerks* erforderlich.

1. Technische Funktionsweise des Tor-Netzwerks

Das *Tor-Netzwerk* ist allgemein eine Möglichkeit zur Anonymisierung des Datenverkehrs im Internet.[361] Um eine solche Anonymisierung zu erreichen, stellen Freiwillige ihre Rechner dem Netzwerk als Server zur Verfügung.[362] Dies sind die sog. *Relays*, die den Datenverkehr der Tor-Nutzer so weiterleiten, dass er nur noch schwer nachvollziehbar ist.[363]

Ein Nutzer, der seinen Datenverkehr anonymisieren möchte, muss den sog. *Tor-Browser* herunterladen.[364] Wird dieser für Internetkommunikation verwendet, lädt der *Tor-Browser* sich zunächst eine Liste aller verfügbaren *Relays* von einem zentralen Verzeichnisserver herunter.[365] Anschließend wählt er eine zufällige sog. *Route* von insgesamt drei *Relays* aus, über die die Kommunikation ablaufen soll.[366] Die *Relays* werden als *Guard (1. Relay), Middle (2. Relay), Exit (3. Relay)* bezeichnet.[367] Dabei kennen die

360 *Reid/Harrigan*, SPSN 2013, 197 (218); *Feld/Schönfeld/Werner*, PCS. 2014, 1121 (1122f.); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
361 *Krause*, NJW 2018, 678 (678).
362 *Owen/Savage*, GCIG No. 20, 2015, 1 (1).
363 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (128).
364 *Owen/Savage*, GCIG No. 20, 2015, 1 (1).
365 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (128); *Owen/Savage*, GCIG No. 20, 2015, 1 (1).
366 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).
367 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).

Relays untereinander jeweils nur den vorangegangenen und den nachfolgenden *Relay* und die Kommunikation untereinander wird verschlüsselt.[368]

Der typische Zugriff – etwa auf die Google-Seite – läuft nun über die Umwege dieser drei *Relays* ab. So kann etwa der Google-Server, auf den zugegriffen wird, nur die IP-Adresse des *Exit-Relays* als diejenige erkennen, die auf die Google-Seite zugreift.[369]

Genauso läuft die Verbindung zum *Peer-to-Peer-Netzwerk* von Bitcoin über das *Tor-Netzwerk* ab, sodass für die *nodes*, mit dem der Nutzer sich verbindet, nur die IP-Adresse des *Exit-Relays* sichtbar ist.

So ist es für Nutzer möglich, ihre eigene IP-Adresse zu verbergen.

2. IP-Adressen-Ermittlung trotz des Tor-Netzwerks

Um trotzdem die oben beschriebene Verbreitung von Transaktionsnachrichten auswerten zu können und so die IP-Adressen von Bitcoin-Adressen ermitteln zu können, haben *Biryukov/ Khovratovich/ Pustogarov*[370] die oben beschriebene Auswertungsmöglichkeit erweitert. Diese Erweiterung basiert darauf, dass eine Verbindung mit Bitcoin-Netzwerk über das *Tor-Netzwerk* verhindert wird.[371]

Um dies zu erreichen, wird der sog. *Denial-of-Service*-Schutz (kurz: *DoS*) des Bitcoin-Netzwerks ausgenutzt.[372] *Denial-of-Service*-Attacken sind typische Cyberangriffe, bei denen ein Netzwerk absichtlich so überlastet wird, dass es nicht mehr verfügbar ist. Dies funktioniert regelmäßig dadurch, dass unzählig viele Anfragen an ein Netzwerk gestellt werden, unter denen dann das Netzwerk zusammenbricht.

