POLIZEIAKADEMIE NIEDERSACHSEN

Kryptowährungen als Mittel zur Finanzierung des islamistischen Terrorismus

Bachelorarbeit im Bachelorstudiengang „Polizeivollzugsdienst (B.A.)“ an der Polizeiakademie Niedersachsen

von

Thomas Faelligen

Abgabedatum: *09.05.2016*

POLIZEIAKADEMIE NIEDERSACHSEN

Kryptowährungen als Mittel zur Finanzierung des islamistischen Terrorismus

Bachelorarbeit

von

Thomas Faelligen

BA 07/13, StGr. 310 H

t.faelligen@arcor.de

Tel.: 0152 54 06 38 91

Betreuer:	Dr. Roman Povalej, Professor an der Polizeiakademie
Zweitprüferin:	KHK'in Kathrin Jahn
Studienort:	Hann. Münden
Dienststelle:	PD GÖ / PI Nienburg ZKD
Abgabedatum:	09.05.2016

Inhaltsverzeichnis

1 Einleitung

„*Wo waren Sie am 11. September?*“

Die meisten Leser werden nun innerlich einen detaillierten Film abspulen, obwohl weder Jahr noch Uhrzeit aus der Frage hervorgehen. Auch der Autor kann sich noch gut erinnern:

Am 11. September 2001 kam meine Mutter früher als sonst nachhause, rief uns ins Wohnzimmer und schaltete den Fernseher ein. Dort war zunächst von einer „Naturkatastrophe“ oder „vielleicht einem Flugzeugabsturz“ die Rede, so als könne man die Wahrheit gar nicht glauben. Ich war gerade in die sechste Klasse gekommen, und obwohl ich mich dunkel an frühere schlimme Ereignisse erinnern kann, hatte ich nun zum ersten Mal das Gefühl, dass da draußen etwas nicht stimmte.

In der Folgezeit kam es zu immer weiteren Vorfällen, die den internationalen islamistischen Terrorismus in den Fokus rückten und die in der aktuellen Konfrontation mit dem sogenannten Islamischen Staat einen Höhepunkt finden.

Die Täter verüben nicht nur Anschläge auf europäischem Boden wie jüngst in Paris (13.11.2015) oder Brüssel (22.03.2016), sondern nutzen diesen auch zur Vorbereitung ihrer Taten, bedienen sich moderner sozialer Medien zur Propaganda in Europa, und rekrutieren sogar Kämpfer aus den westlichen Demokratien.[1] Damit ist dies ein Thema, das auch vonseiten der deutschen Polizei höchste Aufmerksamkeit verdient hat.

Gegenstand dieser Arbeit ist die Finanzierung des islamistischen Terrorismus unter Verwendung von Kryptowährungen. Ob solche Währungen überhaupt zur Finanzierung dschihadistischer Aktivitäten eingesetzt werden, ist bislang nicht belegt. Dennoch ist dies kein unrealistisches Szenario, das schon allein aufgrund seines Potenzials eine nähere Betrachtung rechtfertigt.

Motivation für diese Arbeit ist vor allem die Hoffnung, damit einen Beitrag zur Bekämpfung des islamistischen Terrorismus leisten zu können. Ein Auslöschen der zugrundeliegenden Konflikte und Ideologien kann natürlich nicht erreicht werden, ein teilweise Schwächung scheint immerhin möglich.

1 siehe Kapitel 2.3.

Ziele der Arbeit sind daher:

1. Dem nicht weiter spezialisierten Sachbearbeiter aufzuzeigen, was konkret auf derartige Aktivitäten hinweist, damit Erkenntnisse gesammelt und weitergeleitet werden können.
2. Dem spezialisierten Sachbearbeiter Ansätze zu geben, welche Interventionen im Einzelfall denkbar sind und was für Ermittlungsansätze, gegebenenfalls in Zusammenarbeit mit anderen Behörden, genutzt werden können.
3. Eine weitergehende Zusammenarbeit von Polizei und Wissenschaft anzuregen, um die zahlreichen sich anschließenden Fragen zu untersuchen und konkrete Konzepte zu entwickeln.

Im Grundlagenkapitel 2 „Islamistischer Terrorismus“ wird zunächst eine Einführung in die aktuell relevanten dschihadistischen Entwicklungen (2.1) und die zugrunde liegende Ideologie (2.2) unternommen. Es folgt eine Darstellung der Bezüge zu westlichen Staaten (2.3) und eine Übersicht über gängige Finanzierungsmodelle (2.4).

In einem weiteren Grundlagenkapitel 3 „Kryptowährungen“ werden kryptographische Grundlagen erklärt (3.1), die Funktionsweise von Kryptowährungen am populären Beispiel Bitcoin erläutert (3.2), und ein Blick auf weitere Währungen geworfen (3.3).

Kapitel 4 „Terrorismusfinanzierung mittels Kryptowährungen“ beinhaltet Szenarien, wie Kryptowährungen in Form von direkten Spenden (4.1) oder Off-Chain-Transaktionen (4.2) zur Unterstützung des Dschihadismus verwendet werden könnten. Danach wird ein Blick auf ihre Verwertbarkeit geworfen (4.3).

Hieran anknüpfend folgt in Kapitel 5 „Identifikation der Akteure und Gegenmaßnahmen“ zunächst eine tabellarische Aufstellung und dann in den Punkten 5.1 bis 5.4 eine ausgewählte Reihe von Ermittlungsansätzen, die in diesem Zusammenhang erfolgversprechend erscheinen.

Die Ergebnisse der Arbeit werden in Kapitel 6 „Zusammenfassung und Ausblick“ noch einmal festgehalten. Außerdem werden dort Anregungen für künftige Arbeiten und Anstrengungen gegeben.

Rechtliche Fragen werden in dieser Arbeit bewusst nicht thematisiert.

2 Islamistischer Terrorismus

Der Islamistische Terrorismus umfasst Gewalthandlungen, die auf Grundlage einer islamistischen Ideologie begangen werden. Ideologische Rechtfertigung ist der Dschihad weswegen sich im Englischen der Begriff *jihadism* eingebürgert hat. Die deutsche Entsprechung *Dschihadismus* soll im Folgenden synonym für den islamistischen Terrorismus verwendet werden. Umfasst sind grundsätzlich auch alle Handlungen, die von terroristischen Vereinigungen im Rahmen des Bürgerkriegs als Konfliktpartei oder unter Ausübung von Staatsgewalt begangen werden und daher keinen Terror im engeren Sinne darstellen.

In Kapitel 2.1 wird ein Blick auf die wesentlichen aktuellen Entwicklungen des Dschihadismus geworfen, ehe in Kapitel 2.2 dessen ideologische Grundlage betrachtet werden. Kapitel 2.3 stellt Bezüge des Dschihadismus zu westlichen Staaten her. In Kapitel 2.4 werden Modelle der Finanzierung des islamistischen Dschihadismus vorgestellt.

2.1 Dschihadimus als Phänomen der Gegenwart

Der Dschihadismus ist eine moderne Erscheinung, deren Anfänge im Krieg gegen die sowjetische Besatzung Afghanistans in den 80er Jahren des vergangenen Jahrhunderts liegen. Aus den islamistischen Auslandskämpfern, die als *Mudschaheddin* dort den Dschihad gegen die atheistischen Besatzer (die Sowjets) unterstützten, ging Ende der 80er Jahre die Gruppe **Al Qaida** unter Führung Osama Bin Ladens hervor[2]. Nach der Stationierung US-amerikanischer Streitkräfte in Saudi-Arabien im Rahmen der Annektion Kuwaits durch den Irak ab 1991 richtete sich das Augenmerk Al Qaidas verstärkt auf die USA und ihre Verbündeten in Europa sowie die kooperierenden Regime des arabischen Raums.[3] Dies gipfelte im Anschlag auf das World Trade Center vom 11. September 2001. Im darauf reagierenden Engagement der USA und zahlreicher Bündnispartner in Afghanistan und der Entwicklung von umfassenden Anti-Terror-Strategien inklusive gezielter Tötungen, aber gerade auch Finanzsanktionen, wurde Al Qaida weitgehend in den Untergrund gedrängt.[4] Anstelle einer globalen Gruppe sind heute lokale

2 Vgl. Seidensticker 2015 [48] S. 92, Neumann 2015 [43] S. 56, 60-62.
3 Vgl. Seidensticker 2015 [48]. S. 94f.
4 Vgl. Zarate 2013 [52] S. 87, Cronin 2015 [14] S. 90.

Ableger aktiv, insbesondere im Maghreb (AQIM) und auf der arabischen Halbinsel (AQAP).[5] Im Syrienkrieg ist Al Qaida mit der Al Nusra-Front vertreten.[6] Al Qaida hat aber von Anschlägen im Westen keineswegs Abstand genommen, sondern propagiert im seit 2011 erscheinenden Onlinemagazin *Inspire* (arabisch und englisch, herausgegeben durch AQAP[7]) den sogenannten ***Lone Jihad***[8]: Ohne zentrale Planung werden im Westen lebende Einzelpersonen aufgefordert, Ziele auf eigene Faust anzugreifen; zur „Inspiration" dienen Bombenrezepte, Todeslisten, u.ä. Stéphane Charbonnier, ein beim Angriff auf die Pariser Redaktion von Charlie Hebdo am 7. Januar 2015 getöteter Karikaturist, stand auf einer solchen Liste[9], Al Qaida bekannte sich zu dem Anschlag[10].