Damit das Bitcoin-Netzwerk nicht durch eine *DoS*-Attacke überlastet wird, sieht das Bitcoin-Protokoll vor, dass jeder *node* eine Liste der IP-Adressen anlegt, mit denen er verbunden war und diese nach einem Strafpunktesystem bewertet, wenn sie „falsche“[373] Nachrichten versenden.[374] „Falsche“ Nachrichten sind etwa Transaktionsnachrichten ohne Inhalt oder

368 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).
369 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).
370 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (1ff.).
371 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
372 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3).
373 Übersetzung des englischen Begriffs „malformed“.
374 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3).

neue Blöcke ohne Inhalt. Erreicht nun eine bestimmte IP-Adresse eine bestimmte Höhe an Strafpunkten, wird sie für 24 Stunden für das Netzwerk gesperrt.[375]

Diesen Schutzmechanismus des Bitcoin-Netzwerks machen sich *Biryukov/ Khovratovich/ Pustogarov* zu Nutze, indem sie sich zunächst selbst über das *Tor-Netzwerk* mit anderen Bitcoin-*nodes* verbinden.[376] Dabei erkennen dann die Bitcoin-*nodes* nur die IP-Adresse des jeweiligen *Exit-relays* des *Tor-Netzwerks* als die IP-Adresse des verbundenen *nodes*.[377] Anschließend versenden *Biryukov/ Khovratovich/ Pustogarov* über diese Verbindung leere Transaktionsnachrichten an die verbundenen *nodes*, sodass die IP-Adressen der *Exit-relays* für eine weitere Verbindung mit dem Bitcoin-Netzwerk für 24 Stunden gesperrt werden.[378]

So kann verhindert werden, dass andere *nodes* sich über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbinden und so ihre IP-Adresse verschleiern. So können weiterhin die tatsächlichen IP-Adressen der Ersteller von Transaktionsnachrichten nach dem oben beschreibenen Verfahren[379] ermittelt werden.

Um die Ermittlung von IP-Adressen durch Auswertung der Verbreitung von Transaktions-nachrichten zu verhindern, wurde nach der Veröffentlichung der Methode von *Biryukov/ Khovratovich/ Pustogarov* die Verbreitung von Transaktionsnachrichten im Bitcoin-Protokoll entsprechend angepasst.[380] Allerdings soll auch das so angepasste Bitcoin-Protokoll Schwächen und Angriffsmöglichkeiten haben.[381]

3. Auswertung des Datenverkehrs

Die soeben dargestellte Methode, haben *Biryukov/ Pustogarov*[382] weiterentwickelt und hierbei nicht nur den *DoS*-Schutz des Bitcoin-Protokolls ausgenutzt, sondern auch Eigenheiten des *Tor-Netzwerkes* selbst, um den

375 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3).
376 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
377 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
378 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
379 Siehe hierzu unter Kap. 3, B.I.
380 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3).
381 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3) m.w.N.
382 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (122ff.).

Datenverkehr der *nodes,* die über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbunden sind, auszuwerten.[383]

Hierzu haben *Biryukov/ Pustogarov* zunächst eigene Bitcoin-*nodes* mit dem Bitcoin-Netzwerk verbunden und zusätzlich eigene *Tor-Exit-Relays* für das *Tor-Netzwerk* zur Verfügung gestellt.[384] Im Anschluss haben sich *Biryukov/ Pustogarov* selbst über *Tor-Exit-Relays,* die nicht von ihnen zur Verfügung gestellt wurden, mit Bitcoin-*nodes* verbunden, die nicht unter ihrer Kontrolle standen. Über diese Verbindung wurden dann, wie oben bereits dargestellt, wieder „falsche" Nachrichten an diese Bitcoin-*nodes* versendet.[385]

So konnten alle *Tor-Exit-Relays,* die nicht unter der Kontrolle von *Biryukov/ Pustogarov* standen, vom Bitcoin-Netzwerk gesperrt werden.[386] Wollte sich ein Nutzer nun über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbinden, musste er hierzu zwangsläufig einen der *Exit-Relays* wählen, die *Biryukov/ Pustogarov* bereitgestellt hatten.[387] So konnte der Datenverkehr eines Nutzers, der sich über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbunden hat, aufgezeichnet werden.[388] Zusätzlich haben *Biryukov/ Pustogarov* teilweise auch einzelne *Guard-Relays* für das *Tor-Netzwerk* bereitgestellt, sodass auch die IP-Adresse des verbundenen Nutzers ermittelt werden konnte und mit Bitcoin-Adressen in Verbindung gebracht werden konnte.[389]