Die Gruppe **ISIS** (im Folgenden immer so genannt, weitere Bezeichnungen: IS, ISI, ISIL, Islamischer Staat, Daesh, Dawlat, Khilafa) ist aus der Gruppe Al Qaida im Irak (AQI) hervorgegangen. Während der Besetzung des Iraks durch die USA 2003-2011 verübte diese sunnitische Gruppe zahlreiche Anschläge auf mit den Streitkräften assoziierte Einrichtungen, aber insbesondere auch auf die schiitische Zivilbevölkerung und die jesidische Minderheit.[11] Sie zeichnete sich dabei durch eine Grausamkeit und Maßlosigkeit aus, die selbst vom heutigen Al Quaida-Chef az-Zawahiri in einem Brief an den damaligen Anführer von AQI, az-Zarqawi, gerügt wurde.[12] Die gesteigerte Gewaltsucht des ISIS mag ideologische oder strategische Gründe haben. So propagiert der islamistische Vordenker Abu Bakr Naji in „The Management of Savagery" eine Strategie, die an das Vorgehen von ISIS erinnert.[13] Obwohl durch die abschreckende Gewalt zunächst der Unterstützung der sunnitischen Stämme beraubt,[14] gelang es ISIS nach Abzug der amerikanischen Truppen aus dem Irak und Ausbruch des Bürgerkriegs im Nachbarland Syrien, seit 2011 immer größere Flächen in diesen Staaten zu kontrollieren, was im Ausruf des Kalifats

5 Vgl. Seidensticker 2015 [48] S. 100, Neumann 2015 [43] S. 166-177.
6 Vgl. Seidensticker 2015 [48] S. 100.
7 Nach Neumann 2015 [43] S. 67, 177 unter Regie des 2011 getöteten *Anwar al-Awlaki*. In *Inspire* selbst ist „*Al Malahem Media*" als Herausgeber angegeben.
8 Oder *lone wolf jihad*, bei Neumann 2015 [43] S. 67, 158f. „einsame Wölfe". Der Begriff lässt sich bereits aus der Bezeichnung „*lone mujahid"* in *Inspire* 1 (2010) [1] S. 40 ableiten, inmitten einer Sektion zum „Open Source Jihad" (S. 32ff.). In *Inspire* 10 (2013) [2] S. 46 steht der Begriff *Lone Jihad* in einer Überschrift.
9 Vgl. *Inspire* 10 (2013) [2] S. 15.
10 im Rahmen eben einer solchen *Lone-Jihad-Operation*, siehe *Inspire* 14 (2015) [3] S. 37ff.
11 Ein geschichtlicher Abriss zu ISIS und seinen Vorgängern findet sich in Neumann 2015 [43] S. 67ff., ausführlicher al-'Ubaydi et al. 2014 [50] S. 8-26.
12 Vgl. Az-Zawahiri 2005 [53] S. 4ff., besonders S. 10.
13 Vgl. Neumann 2015 [43] S. 86ff.; siehe ferner Brachman / McCants 2006 [10] S. 6-14; die englische Übersetzung des Buches befindet sich im digitalen Anhang [40].
14 Vgl. Cronin 2015 [14] S. 94f., Neumann 2015 [43] S. 78f.

am 29.06.2014[15] gipfelte. Hierbei spielten Auslandskämpfer einer jüngeren Generation aus dem ganzen arabischen Raum, aber nicht zuletzt auch aus Westeuropa, eine wichtige Rolle. Die nun folgende Intervention benachbarter Staaten wie auch westlicher Kräfte führte zu einer weiteren Globalisierung des Konflikts. Außerdem erklärten, durch den Erfolg von ISIS beeindruckt, diverse lokale dschihadistische Gruppen ihre Treue (z. B. Boko Haram, Teile von AQAP, libysche Gruppen, Teile des Kaukasusemirats).

ISIS bedient sich stärker noch als Al Qaida moderner Kommunikationsmittel. So erscheinen neben dem professionellen Propagandamagazin *Dabiq* (arabisch, englisch, teils andere Sprachen) diverse Kriegsberichte, Nachrichten, Bildmaterial und Videos. Diese werden auf Seiten wie *justpaste.it* oder *archive.org* eingestellt und in sozialen Medien (z.B. auf *twitter*) über ein Netzwerk assoziierter Accounts bzw. durch Sympathisanten verlinkt.[16] ISIS richtet ein erhöhtes Augenmerk auf Kommunikationssicherheit und gibt Empfehlungen unter anderem zum Verzicht auf iPhones zugunsten von Android-Smartphones, zur Nutzung von Chatsecure, Surespot und Kik (sämtlich Messenger mit jeweils unterschiedlichen Sicherheitskonzepten), oder zum Aufrufen dschihadistischer Seiten über Tor (einen populären Anonymisierungsdienst zur Verschleierung der IP- Adresse).[17]

ISIS erhebt den Anspruch, sich an alle Sunniten weltweit zu richten. Diese werden wahlweise zur ***Hidschra*** oder zum Lone Jihad aufgefordert.[18] Hidschra bezeichnet ursprünglich den Auszug Mohammeds von Mekka nach Medina im Jahre 622, hier im speziellen die Einreise von Sunniten in das von ISIS kontrollierte Territorium. ISIS gibt in einem online veröffentlichten Reiseführer Tipps zur Reise aus Europa über die Türkei in das Gebiet des Kalifats[19] und fordert im Dabiq nicht nur Kämpfer, sondern auch Familien und bestimmte Berufsgruppen zur Hidschra auf[20]. Dies unterstreicht den Anspruch von ISIS auf Staatlichkeit.

Neben Al Qaida und ISIS existieren weitere dschihadistische Gruppierungen, die jedoch weniger global orientiert sind und daher aus westlicher Sicht eine geringere Bedeutung haben.

15 Vgl. Al-'Ubaydi et al. 2014 [50] S. 9, *Dabiq* 1 (2014) [25] S. 7.
16 siehe Screenshot am Ende dieses Kapitels.
17 Vgl. *Hijrah* 2015 [28] S. 47.
18 Vgl. *Dabiq* 12 (2015) [27] S. 3.
19 Der entsprechende Reiseführer *Hijrah* 2015 befindet sich im digitalen Anhang [28].
20 Vgl. *Dabiq* 12 (2015) [27] S. 33, *The Revived Caliphate* 2014 [24] S. 73.

Es folgt ein nachbearbeiteter (vergrößerter) Screenshot einer Recherche nach einem arabischen Hashtag vom 27.04.2016 auf *twitter.com*. Eine systematische Recherche wurde nicht betrieben, er soll lediglich als Beispiel dienen:

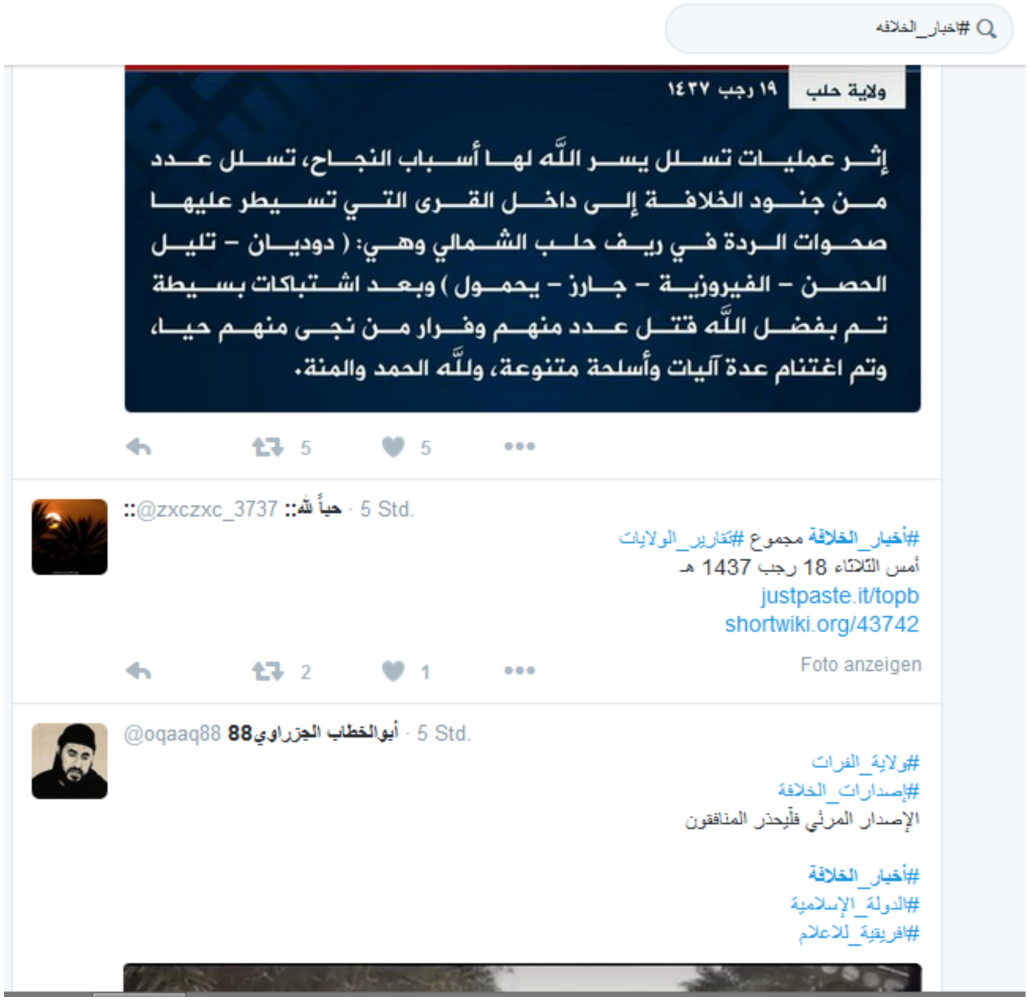

***Abbildung 1 (Screenshot)**:* Ergebnisse auf *twitter.com* für den Hashtag #اخبار_الخلافه (zu deutsch etwa: „Nachrichten aus dem Kalifat“, URL: https://twitter.com/hashtag/%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1_%D8%A7%D9%84%D8%AE%D9%84%D8%A7%D9%81%D9%87?src=rela
Der Link *justpaste.it/tobp* ist als. pdf im digitalen Anhang einzusehen [32]. Beim Profilbild von *@oqaaq88* handelt es sich um das Konterfei az-Zarqawis. Das von ihm gepostete Video (unterer Bildrand) ist ein Propagandavideo der ISIS-Agentur *Al Furat*, das die Enthauptung von Gefangenen zeigt. Weitere Screenshots befinden sich im digitalen Anhang. Übersetzungen des arabischen Hashtags auf deutsch oder englisch sind weniger ergiebig (Beispiele: #KhilafaDE, #ISIS, #AllEyesOnISIS).

2.2 Ideologischer Hintergrund

All diese Entwicklungen sind schwer zu verständlich, ohne die ideologischen Hintergründe des Dschihadismus zu kennen. Unter dem Begriff ***Islamismus*** versteht man Bestrebungen, sämtliche Bereiche des privaten und öffentlichen Lebens nach den Regeln des Islam zu gestalten. Allgemein werden die gegenwärtigen Lebensumstände der Muslime als unislamisch, pervertiert und sündhaft angesehen. Dieser Zustand wird mit dem Begriff *Dschahiliya* bezeichnet, der eigentlich die vorislamische heidnische Zeit bezeichnet. Dies wird unter anderem auf eine Dominanz der islamischen Welt durch den Westen zurückgeführt.[21]

Abhilfe schaffen soll in der hier relevanten ***salafistischen*** Ausprägung ein staatliches Gebilde, dessen Wesen, Führung, Gesetze sich streng am Islam ausrichten. Dabei sind zwei Rechtsquellen dominant: Der **Koran** und die ***Sunna***, das Vorbild Mohammeds, welches in *Hadithen*, kurzen Augenzeugenberichten, überliefert ist.[22] Es gibt mehrere kanonische Hadithsammlungen, die verbreitetsten sind der Sahih Muslim und der Sahih al-Buchari. Während der Sunnismus noch weitere Rechtsquellen (*Idschma* und *Qiyas*) kennt und in vier anerkannte Rechtsschulen, jeweils mit einer anderen Auffassung des *Fiqh* (Erörterung dieser Rechtsquellen) unterteilt ist, ist es für die salafistische Strömung des Islamismus typisch, eine wörtliche Auslegung des Koran ohne Rücksicht auf die Tradition der Koranexegese (*Tafsir*) zusammen mit der *Sunna* als alleinige Quellen des Handelns anzuerkennen. Solche Strömungen werden auch als islamischer ***Fundamentalismus*** bezeichnet.[23]

Die fundamentalistische Auffassung erlaubt es, dass Aufforderungen des Koran, die Ungläubigen (***Kufar***) unter gewissen Umständen bis auf den Tod zu bekämpfen, zum Leitbild des Handelns genommen werden. Als Kufar gelten auch Apostaten (vom Glauben abgefallene Muslime), als solche werden beispielsweise die *Bahai* angesehen, teils aber auch all jene Muslime, die sich den fundamentalistischen Ideen widersetzen, oder gar die gesamte Schia, die abwertend als *Rafida* (pl: Rawafid; „Ablehner“) bezeichnet wird, da sie die Kalifen vor Ali „ablehne“. [24]

21 Vgl. Seidensticker 2015 [48] S. 9 (Definition), S. 55 (Dschahiliya), S.36f. (westliche Dominanz). Zu letzterem auch Neumann 2015 [43] S. 50.
22 Vgl. Seidensticker 2015 [48] S. 19 und besonders S. 24f.
23 Vgl. Seidensticker 2015 [48] S. 11f.
24 Eine gebündelte Darstellung zu dieser Thematik findet sich in Seidensticker 2015 [48] S. 104-113.

Um die Tötung eines Muslim im Dschihad zu rechtfertigen, wird der ***Takfir*** angewandt, die Exkommunikation bzw. Erklärung zum Apostaten.[25] Ein solcher Muslim wird als *Murtad* bezeichnet. Im aktuellen Dabiq wird beispielsweise der deutsche Konvertit und Salafist *Pierre Vogel* als Murtad bezeichnet, wohl da er öffentlich Anschläge wie den vom 13.11.2015 in Paris als *haram*, Sünde bezeichnet hatte (dies impliziert ein augenscheinlich von der ISIS-Agentur Furat Media publiziertes Video, im Dabiq selbst findet sich keine Begründung).[26]

Unterschiedliche Auffassungen bestehen besonders darin, was der einzelne Muslim tun soll, um auf ein islamisches Kalifat hinzuwirken. So wird teilweise ein Rückzug aus der verdorbenen Gesellschaft (innere Hidschra) propagiert, gegensätzliche Strömungen sehen im **Dschihad** das Mittel der Wahl. Dschihad bezeichnet im Koran den bewaffneten Kampf der jungen muslimischen Gemeinde gegen die sie bedrängenden Völker. Hierbei wiederum ist umstritten, ob der Dschihad nur zur Befreiung von nichtmuslimischen Herrschaften zulässig ist, oder ob auch invasives Vorgehen dadurch gerechtfertigt werden kann. Auch ist umstritten, ob es genüge, wenn eine islamische Gesellschaft eine Reihe von Kämpfern stelle, oder ob der Dschihad eine individuelle Pflicht für jeden Einzelnen sei. Generell wird ein Krieg *zwischen* Muslimen nie als Dschihad bezeichnet. Zum Dschihad kann die Tötung von Muslimen daher nur werden, wenn zuvor der Takfir angewandt wurde[27] Dies ist zu Beispiel im sunnitisch-schiitischen Konflikt im Irak der Fall, wo ISIS die Tötung von Schiiten als Dschihad vorantreibt, da es sich bei den Schiiten generell um eine Abspaltung handele.[28]

Auch was den Dschihad gegen Juden und Christen angeht, gibt es unterschiedliche Auffassungen. Um Anschläge auf diese laut Koran zunächst geschützte Gruppen zu rechtfertigen, wird angeführt, dass die westlichen Staaten den arabischen Raum militärisch und politisch unterdrückt hielten (US-Streitkräfte in Saudi Arabien, Eingriffe in Irak und Syrien, aber auch: erhöhte Kindersterblichkeit durch UN-Sanktionen gegen den Irak unter Saddam Hussein).[29] Während Al Qaida jedoch „nur“ zur Tötung besonders islamfeindlicher oder besonders einflussreicher Personen auffordert,[30] hält

25 Vgl. Seidensticker 2015 [48] S. 109.
26 *Dabiq* 14 (2016) [31] S. 16. Das Video ist betitelt mit „Die Wahrheit über Pierre Vogel“ und kann (Stand 07.05.2016) über folgenden Link abgerufen werden: https://drive.google.com/file/d/0BwukzJVK7EetWTNCT2ZFdXFpd1E/view?pref=2&pli=1
27 Zum Dschihad siehe Seidensticker 2015 [48] S. 105-109.
28 Vgl. *Dabiq* 13 (2016) [30] S. 10ff.
29 Vgl. Seidensticker 2015 [48] S. 111.
30 Vgl. *Inspire* 14 (2015) [3] S. 82ff.

ISIS die gesamte Bevölkerung westlicher Demokratien für verantwortlich.[31] ISIS legt großen Wert auf Anerkennung seines Kampfes als Dschihad und führt als Beweis u.a. Bilder gefallener Mudschaheddin an, deren Leichen noch nach Tagen frisch seien, ganz wie es im Koran, Sure 2:154 beschrieben werde.[32] Hintergrund ist, dass im Dschihad gefallene Kämpfer (*Märtyrer*) nach islamischer Vorstellung sofort ins Paradies einziehen, während sich bei einem gewöhnlichen Muslim erst am jüngsten Tag entscheidet, ob ihm das Paradies oder das Höllenfeuer zuteil wird.[33]

Eine genaue Analyse der ideologischen Rechtfertigungen könnte Klarheit liefern, ob hier eher eine Ideologie strategisch durchgesetzt wird, oder ob eine Strategie ideologisch gerechtfertigt wird. Dies könnte Thema einer eigenen Bachelorarbeit sein.

Die Tendenz, bekannte islamische Topoi auf sich selbst zu umzumünzen, zeigt sich auch in der Namensgebung *Dabiq* für das eigene Magazin. Nach der islamischen **Eschatologie**, wie sie im Sahih Muslim[34]dargelegt ist, ist das Dorf Dabiq im Norden Syriens einer von zwei möglichen Orten, an dem die Heere der Kreuzfahrer auf die Streitmacht der Muslime treffen werden (der andere genannte Ort liegt in der Türkei).[35]

Ein weiteres Charakteristikum ist die Anlehnung an die Zeit der Kreuzzüge. So werden westliche Christen im Vokabular von Al Qaida und ISIS häufig als ***Kreuzfahrer*** bezeichnet[36], was eine Aggression seitens des Westens und einen defensiven Dschihad impliziert. Die Ambitionen, das Kalifat bis nach Rom auszudehnen,[37] unterstreicht diese Bezugnahme.