III. Bloom-Filter-Attacks

Eine weitere Möglichkeit, um Bitcoin-Adressen und Wallets mit IP-Adressen zu verknüpfen, sind die sog. *Bloom-Filter-Attacks*.[390] Hierbei wird die technische Eigenheit der sog. *Bloom-Filter* ausgenutzt, die bei sog. *Simpli-*

383 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (125f.).
384 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (125).
385 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
386 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
387 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
388 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
389 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126f.).
390 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (326ff.); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9ff.

fied Payment Verification Clients (im Folgenden als *SPV-Clients* bezeichnet) eingesetzt werden.[391]

Hintergrund der *SPV-Clients* ist die große Datenmenge, die bei der Teilnahme am Bitcoin-Netzwerk versandt, empfangen und gespeichert werden muss.[392] Da auch Bitcoin das Ziel verfolgt, ein einfach verwendbares Zahlungsmittel und -system anzubieten, ist diese große Datenmenge hinderlich – insbesondere, wenn Bitcoin auch als mobile Zahlungsmethode verwendet werden soll. Aus diesem Grund gibt es den sog. *SPV-Client*, der mit einer geringeren Datenmenge auskommt.[393] Dieser verbindet sich mit einem *Full-node* und hinterlegt bei ihm einen sog. *Bloom-Filter*, in dem die *public keys* und Bitcoin-Adressen hinterlegt sind, die für den Nutzer eines *SPV-Clients* relevant sind – dies sind regelmäßig die *public keys* und Bitcoin-Adressen des jeweiligen Nutzers.[394]

Ein *Bloom-Filter* ist dabei eine Datenstruktur, die über *Hashfunktionen* einen schnellen Abgleich ermöglicht, ob bestimmte Daten in einer Datenstruktur enthalten sind.[395] Dabei werden *Bloom-Filter* danach bewertet, wie hoch ihre Falsch-Positiv-Rate ist.[396] Im Fall von Bitcoin *SPV-Clients* werden *Bloom-Filter* mit einer Falsch-Positiv-Rate von 0,0146% verwendet.[397]

Wenn nun der *Full-node* neue Transaktionen von anderen *nodes* empfängt, fragt er beim *Bloom-Filter* ab, ob die *public keys* und Bitcoin-Adressen der neuen Transaktionen im *Bloom-Filter* enthalten sind.[398] Nur wenn das der Fall ist, leitet er die relevanten Transaktionsnachrichten an den *SPV-Client* weiter.[399] Dieser kann dann die Transaktionen verifizieren, wenn sie etwa in seiner *Wallet* enthalten sind.[400]

391 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (326); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
392 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327f.); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9f.
393 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 10.
394 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9f.
395 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9.
396 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9.
397 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 10.
398 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327).
399 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327).
400 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9f.

Die Ermittlungsmöglichkeit besteht nun für den *Full-node*, mit dem sich ein *SPV-Client* verbindet.[401] Da in der Bitcoin-Blockchain alle bisher verwendeten *public keys* und Bitcoin-Adressen enthalten sind, ist es für einen *Full-node* möglich, alle *public keys* und Bitcoin-Adressen des Bitcoin-Netzwerks beim *Bloom-Filter* abzufragen.[402] Da sowohl *public keys* als auch Bitcoin-Adressen bei dem *Bloom-Filter* hinterlegt sind, sinkt die Wahrscheinlichkeit, dass ein doppelt-falsch-positives Ergebnis ermittelt wird.[403] Wenn also sowohl *public key* als auch Bitcoin-Adresse als positives Ergebnis vom *Bloom-Filter* angegeben werden, ist es äußerst wahrscheinlich, dass die Bitcoin-Adressen sich tatsächlich in der *Wallet* des *SPV-Clients* befinden.[404]

Da außerdem eine Netzwerkverbindung zwischen *SPV-Client* und *Full-node* aufgebaut werden muss, in der zur Kommunikation auch die IP-Adresse des *SPV-Clients* übermittelt werden muss, können insoweit Bitcoin-Adressen einer IP-Adresse zugeordnet werden, sofern der *SPV-Client* nicht über das *Tor-Netzwerk* mit dem *Full-node* verbunden ist.[405]

IV. Zwischenergebnis

Die *Peer-to-Peer*-Verbindung des Bitcoin-Netzwerks bietet die Möglichkeit die IP-Adressen von Bitcoin-Nutzern zu ermitteln und diese unter Umständen einer Bitcoin-Adresse zuzuordnen.