Die Inanspruchnahme des Islams seitens ISIS darf nicht übersehen, sollte aber auch nicht überschätzt werden. Die Führer ebenso wie die Kämpfer handeln aus unterschiedlichen Motiven. Die Führung von ISIS besteht aktuell fast ausschließlich aus Irakern, von denen einige bereits unter Saddam Hussein Positionen in der Armee oder Verwaltung innehatten.[38] Die irakische

31 Vgl. Neumann 2015 [43] S. 161, das dortige Zitat findet sich in *Dabiq* 4 (2014) [26] S. 9.
32 Siehe *The Revived Caliphate* 2014 [24] S. 61, dort auch eine englische Übersetzung der Sure.
33 Vgl. Seidensticker 2015 [48] S. 110f.
34 *Sahih Muslim* Buch 41, Hadith 6924. In der hier verwendeten Ausgabe [39] wird eine andere Zählweise verwendet: Buch 64, Kapitel 35, Nr. 2030 (Band II S. 1070).
35 Siehe auch Neumann 2015 [43] S. 88f. und als Primärquelle *The Islamic State* 2015 [29] S. 90f.
36 Die englische Bezeichnung *crusader* findet sich beispielsweise in *Dabiq* 14 (2015) [31] 40 mal, in *Inspire* 10 (2013) [2] immerhin 16 mal.
37 Man betrachte beispielsweise die Titelseite des *Dabiq* 4 (2014) [26], eine Fotomontage der IS-Flagge auf dem Petersplatz.
38 Vgl. Neumann 2015 [43] S. 91.

Anhängerschaft setzt sich aus sunnitischen Stämmen zusammen, deren Hauptfeind die schiitisch geprägte Zentralregierung des Irak ist. Außerdem bestehen ethnische Konflikte zu den (größtenteils sunnitischen) Kurden. Der Konflikt mit den Jesiden ist sowohl ethnisch als auch konfessionell geprägt. Auf syrischer Seite hat die Reaktion des Assad-Regimes auf den sogenannten *Arabischen Frühling* einen unübersichtlichen Bürgerkrieg ausgelöst, in dem die Al-Nusra-Front und ISIS als relativ gut organisiert und schlagkräftig gelten und somit gegenüber den zerstrittenen „gemäßigten" Oppositionsgruppen eine höhere Attraktivität besitzen. Die örtlichen Kämpfer handeln dabei vielfach aus rationalen Motiven.[39] Am einheitlichsten ideologisch motiviert sind die Auslandskämpfer. Sie erlauben es ISIS, sich als pansunnitische Bewegung darzustellen und dienen auch als Sprachrohr zum Westen.[40]

2.3 Bezüge zu westlichen Staaten

Der islamistische Terrorismus hat zwar sein Zentrum in den sunnitisch geprägten Bereichen des arabischen Raums und Afghanistans / Pakistans, dennoch richtet sich das Augenmerk der Dschihadisten auch und gerade auf den Westen, zum einen in zuletzt vermehrt auftretenden terroristischen Aktionen, ganz besonders aber in der Propaganda. Ziel solcher Anschläge und Propaganda kann es sein, die entsprechenden Staaten zu einer militärischen Enthaltung bzw. einem Rückzug zu bewegen, oder aber eine Überreaktion des Staates und weitere Polarisierung hervorzurufen. Beides kann aus dschihadistischer Sicht nützlich sein, letzteres vor allem, um die lokalen sunnitischen Gegner als Kollaborateure und Marionetten hinstellen und den Bürgerkrieg weiterhin als Dschihad gegen die Kreuzfahrer klassifizieren zu können.[41]

Abgesehen von diesen strategischen Gründen ist der Westen aber auch deshalb vom Dschihadismus betroffen, weil hier teils sehr große sunnitische Minderheiten leben, die sich mit den Konflikten in der islamischen Welt identifizieren. So ist zu beobachten, dass islamistisches Gedankengut vor modernen, wohlhabenden und säkularen Gesellschaften keinen Halt macht, sondern dass gerade das Klischee einer moralisch verkommenen Konsumgesellschaft dem Islamismus die Möglichkeit gibt, sich als Gegenmodell zu etablieren. So hat sich seit der Jahrtausendwende unter

39 Zu den Motivationen der einheimischen Kämpfer vgl. Neumann 2015 [43] S. 91f.
40 Für eine Darstellung der Motive der Auslandskämpfer siehe Neumann 2015 [43] S. 112-121.
41 Vgl. Neumann 2015 [43] S. 162.

anderem in Deutschland eine wachsende salafistische Szene etabliert, deren prägendes Element ein ideologischer Fundamentalismus ist, der sich in einer strikten Ablehnung des pluralistischen Gesellschaftsmodells widerspiegelt. Innerhalb dieser Szene existieren auch Strömungen, die den gewaltsamen Kampf propagieren.[42] Solche Personen(gruppen) könnten durch entsprechende Aufrufe oder bestimmte Anlässe (z.B. Veröffentlichung von Mohammed-Karikaturen) zum Lone Jihad angestachelt werden.

Erschreckend ist besonders die große Zahl der aus Deutschland und anderen europäischen Staaten in das syrisch-irakische Kriegsgebiet Ausreisenden. Eine Analyse der Radikalisierungshintergründe der aus Deutschland Ausgereisten zeigt, dass es sich vielfach um in Deutschland geborene junge Männer handelt, die oft zunächst im Bereich der einfachen Kriminalität aufgefallen sind. Es folgte schließlich eine Verankerung im Umfeld der salafistischen Szene und eine Zuwendung zum Islam in seiner fundamentalistischen Ausprägung. Dabei scheint besonders die gegenseitige soziale Unterstützung eine wesentliche Rolle zu spielen. So finden sich unter den Auswanderern oft ganze Gruppen, die schon zuvor in der salafistischen Szene eng miteinander verbunden waren.[43]

ISIS ruft insbesondere auch „Zivilisten“ dazu auf, sich auf die Hidschra in das Kalifat zu machen. Dabei werden gezielt Angehörige bestimmter spezialisierter Berufsgruppen gesucht, an denen es offenbar mangelt.[44] Es ist möglich, dass ISIS auch versuchen wird, Absolventen bestimmter Fächer anzuwerben und somit am gut ausgebauten westlichen Ausbildungssystem teilzuhaben. Auch könnte versucht werden, das Fachwissen bestimmter Firmen abzuschöpfen.

Westliche Staaten sind somit strategisch wie ideologisch in vielerlei Hinsicht für den Dschihadismus bedeutsam. Nicht unterschätzt werden sollte auch, dass Faktoren wie die gut ausgebaute Infrastruktur, die soziale Absicherung und die einfache Verfügbarkeit vieler Waren und Dienstleistungen einen attraktiven Aktions- und Rückzugsraum für dschihadistische Gruppierungen bedeuten. Zwar herrscht diesbezüglich mittlerweile eine stärkere Sensibilität seitens des Verfassungsschutzes und der Polizei. Dennoch ist nicht auszuschließen, dass Europa und Amerika für diverse logistische Zwecke,

42 Zur salafistischen Szene in Europa siehe Seidensticker 2015 [48] S. 27f. sowie Neumann 2015 [43] S. 138ff.

43 BKA et al. 2015 [12] haben hierzu eine umfangreiche Analyse vorgelegt; siehe auch Neumann 2015 [43] S. 144f. Zur Bedrohung durch Auslandskämpfer findet sich eine differenzierte Einschätzung in al-‘Ubaydi et al. (2014) [50] S. 89-99.

44 Siehe *The Revived Caliphate* (2014) [24] S. 73.

Ausarbeitung ideologischer Schriften, Bearbeitung und Verbreitung propagandistischen Bildmaterials, Programmierung von Anwendungen oder allgemein für solche Handlungen eine Bedeutung spielen, die in einem Kriegsgebiet schwer zu realisieren sind und bei denen die Gefahr der Strafverfolgung relativ gering ist. Eine Untersuchung solcher Aktivitäten anhand offen zugänglicher Quellen im Sinne einer wissenschaftlichen Arbeit ist schwierig und wurde hier nicht unternommen. Entsprechende Ermittlungen werden mit Sicherheit durch die zuständigen Behörden durchgeführt.

2.4 Modelle der Terrorismusfinanzierung

Die Bedrohung durch derart global agierende Terrororganisationen auch im Westen erscheint ernst und äußerst aktuell. Es ist eine drängende Herausforderung für die Sicherheitsbehörden, hierauf die passenden Antworten zu finden. Neben Aufklärung, Überwachung oder Prävention ist auch das Abschneiden finanzieller Mittel eine solche Antwort.

Dschihadistische Gruppen benötigen ein gewisses Einkommen, um handlungsfähig zu bleiben. Kosten bereiten nicht nur die Planung und Durchführung von Anschlägen, sondern auch die Aufrechterhaltung von Infrastruktur, die Versorgung der Mitglieder, Propaganda, Rekrutierung, Unterhalt von Trainingscamps, und Leistungen an die sympathisierende Bevölkerung, beziehungsweise, im Fall von ISIS, an die Einwohner des Kalifats.[45] Die Durchführung von Aktionen im Rahmen des Lone Jihad ist hingegen vergleichsweise günstig.[46] Das bedeutet jedoch nicht, dass Maßnahmen gegen die Finanzierung des Dschihadismus hier aussichtslos sind. Denn auch der Lone Jihad wäre ohne die Ausstrahlungskraft eines globalen Dschihad und ohne die Verbreitung entsprechender Propaganda in weitaus geringerer Form zu erwarten.

Um ihre Kosten zu decken, bedienen sich dschihadistische Gruppen einer Vielzahl verfügbarer Quellen. Als „klassische“[47] Modelle gelten private Spenden, der Missbrauch gemeinnütziger Organisationen, organisierte Kriminalität, Schutzgelderpressung, Lösegelderpressung, Unterhalt legaler Unternehmen und Finanzierung durch staatliche Stellen.[48] Bedingt durch seine quasistaatliche Rolle bedient sich ISIS jedoch einer breiteren Palette von

45 Vgl. Humud et al. 2015 [23] S. 13f., FATF 2015 (b) [19] S. 9f.
46 Vgl. FATF 2015 (b) [19] S. 10f., Normark / Ranstorp 2015 [45] S. 8ff.
47 „*Traditional Methods*“ laut Einteilung in FATF 2015 (b) [19] S. 13-20.
48 Vgl. ebd.

Mitteln, wie dem Verkauf von Öl, dem Schmuggel erbeuteter Antiquitäten, der Konfiszierung der Bestände örtlicher Banken, oder der Besteuerung von Warenverkehr und Einkommen im kontrollierten Gebiet.[49]

Eine weitere Quelle stellen Gelder dar, die durch Sympathisanten in anderen, auch westlichen Staaten, erwirtschaftet und anschließend transferiert werden. Dieses Einkommen macht nach derzeitigem Stand nur einen kleinen Teil des Gesamteinkommens von ISIS aus.[50] Durch die Beschneidung anderer Mittel könnte seine Wichtigkeit jedoch steigen. Außerdem sollte grundsätzlich auch jede geringe Quelle mit der nötigen Aufmerksamkeit behandelt werden.

Die **Erwirtschaftung** von Geldern durch Angehörige der westlichen salafistischen Szene oder anderer Sympathisanten und die Nutzbarmachung für den Dschihadismus kann grundsätzlich auf legalem wie auf illegalem Weg erfolgen. Das Sammeln von Spenden für vermeintlich wohltätige Zwecke, die Aufnahme von Krediten ohne Rückzahlungsabsicht, oder andere Arten von Betrug stellen nur einige der Möglichkeiten dar.[51]

Die **Nutzbarmachung** bedeutet nicht zwangsläufig einen Transfer ins dschihadistische Kerngebiet. Möglich ist auch eine Nutzung für Tätigkeiten im Westen (beispielsweise Logistik, Propaganda, Spionage) oder ein Einkauf benötigter Waren oder Dienstleistungen. So bringen Auslandskämpfer in vielen Fällen selbst bezahlte Ausrüstungsgegenstände in das Kalifat mit.[52]

Der Transfer von Geldern aus dem Westen in den Einflussbereich kann auf verschiedenen Wegen stattfinden.

In manchen Fällen werden Bargeld, Gold, Kreditkarten oder andere Wertgegenstände auf direktem Wege durch spezielle Kuriere überführt oder von Auslandskämpfern mitgebracht.[53]

Eine weitere viel genutzte Methode ist auch die **Überweisung** kleinerer Beträge an scheinbar privat genutzte reguläre Bankkonten im Aktionsbereich von ISIS.[54]

Statt über reguläre Bankkonten können Transaktionen jedoch oft einfacher, schneller und anonymer über sogenannte ***Money Service Businesses*** bzw. ***Money and Value Transfer Services*** wie *Western Union, Money Gram* und

49 Vgl. FATF 2015 (a) [18] S. 12-18., Humud et al. 2015 [23] S. 4-12, Levitt 2014 [33] S. 2-10.
50 Vgl. Humud et al. 2015 [23] S. 11, FATF 2015 (a) [18] S. 18f.
51 Vgl. Normark / Ranstorp 2015 [45] S. 12-18.
52 Vgl. FATF 2015 (b) [19] S. 24ff.
53 Vgl. FATF 2015 (a) [18] S. 29., Normark / Ranstorp 2015 [45] S. 20.
54 Vgl. FATF 2015 (a) [18] S. 27f..

dergleichen abgewickelt werden. Diese Dienste sind in vielen Staaten des Nahen Ostens verfügbar und werden oft für Rücküberweisungen von Gastarbeitern und anderen Migranten an ihre Familien genutzt.[55]

Eine weitere Möglichkeit stellt das im Nahen Osten weit verbreitete ***Hawala***-Finanzsystem dar, das ebenfalls vielfach für Überweisungen von Migranten an ihre Familien genutzt wird. Hawala basiert auf einem Netz aus selbständigen Hawaladaren, sprich Händlern, die untereinander Zahlungen auf verschiedenen Wegen vornehmen. Ein Kunde kann bei seinem örtlichen Hawaladar eine Einzahlung machen, die der vorgesehene Empfänger dann bei seinem eigenen Hawaladar abheben kann, schon bevor eine Transaktion zwischen den Hawaladaren stattgefunden hat. Dabei kann zur Authentifizierung ein Passwort ausreichend sein. Das System basiert auf Reputation der Hawaladare und gegenseitigem Vertrauen. Die Transaktionen können weitgehend geheim und anonym gehalten werden, geschehen sehr schnell und sind nur mit geringen Gebühren belastet. [56]Schwachpunkt dieser Methode ist jedoch, dass Hawaladare suspekte Zahlungen verweigern und zur Entanonymisierung beitragen können, wenn sie nicht wünschen, dass ihre Dienste zur Terrorismusfinanzierung in Anspruch genommen werden. Auch sind manche Methoden, wie das fundraising über soziale Medien, mit Hawala nicht möglich.[57]

Der virtuelle Transfer von Kryptowährungen könnte ein weiteres Modell zur Finanzierung des Dschihadismus durch Sympathisanten aus dem Westen darstellen. Dieses Modell verspricht die Möglichkeit einer recht weitreichenden Anonymisierung, ist sehr schnell und günstig und hat darüber hinaus den Vorteil, dass eine in die Wege geleitete Transaktion grundsätzlich nicht mehr rückgängig gemacht oder verändert werden kann.[58]

Bevor jedoch im vierten Kapitel Szenarien der Terrorismusfinanzierung mittels Kryptowährungen angesprochen werden, ist zunächst eine Einführung in deren Grundlagen und Konzepte notwendig.

55 Vgl. ebd. S. 28, Normark / Ranstorp 2015 [45] S. 18f.
56 Einen umfassenden Überblick über Hawala bietet FATF 2013 [17].
57 Zu Vor- und Nachteilen von Hawala für Zwecke der Terrorismusfinanzierung siehe Brantly 2014 [11] S. 2.
58 Vgl. FATF 2015 (b) [19] S. 35f.

3 Kryptowährungen

Es existieren verschiedene Konzepte von Kryptowährungen, allen gemeinsam ist die Verwendung einer dezentralen Infrastruktur ebenso wie die Nutzung kryptographischer Konzepte als Notwendigkeit. Damit unterscheiden sich Kryptowährungen von anderen Konzepten für online-Transaktionen, wo eine herkömmliche Transaktion lediglich online verwaltet wird und Kryptographie nur notwendig ist, um immanenten Sicherheitsproblemen des Internets zu begegnen und auch online eine Legitimation ohne gegenständlichen Beweis (wie Gesicht oder Unterschrift) zu gewährleisten.[59]

Neben der Bezeichnung Kryptowährung sind auch die Bezeichnungen digitale oder virtuelle Währung verbreitet, die in dieser Arbeit jedoch nicht verwendet werden.

Eine dezentrale Infrastruktur bedeutet konkret die Nutzung eines ***Peer-to-Peer-Netzwerkes (P2P)***. Ein P2P-Netzwerk zeichnet sich durch direkte Internetverbindungen zwischen gleichberechtigten *Clients* aus, im Gegensatz zur hierarchischen Server-Client-Struktur, wie sie im World-Wide-Web, bei E-Mail und anderen Anwendungen vorherrschend ist. Ein einzelner Client im P2P-Netzwerk wird als *Peer* bezeichnet.[60]

Die dezentrale Infrastruktur hat auch die Notwendigkeit einer ***Blockchain*** zufolge, einer Datenbank des gesamten Zahlungsverkehrs, die für jeden zugänglich ist.

Kryptowährungen basieren auf Transaktionen zwischen **pseudonymen Adressen**. Ein Nutzer kann beliebig viele dieser Adressen erzeugen. Er kann virtuelles Geld von einer seiner eigenen Adressen auf eine beliebige eigene oder fremde Adresse überweisen. Von dieser Adresse aus kann der nächste Nutzer es weiter überweisen. Dazu muss er mittels **Kryptographie** beweisen, dass er dazu berechtigt ist. Um unter anderem zu gewährleisten, dass kein virtuelles Geld doppelt überwiesen wird, muss jede Transaktion von einer Reihe anderer Nutzer (sogenannte *Miner*) auf Korrektheit überprüft werden. Derart bestätigte Transaktionen werden in einem Block in der Blockchain gespeichert. Mithilfe der Blockchain lässt sich jede Transaktion auf Schlüssigkeit überprüfen und verifizieren, Fehler werden – so die Theorie – ausgeschlossen.

59 Vgl. Antonopoulos 2015 [6] S. 1ff.
60 Eine Einführung in P2P-Netzwerke bieten Mahlmann / Schindelhauer 2007 [34] S. 6-8.

In Kapitel 3.1 werden die kryptographischen Grundlagen für Kryptowährungen betrachtet, ehe in Kapitel 3.2 eine Erläuterung der Funktionsweise am Beispiel von Bitcoin erfolgt. In Kapitel 3.3 werden alternative Kryptowährungen vorgestellt.