Zwar gibt es etwa durch das *Tor-Netzwerk* die Möglichkeit IP-Adressen zu verschleiern, allerdings beinhalten auch diese Möglichkeiten ihre Schwachstellen, die eine erweiterte Auswertungsmöglichkeit zur Folge haben können.

Eine weitere Möglichkeit zur Ermittlung von IP-Adressen sind die bei *SPV-Clients* verwendeten *Bloom-Filter*.

Zu berücksichtigen ist aber auch hier, dass die vorgestellten Ermittlungsmöglichkeiten immer von den jeweiligen technischen Funktionsweisen und dem Nutzerverhalten abhängen und auf Grund der fortwährenden Anpassung der technischen Funktionsweise nicht abschließend oder allgemeingültig sind.

401 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (328); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
402 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
403 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
404 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
405 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (328).

C. Auswertung durch Verknüpfung mit anderweitig verfügbaren Daten

Neben den bereits dargestellten Auswertungsmöglichkeiten ist es außerdem möglich, die Blockchain-Daten mit anderweitig verfügbaren Daten zu verknüpfen, um hieraus weitergehende Erkenntnisse über die Identitäten der Bitcoin Nutzer und deren Transaktionsverhalten zu erhalten.

So kann etwa das Internet – insbesondere Internetforen – nach Bitcoin-Adressen durchsucht werden, die von Nutzern oder Dritten veröffentlicht wurden (hierzu unter I.). Außerdem können etwa Daten von Drittanbieter-Cookies ausgewertet werden (hierzu unter II.) und bei blockchain-basierten *Internet-of-Things*-Anwendungen (im Folgenden als *IoT* bezeichnet) etwa Standortdaten ausgewertet werden (hierzu unter III.).

I. Durchsuchen des Internets nach Bitcoin-Adressen

Vor allem in der Anfangszeit von Bitcoin und anderen Kryptowährungen veröffentlichten Bitcoin-Nutzer ihre eigenen Bitcoin-Adressen – insbesondere in ihren Signaturen in Internetforen – um die Kryptowährung populär zu machen.[406]

Da die Bitcoin-Adressen und *public keys* eine bestimmte Zeichenstruktur haben[407], können Internet und Forenseiten systematisch nach derartigen Zeichenstrukturen mittels *Web-Crawler*[408] durchsucht werden.[409] So können zunächst verschiedenste Bitcoin-Adressen ermittelt und im Anschluss ausgewertet werden, ob diese etwa im Zusammenhang mit weiteren Informationen – wie etwa einer E-Mail-Adresse – veröffentlicht wurden.[410]

406 *Reid/Harrigan*, SPSN 2013, 197 (213); *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1.

407 Für ein Beispiel vgl. *Kaulartz*, CR 2016, 474 (475).

408 Ein *Web-Crawler* ist ein Programm, das automatisch das Internet oder Webseiten nach bestimmten Inhalten durchsucht.

409 *Reid/Harrigan*, SPSN 2013, 197 (213); *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1 (3).

410 *Reid/Harrigan*, SPSN 2013, 197 (213); *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1 (3f.).