3.1 Kryptographische Grundlagen

Für das Verständnis von Kryptowährungen sind zwei mathematische Konzepte aus der Kryptographie unerlässlich: kryptographische Hash-Funktionen und Signaturen.

Signaturen wiederum sind untrennbar mit **asymmetrischer Verschlüsselung**[61] verbunden. Bei einer asymmetrischen Verschlüsselung wird eine Nachricht mit einem Schlüssel ***pk*** (für *public key*) verschlüsselt. Dieser ist öffentlich, was das Problem des Schlüsseltauschs bei der herkömmlichen symmetrischen Verschlüsselung behebt. Damit einher geht aber, dass ***pk*** nicht geeignet sein darf, die Nachricht zu entschlüsseln, denn sonst könnte jeder, der die Nachricht abfängt und den öffentlichen Schlüssel recherchiert, sie auch lesen. Zum Entschlüsseln ist daher ein anderer Schlüssel ***sk*** (*secret key*) nötig, den nur der Empfänger kennt. Mathematisch betrachtet ist die Verschlüsselung mit ***pk*** eine Funktion, die aus der Nachricht ***m*** (*message*) und dem Schlüssel ***pk*** eine verschlüsselte Nachricht ***c*** (*ciphertext*) berechnet. Diese darf sich jedoch nicht einfach nach ***m*** umstellen und auflösen lassen, es ist sozusagen eine Einweg-Funktion. Andererseits muss eine Funktion existieren, die ***c*** mithilfe von ***sk*** wieder auf ***m*** abbildet. Diese darf sich natürlich nicht nach ***sk*** auflösen lassen, da sonst der Absender aus ***m*** und ***c*** auf ***sk*** schließen könnte. Schließlich muss sich ***pk*** aus ***sk*** generieren lassen, aber nicht umgekehrt. Es gibt mathematische Verfahren, die diese Anforderungen erfüllen, die bekannteste davon ist *RSA*. Die genauen mathematischen Grundlagen sind jedoch nicht Bestandteil dieser Arbeit.

Eine **Signatur**[62] funktioniert grundsätzlich ganz ähnlich. Hier geht es dem Sender einer Nachricht darum, zu beweisen, dass niemand anders als er die Nachricht gesendet hat. Dazu berechnet er aus der Nachricht ***m*** mithilfe von ***sk*** eine Signatur ***s*** (*signature*), die er zusammen mit dieser Nachricht verschickt. Dieser Vorgang gleicht einer Entschlüsselung, nur dass ***m*** zuvor

61 Zu asymmetrischer Verschlüsselung siehe Schmeh 2013 [47] S. 175-200.

62 Zu Signaturen siehe Narayanan et al. 2016 [42] S. 37-41, Antonopoulos 2015 [6] S. 62-69, Schmeh 2013 [47] S. 201-210.

bekanntlich gar nicht verschlüsselt war und der „entschlüsselte“ Text ***s*** daher natürlich keinen Sinn ergibt. Natürlich darf sich wiederum ***sk*** nicht aus ***m*** und ***s*** zurück berechnen lassen. Der Empfänger „verschlüsselt“ nun die empfangene Signatur ***s*** mithilfe von ***pk*** und prüft, ob die „verschlüsselte“ Signatur ***m'*** mit der Nachricht ***m*** übereinstimmt, die er ebenfalls erhalten hat. Natürlich darf sich ***s*** nicht einfach aus ***m*** und ***pk*** erstellen lassen, denn dann könnte jeder, der ***pk*** kennt, eine gültige Signatur zu einer beliebigen Nachricht erstellen. Es gibt jedoch auch hier mathematische Konzepte, die diese Anforderungen erfüllen.

Die Berechnung einer Signatur aus einer großen Zahl ist sehr aufwändig und liefert eine große Datenmenge als Ergebnis. Dies ist einer der Gründe für die Verwendung kryptographischer Hash-Funktionen.

Eine **Hash-Funktion**[63] bildet eine beliebig große Zahl auf einer Zahl fester Länge ab. Die erzeugte Zahl wird als Hash bezeichnet. Beispielsweise ließe sich der Text dieser Bachelorarbeit dezimal kodiert einfach als sehr große Zahl auffassen. Aus dieser Zahl könnte mittels mathematischer Berechnungen eine neue, wesentlich kürzere Zahl erstellt werden. Wendet man hierzu die Funktion *SHA-256* an, ergibt sich eine Reihe von 256 Bitfeldern, die jeweils mit 0 oder 1 gefüllt sind. Diese Reihe ließe sich wiederum in eine Dezimal, Buchstabenfolge, oder in ein beliebiges anderes Format umkodieren.

Wollte man diese Bachelorarbeit nun signieren, könnte man stattdessen auch einfach mit deutlich geringerem Rechenaufwand ihren Hash-Wert signieren, vorausgesetzt natürlich, dieser kann nicht gefälscht werden. Denn sonst könnte ein Angreifer eine korrekt signierte Nachricht dieser Bachelorarbeit kopieren und dann den Text der Bachelorarbeit so verändern, dass ihr Hash-Wert immer noch mit dem signierten Hash-Wert übereinstimmt. Diese veränderte Arbeit könnte er zusammen mit der Originalsignatur weiterverschicken, sodass der Anschein einer unkorrumpierten Nachricht entsteht. Das Fälschen eines Hash-Wertes ist tatsächlich wesentlich einfacher als das eigentliche Fälschen der Signatur, weil lediglich eine ***Kollision*** gefunden werden muss, die denselben Hash-Wert erzeugt. Daher stellt die Kryptographie hohe Anforderungen an Hash-Funktionen, die auch von einer Reihe von Anwendungen erfüllt werden.[64] Insbesondere darf sich aus dem Hash-Wert der Originalwert nicht zurückrechnen lassen, Kollisionen müssen

63 Zu Hash-Funktionen siehe Narayanan et al. 2016 [42] S. 23-31, Schmeh 2013 [47] S. 225-264.

64 Neben den verschiedenen *SHA-2*-Funktionen (wie SHA 256) sind *SHA-3* / *Keccak* und *RIPEMD* besonders verbreitet, vgl. Schmeh 2013 [47] S. 245 bzw. 241.

sehr unwahrscheinlich und nicht deterministisch[65] erzeugbar sein, bereits kleine Änderungen der Originalnachricht müssen zu einem völlig veränderten Hash-Wert führen. Um die Sicherheit zu erhöhen, werden Hash-Funktionen häufig mehrmals hintereinander angewandt.

Hash-Werte sind nicht nur nützlich, um Signaturen zu vereinfachen, sondern dienen auch sonst häufig zur Identifikation und Verifikation, wenn die sensiblen Daten selbst nicht gespeichert werden sollen oder zu groß wären. Zum Beispiel ist die Standard-Bitcoinadresse ein Hash des dazugehörigen öffentlichen Schlüssels ***pk***. Auf diese Weise wird bei einer Transaktion der ***pk*** des Empfängers nicht veröffentlicht (wohl aber der des Senders). Es gibt zahlreiche weitere Anwendungen, die hier unerwähnt bleiben müssen.

3.2 Funktionsweise am Beispiel Bitcoin

Von allen Kryptowährungen hat *Bitcoin* bisher die weiteste Verbreitung erfahren. Bitcoin ist auch die erste moderne Kryptowährung, und viele neue Kryptowährungen unterscheiden sich nur in Marginalien.[66] Darüber hinaus ist anzunehmen, dass Terrorismusfinanzierung, wenn überhaupt mittels Kryptowährungen, dann zunächst über Bitcoin stattfinden wird. Das erklärt sich aus deren weiter Verbreitung und Verfügbarkeit, der vergleichsweise hohen Akzeptanz, dem relativ stabilen Wechselkurs und der Existenz leicht zu bedienender Software für viele Geräte. Bitcoin weist bekannte Mängel bezüglich Anonymität auf, doch es ist wahrscheinlicher, dass zunächst die vorhandenen Behelfe genutzt werden, ehe auf eine weitgehend anders aufgebaute Währung zurückgegriffen wird. Dennoch sollen im nächsten Unterpunkt 3.3 einige Währungen mit anderen Sicherheitskonzepten nicht unerwähnt bleiben.

Um Bitcoin nutzen zu können,[67] werden zunächst zwei Dinge benötigt: Eine Software und die eigentlichen *Coins*. Um an Coins zu gelangen, benötigt man eine Bitcoinadresse und einen anderen Nutzer, der vorhandene Coins darauf überweist, zum Beispiel im Tausch gegen Euro. In aller Regel übernehmen kommerzielle Dienste diese Funktion. Die Coins selbst sind nicht als Datensatz (Seriennummer oder dergleichen) vorhanden, sondern ergeben sich einzig aus der Kette der Überweisungen, wie im Folgenden beschrieben.

65 Streng ausgelegt heißt das, es darf keine Methode existieren, die im Durchschnitt schneller zu einer Kollision führt als das reine Austesten.
66 Zu typischen Unterschieden vgl. Antonopoulos 2015 [6] S. 221.
67 Eine erste allgemeine Einführung bietet Antonopoulos 2015 [6] S. 15-29.

Es gibt unterschiedliche **Bitcoin-Software**, die sich um die Generierung und Verwaltung der Schlüssel und Adressen, das Verbinden mit dem P2P-Netzwerk, das Senden von Transaktionen und die Kenntnisnahme bestätigter Transaktionen kümmert. Tatsächlich ist das alles, was eine Bitcoin-Software für den durchschnittlichen Nutzer können muss.

Eine Bitcoin-Software generiert zunächst einen oder mehrere private Schlüssel, die in einer Datei gespeichert werden. Um dies möglichst sicher zu gestalten, gibt es diverse Ansätze wie die Nutzung von Verschlüsselung oder spezielle Hardware. Die Schlüsseldatei wird ***Wallet*** genannt, ein Begriff, der oft auch für die gesamte Software verwendet wird. Ein weiterer oft für die Software verwendeter Begriff ist *Bitcoin-Client*, der hier aber gemieden werden soll, um Konfusionen mit dem Begriff Client im Kontext des P2P-Netzwerkes nicht entstehen zu lassen. Die von der Wallet-Software generierten Schlüssel sind hohe Zufallszahlen.[68] Von den privaten Schlüsseln wird je ein öffentlicher Schlüssel abgeleitet. Aus diesem wird ein Hash gebildet, der mit einem Präfix versehen und zur besseren Lesbarkeit in einem bestimmten Format (*base58checksum*) kodiert wird. Auf diese Weise entstehen die typischen **Bitcoinadressen**.[69]

Wenn ein Nutzer nun eine seiner Adressen einem Tauschdienst mitgeteilt und Geld an den Tauschdienst überwiesen hat, sollte die Software nach einer gewissen Zeit eine eingehende Transaktion feststellen. Dies geschieht über eine Suche in der zentralen Datenbank aller Transaktionen, der **Blockchain**.[70] Zentral ist irreführend: genau genommen verbindet die Software sich einfach mit einigen zufälligen Peers und synchronisiert von diesen die Blockchain. Ausgehend von den **Minern**,[71] die die Blockchain berechnen, verteilt sich so die Blockchain auf viele Geräte, von denen sie immer weiter abgefragt werden kann. Eine Bitcoin-Software, die auf diese Weise immer die gesamte Blockchain synchronisiert, wird *Full Node* genannt. Geräte mit weniger Speicherplatz oder Bandbreite sind stattdessen meist mit einem *Simple Payment Verification Client (SPV-Client)* ausgestattet. Diese Bitcoin-Software fragt nur die für ihre Wallet relevanten Transaktionen bei ihren Peers nach.[72]

68 Eine Ausnahme stellen Hierarchical Deterministic Wallets (HD-Wallets) dar, siehe hierzu Kapitel 5.3.
69 Vgl. Antonopoulos 2015 [6] S. 68-76.
70 Zur Blockchain siehe Antonopoulos 2015 [6] S. 161ff. sowie die Angriffe in Kapitel 5.1 und die dortigen Hinweise.
71 Zum *Mining*, das hier nicht weiter thematisiert wird, siehe Antonopoulos 2015 [6] S. 175-212.
72 Zu SPV-Clients siehe Kapitel 5.2 S. 42ff. und die dortigen Hinweise.

Hat die Wallet-Software eine **Transaktion**[73] auf eine eigene Adresse gefunden, kann dieser Input weiter verwendet werden, um beispielsweise bei einem Online-Händler einzukaufen. Hierzu muss die Software eine Transaktion auf eine Adresse des Händlers generieren und diese an ihre verbundenen Peers senden. Diese prüfen auf Korrektheit und verbreiten sie weiter, bis sie schließlich von den Minern in die Blockchain aufgenommen wird. Eine Transaktion enthält einige Metadaten, eine Reihe von ***Inputs***[74] und eine Reihe von *Outputs*. Ein zulässiger Input ist jeder noch nicht ausgegebene Output einer korrekten Transaktion, ein sogenannter ***unspent transaction output*** **(*UTXO*)**, sprich: eine Reihe von Coins auf einer Adresse. Um diesen UTXO weiter verwenden zu können, muss der Nutzer beweisen, dass er über ihn verfügen darf. Hierzu muss er zunächst den öffentlichen Schlüssel ***pk*** zur Adresse des UTXO bekanntgeben, damit dessen Hash auf Übereinstimmung geprüft werden kann. Außerdem muss er mithilfe des ***sk*** eine Berechnung ausführen, die anhand des ***pk*** überprüft werden kann. Auf Protokollebene betrachtet muss er ein ***unlocking script***[75] schreiben, das zu dem zuvor generierten ***locking script*** des zu verwendenden UTXO passt. In aller Regel enthält das locking script den Hash eines ***pk*** und das unlocking script wie beschrieben den ***pk*** und seine mit ***sk*** erstellte Berechnung.[76] Es können aber auch andere locking scripts generiert werden, die sich entsprechend anders entsperren lassen. Die gängige Bitcoin-Software unterstützt nur den Standardfall, und lediglich Nutzer mit entsprechendem Spezialwissen werden auf andere Scripts zurückgreifen. Allerdings gibt es ein Verfahren, das jedem Nutzer die Verwendung eines fortgeschrittenen Scripts ermöglicht: Die Transaktion auf eine Bitcoinadresse, die nicht wie im Normalfall mit dem Präfix 1, sondern mit 3 beginnt. Hierbei handelt es sich um den Hash eines locking scripts.[77] Der Sender selbst weiß nichts über die Einzelheiten dieses Scripts, er kann lediglich am Präfix 3 des Hashs erkennen, dass es sich nicht um eine Standardüberweisung handelt. Der Eigentümer dieser Adresse muss bei Weiterverwendung der Bitcoins zunächst das passende locking script zur Überprüfung des Hashs vorweisen. Danach muss er das dazu passende unlocking script ausführen. Dies könnte zum Beispiel eine Reihe verschiedener Signaturen sein. Auch für die Nutzung solch fortgeschrittener

73 Zu Transaktionen vgl. Antonopoulos 2015 [6] S. 111ff.
74 Siehe ebd. S. 117-120.
75 Zu *scripts* in Bitcoin siehe Antonopoulos 2015 [6] S. 123-138, Narayanan et al. 2016 [42] 79-88.
76 Hierbei handelt es sich um eine ECDSA-Signatur, vgl. Narayanan et al. 2016 [42] S. 40.
77 Siehe Antonopoulos 2015 [6] S. 134-137 zur allgemeinen Funktionsweise, 136 zur Entstehung des Präfixes.

Scripts gibt es Grenzen, da sie bei der Verifikation von vielen Bitcoin nodes ausgeführt werden müssen, diese jedoch in aller Regel nur eine Reihe von standardisierten Scripts akzeptieren. In der Zukunft könnten natürlich neue Standards etabliert werden.

Der **Output**[78] einer Transaktion besteht aus einer Reihe von Coins und einem locking script, das beschreibt, was zu tun ist, um diese Coins weiter benutzen zu können. Außerdem enthält eine Transaktion in den allermeisten Fällen eine geringe Transaktionsgebühr, die sogenannte ***transaction fee***.[79] Diese wird nicht explizit angegeben, sondern berechnet sich aus der Differenz zwischen Inputs und Outputs. Es handelt sich um eine Abgabe an die Miner, um das zügige Verarbeiten der Transaktion attraktiver zu machen.

Eine Transaktion kann mehrere Inputs haben. Müssen nämlich viele Coins überwiesen werden, werden oft mehrere UTXOs, jeweils mit eigenem unlocking script benötigt. Auf welcher der eigenen Adressen diese UTXOs liegen, ist dafür nicht relevant. Die Zusammensetzung wird von der installierten Bitcoin-Software automatisiert vorgenommen. Die UTXOs müssen jeweils komplett in eine Transaktion einfließen. Daher ist es wahrscheinlich, dass „Rückgeld“ benötigt wird, hierzu wird einfach ein zweiter Output auf eine eigene Adresse, die sogenannte ***change address***,[80] generiert. Die Software macht dies automatisch, oft unter Generierung einer völlig neuen Adresse. Eine gültige Transaktion kann aber auch an *mehrere fremde* Adressen gehen. Aufgrund der transaction fee kann es durchaus sinnvoll sein, mehrere Zahlungen in einer Transaktion an viele Adressen zusammenzufassen. Allerdings sehen die weit verbreiteten Softwareanwendungen diesen Fall nicht vor, sodass fortgeschrittene Kenntnisse oder Implementierungen zur Generierung erforderlich sind.

Neue Coins werden beim Prozess des Minings generiert, der eine hohe Rechenleistung erfordert. Um auf einfacherem Wege Coins zu erhalten, kann ein Nutzer diese gegen andere Werte tauschen. Am weitesten verbreitet sind hier spezialisierte Anbieter, die gegen Überweisung von Fiat-Währungen[81] Coins an eine Adresse des Nutzers überweisen. Die akzeptierten Zahlungsmethoden sind unterschiedlich und reichen bis hin zur anonymen *Paysafecard*. In vielen Fällen ist jedoch eine Verifikation der Identität, das

78 Siehe ebd. S. 115-117.
79 Siehe ebd. S. 120-122.
80 Vgl. Narayanan et al. 2016 [42] S. 77.
81 Herkömmliche Währungen. Die Bezeichnung „Fiat“ dient der Abgrenzung zu durch Gold ö.Ä. gedeckten Währungen, vgl. Narayanan et al. 2016 [42] S. 194.

Anlegen eines Accounts und die Verwendung einer regulären Bankverbindung vonnöten. Diese spezialisierten Tauschdienste können ebenso wieder zum Absatz der Coins verwendet werden. Alternativ können mittels Bitcoin Waren eingekauft oder Dienstleistungen bezahlt werden, viele online-Dienste akzeptieren die Währung.