II. Auswertung von Dritt-Anbieter-Cookies

Eine weitere Auswertungsmöglichkeit besteht dann, wenn Bitcoin-Adressen auf Internetseiten angegeben und/oder verwendet werden, die Daten an Drittanbieter weitergeben und die so ermittelten Informationen dann mit den Transaktionsdaten der Blockchain verknüpft werden können.[411] Solche Drittanbieter werden insbesondere bei Online-Shopping-Seiten eingesetzt – etwa für Analyse-, Werbe- oder Zahlungsabwicklungszwecke.[412]

Bei einem normalen Online-Einkauf sind typischerweise folgende Parteien beteiligt:[413]

- Käufer
- Verkäufer
- Zahlungsabwicklungsdienstleister
- *Webtracker*

Bietet nun der Verkäufer die Zahlungsabwicklung über Bitcoin oder eine andere Kryptowährung an, kann es sein, dass auf der abschließenden Bestellseite *Webtracker*[414] von Drittanbietern (wie etwa Googleanalytics) eingesetzt werden.[415] So werden teilweise etwa Daten wie der Preis, der Bestellzeitpunkt, die E-Mail-Adresse des Bestellers oder der Name des Bestellers an Dritte übermittelt.[416]

Außerdem wird der Käufer regelmäßig nach Abschluss des Bestellvorgangs auf eine Zahlungsseite weitergeleitet, die regelmäßig vom Zahlungsabwicklungsdienstleister[417] betrieben wird.[418] Der Zahlungsabwicklungsdienstleistungsanbieter lässt sich dann die entsprechende Summe BTC an eine von ihm benannte – und teilweise extra für diese Zahlung gene-

411 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (1ff.).
412 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (1).
413 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).
414 *Webtracker* sind Analyseprogramme, die das Nutzungsverhalten eines Besuchers einer Internetseite analysieren. Im Fall von Online-Shopping-Seiten wird etwa analysiert, welche Artikel angeklickt oder in den Warenkorb gelegt werden. Vgl. hierzu ausführlich *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (2f.).
415 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).
416 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4ff.).
417 Bspw. der Anbieter https://bitpay.com (letzter Abruf: 20. Dezember 2021) bietet die Abwicklung derartiger Zahlungen an.
418 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).

rierte Bitcoin-Adresse – überweisen.[419] Auch bei diesen Abläufen werden Drittanbieterdienste in Anspruch genommen. So vereinfachen etwa viele Zahlungsabwicklungsdienstleister die Zahlung für den Besteller dadurch, dass die Bitcoin-Empfangsadresse als QR-Code dargestellt wird.[420] Die Erstellung des QR-Codes wird aber regelmäßig von Dritten vorgenommen, sodass hierzu mindestens die Bitcoin-Empfangsadresse an diesen Dritten übermittelt wird.[421] Je nachdem, welche Informationen dabei noch an den Dritten übermittelt werden, kann dieser nun die Blockchain-Transaktionsdaten nach einer entsprechenden Transaktion durchsuchen und so zumindest die Bitcoin-Adresse des Käufers ermitteln.[422]

Je nachdem, welche Daten an Dritte übermittelt werden, ist es für diese im Anschluss möglich anhand der Transaktionsdaten der Blockchain zu ermitteln, welche Transaktionen im Zusammenhang mit den ihnen vorliegenden Daten steht.[423] So kann etwa die maßgebliche Transaktion in der Blockchain herausgefunden werden und so unter Umständen mit der E-Mail-Adresse oder dem Namen des Bestellers verknüpft werden.[424]

III. Standortdaten-Ermittlung bei IoT-Blockchain-Anwendungen

Die neueste Untersuchung des Privatsphäreschutzes bei Blockchain-Anwendungen von *Shahid et. Al.* setzt sich mit der Frage auseinander, ob ein ausreichender Schutz der Privatsphäre bei blockchain-basierten IoT-Systemen besteht, die u.a. auch Standortdaten enthalten und übermitteln.[425]

Betrachtet wird hierbei eine genehmigungsbedürftige Blockchain für ein sog. *Vehicular Ad Hoc Network* (im Folgenden als *VANET* bezeichnet).[426] Ein *VANET* ist ein Kommunikationssystem für Kraftfahrzeuge, die sich gegenseitig über Fahrverhältnisse wie etwa Stau, ein abruptes Bremsen oder

419 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).
420 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (6).
421 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (6).
422 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (6ff.).
423 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (9).
424 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (9f.).
425 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (116ff.).
426 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).

Ähnliches informieren, um mehr Sicherheit im Straßenverkehr zu ermöglichen.[427]

Hierbei läuft die Kommunikation der Fahrzeuge untereinander wiederum über ein *Peer-to-Peer-Netzwerk* ab, in dem die Fahrzeuge jeweils unter den Pseudonymen von *public keys* agieren.[428] Allerdings müssen die Fahrzeuge vorher bei einer zentralen Registrierungsstelle angemeldet werden, die dann die *public keys* vergeben.[429]

Inhalt der Kommunikation sind auch die jeweiligen Standortdaten der Fahrzeuge.[430] Dementsprechend ist es theoretisch möglich, wenn ein *public key* einem Fahrzeug zugeordnet werden kann, ein entsprechendes Bewegungsprofil des Fahrzeugs zu erstellen.[431]

IV. Zwischenergebnis

Die Transaktionsdaten der Blockchain können durch anderweitig verfügbare Daten aus dem Internet angereichert werden, um Ermittlungsergebnisse zu erhalten. Dabei können diese Daten etwa aus einer eigenen Veröffentlichung herrühren[432], aber auch unbewusst vom Betroffenen an Dritte übermittelt werden[433]. Soweit die Identitätsdaten der Betroffenen zentral verwaltet werden, kann dies zu erweiterten Auswertungsmöglichkeiten führen, die hier nur beispielhaft unter III. dargestellt wurden.

Auch hier ist anzumerken, dass die Auswertungsmöglichkeiten stark vom Nutzungsverhalten abhängen und insoweit nicht allgemeingültig sind.

427 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
428 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
429 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
430 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
431 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (120).
432 Siehe hierzu unter Kap. 3, C.I.
433 Siehe hierzu unter Kap. 3, C.II.

D. Zwischenergebnis

Bereits die bloßen Transaktionsdaten in der Blockchain bieten ein breites Spektrum an Auswertungsmöglichkeiten – insbesondere, wenn Hintergründe einzelner Transaktionsdaten bekannt sind und so ein Vergleich möglich ist.

So ist es zunächst möglich, mehrere Bitcoin-Adressen einer *Entität* zuzuordnen. Deren Transaktionsverhalten kann außerdem kategorisiert werden, wenn es vergleichbar ist mit dem Transaktionsverhalten von bekannten Services. Außerdem kann ausgewertet werden, was typisches und was atypisches Transaktionsverhalten ist und ob es bestimmte Transaktionen gibt, die auf illegale Aktivitäten wie Geldwäsche oder Betrug hindeuten.

Diese Auswertungsmöglichkeiten können präzisiert werden, wenn Daten des Netzwerkverhaltens und der Netzwerkverbindungen ausgewertet werden. So ist es unter Umständen möglich, eine Bitcoin-Adresse einer IP-Adresse zuzuordnen und möglicherweise auch den Datenverkehr eines *nodes* auszuwerten.

Weitere Erkenntnisse können sich außerdem durch die Verknüpfung mit anderweitig verfügbaren Daten ergeben.

Besonders hervorzuheben ist, dass die jeweils dargestellten Auswertungsmöglichkeiten kombiniert werden können.

So kann zum Beispiel eine IP-Adresse, die einer Bitcoin-Adresse durch eine *Bloom-Filter*-Attacke zugeordnet werden kann, durch ein *Multi-Input-Clustering*-Verfahren auf eine ganze *Entität* bezogen werden und deren Verhalten insgesamt als das eines *Exchange-Services* klassifiziert werden.

Zu beachten ist aber, dass alle Auswertungsmöglichkeiten entweder vom Nutzungsverhalten des Betroffenen oder von technischen Eigenheiten abhängen. Beides unterliegt einem stetigen, schnellen Wandel – insbesondere auch auf Grund der Auswertungsmöglichkeiten. Aus diesem Grund sind die hier lediglich auszugsweise vorgestellten Auswertungsmöglichkeiten nicht allgemeingültig und hängen davon ab, ob die technischen Eigenheiten und das jeweilige Nutzerverhalten weiterhin bestehen.