Einige Tauschdienste bieten auch an, für den Nutzer eine ***Online-Wallet***[82] zur Verwaltung der Coins anzulegen. Auf diese Weise wird die Installation von Software vermieden, darüber hinaus existieren weitere Vor- und Nachteile. Eine Online-Wallet ähnelt einem herkömmlichen Bankkonto. Tätigt der Nutzer eine Überweisung, werden die Coins einem anderen Nutzer gutgeschrieben. Eine Transaktion in der Blockchain braucht nur dann erzeugt zu werden, wenn der Empfänger gar keinen oder einen andere Online-Wallet-Anbieter hat. In diesem Fall nutzt der Online-Wallet-Anbieter des Senders eine beliebige Auswahl seiner UTXOs. Eine für den Nutzer der Online-Wallet spezifische Adresse braucht nicht erzeugt zu werden.

3.3 Weitere Kryptowährungen

Es existieren eine ganze Reihe weiterer Kryptowährungen, die praktisch aber bislang relativ wenig Bedeutung erfahren haben. Derzeit haben alle diese anderen Währungen zusammen eine deutlich geringere Kapitalisierung als Bitcoin.[83] Das macht sie anfälliger für verschiedene Angriffe, beeinträchtigt ihre Akzeptanz und leistet Kursschwankungen Vorschub. Dennoch könnten aufgrund von Schwächen bei Bitcoin in der Zukunft eine andere Währungen Bedeutung erlangen. Derzeit führt beispielsweise die große Datenmenge zu Zeitverzögerungen bei Bitcoin-Transaktionen. Auch Sicherheitsbedenken könnten zur Favorisierung einer anderen Kryptowährung führen. Eine Auswahl alternativer Währungen wird im Folgenden vorgestellt.

Litecoin[84] unterscheidet sich hauptsächlich in seiner „Geldpolitik“ von Bitcoin, das heißt, es verwendet andere Parameter zur Generierung neuer Coins. Zum Mining nutzt es einen anderen Hash-Algorithmus.[85] Litecoin hat eine vergleichsweise hohe Kapitalisierung.[86]

Namecoin[87] hat nicht die Funktion einer Währung, sondern erlaubt die Ablage

82 Zu Online-Wallets siehe ebd. S. 112ff.
83 Vgl. Narayanan et al. 2016 [42] S. 273.
84 Siehe Narayanan et al. 2016 [42] S. 271.
85 Nämlich *Scrypt*, siehe ebd. S. 219ff.
86 Litecoin hat die zweithöchste Popularität: vgl. ebd. S. 219.
87 Vgl. ebd. S. 270f.; vgl. auch Antonopoulos 2015 [6] S. 228ff.

von Daten in seiner Blockchain. Auf diese Weise wird ein alternatives DNS (eine Art Telefonbuch des Internets) für die Toplevel-Domain .bit generiert, welches nicht zentral gesteuert ist.

Darkcoin[88] hat den Anspruch, erhöhte Anonymität zu gewährleisten, indem zunächst ein Mischen der Inputs verschiedener Sender geschieht. Aus den letztlich in der Blockchain veröffentlichten Transaktionen sollen sich Sender, Empfänger und Betrag nicht mehr nachvollziehen lassen. Darkcoin ähnelt insofern den sogenannten Mixing Services, die in den Kapiteln 4.1 und 5.1 angesprochen werden.

Zerocoin[89] und besonders seine Weiterentwicklung ***Zerocash***[90] bauen auf modernsten Entwicklungen der Kryptographie auf, indem sie *zero-knowledge-proofs* benutzen. Zerocash setzt erstmals auf sogenannte *zk-SNARKs (zero-knowledge Succint Non-interactive ARguments of Knowledge)*[91], die eine performante Implementierung ermöglichen könnten. Die mathematischen Grundlagen von Zerocash sind äußerst komplex und können hier nicht erläutert werden. Der zero-knowledge-proof in Zerocash erfüllt die Funktion der Signatur, indem er beweist, dass der Sender über die gesendeten Coins verfügungsberechtigt ist. Dies kann durch die Peers auch (nahezu) zweifelsfrei überprüft werden. Für die Überprüfung werden aber weder die Adressen der Transaktion, noch die Höhe der transferierten Coins benötigt.[92]

Das Konzept eines zero-knowledge-proof lässt sich nur schwer begreiflich machen. Ein vereinfachendes Beispiel ist das eines Geologen, der eine nicht offensichtliche Regelmäßigkeit zwischen bestimmten seismographischen Messungen und später auftretenden Erdbeben festgestellt hat. Weil eine Kommission ein Preisgeld für den Beweis einer derartigen Regelmäßigkeit ausgesetzt hat, behauptet er nun öffentlich, eine solche festgestellt zu haben. Er will diese aber nicht offenlegen (er ist vielleicht Misanthrop), schließlich sei in der Ausschreibung nur von einem *Beweis* die Rede gewesen, nicht von einer *Offenlegung* der Forschung. Er bietet stattdessen an, zum Beweis seines Wissens eine Reihe von Beben vorherzusagen. Diese Vorhersage glückt, ohne dass dadurch jemand anders auf die Quelle seines Wissens stoßen kann.

88 Vorgestellt in Duffield / Hagan 2014 [16]. Das zu DASH umbenannte Projekt hat einen Webauftritt unter https://www.dash.org/ (Stand 07.05.2016).
89 Vorgestellt in Miers et al. 2013 [37].
90 Vorgestellt in Ben-Sasson et al. 2014 [8].
91 Vgl. ebd. S. 1.
92 Zu Zerocoin, Zerocash und den zugrunde liegenden Konzepten siehe auch Narayanan et al. 2016 [42] S. 185-193.

Im Detail sind zero-knowledge-proofs komplizierter. Es lässt sich aber festhalten, dass es in der Mathematik Konzepte gibt, die einen (nahezu) sicheren Beweis für die Integrität einer Aussage ermöglichen, ohne die Aussage selbst zu offenbaren. Diese Konzepte könnten damit tatsächlich eine neue, stark anonyme Kryptowährung ermöglichen. Allerdings besteht bei der Implementierung derzeit das grundsätzliche Problem, dass einige zentrale Parameter zunächst geheim festgelegt werden müssen. Kenntnis dieser Parameter würde die unautorisierte Nutzung der Coins ermöglichen.[93] Dieses Problem scheint mathematisch zur Zeit nicht lösbar zu sein, sodass jeder Implementierung ein gewisses Misstrauen der Nutzer entgegenstehen muss. Aktuell ist Zerocash nicht implementiert.

4 Terrorismusfinanzierung mittels Kryptowährungen

Am 11.06.2015 wurde Ali Shukri Amin, ein 17-Jähriger Bürger des US-Staates Virginia, zu gut 11 Jahren Haft verurteilt, weil er einerseits einem Bekannten bei dessen Hidschra ins Kalifat behilflich gewesen war, und weil er andererseits selbst über den Twitteraccount *@Amreekiwitness* und über Veröffentlichungen in einem Blog zur Unterstützung von ISIS aufgerufen hatte.[94] Insbesondere hatte er unter dem Titel „Remaining Anonymous Online“ in englischer Sprache eine Sammlung von Ratschlägen veröffentlicht, die sich an ISIS-Sympathisanten richtete und den sicheren Umgang mit Kommunikationstechnologie zum Inhalt hatte. Darin wurden einige gängige Techniken zur Anonymisierung der IP-Adresse, wie die Nutzung von *tails, Tor,* und *GhostVPN* empfohlen und erklärt.[95] Ein weiterer Blogeintrag unter dem Pseudonym „Taqi'ul-Deen al Munthir“ stammt ebenfalls von ihm. Der arabische Titel dieses ansonsten englischsprachigen Eintrags lautet „Bitcoin wa’ Sadaqat al-Jihad“ zu deutsch etwa „Bitcoin und die Spende für den Dschihad“.[96] Darin beklagt er die mangelnden Möglichkeiten zur finanziellen Unterstützung von ISIS und schlägt als Alternative die Nutzung von Bitcoins für Überweisungen aus aller Welt in das Kalifat vor. Konkret empfiehlt er die

93 Vgl. ebd. S. 189f.
94 Siehe Department of Justice 2015 [15] (Pressemeldung) und United States District Court 2015 [51] (Geständnis). Der Fall hat (mit anderem Datum) auch Eingang in FATF 2015 (b) [19] gefunden: S. 36.
95 Siehe Amin 2014 (a) [4] für diesen Blogeintrag.
96 Siehe Amin 2014 (b) [5] für diesen Blogeintrag.

Nutzung von *Dark Wallet*, einer Bitcoin-Software, die Anonymität verspricht, jedoch bislang nicht über das Alpha-Stadium hinausgekommen ist.[97]

Ansonsten bleibt der Autor sehr unspezifisch. Ein Verweis auf die damals bereits geschlossene Plattform *Silk Road*[98] legt nahe, die gespendeten Bitcoins könnten zum Kauf von Waffen über den Online-Schwarzmarkt eingesetzt werden.

Im folgenden Kapitel 4.1 soll das mögliche Szenario einer Verwendung von Kryptowährungen zum Empfang von Spenden untersucht werden. Kapitel 4.2 behandelt als weiteres Szenario den Transfer mittels Off-Chain-Transaktionen. In Kapitel 4.3 werden Möglichkeiten zur Verwertung von Kryptowährungen betrachtet.

4.1 Szenario: Spenden an terroristische Adressen

Transaktionen von Kryptowährungen haben den Vorteil, dass sie nicht einfach von einer Kontrollbehörde unterbunden werden können. Wie jede andere Partei müsste eine solche Behörde den betreffenden ***sk*** kennen, um ein unlocking script für die Coins zu generieren. Es scheint daher, als könnte eine terroristische Gruppe ganz einfach eine Empfangsadresse öffentlich bekannt machen und auf das Eintreffen von Geldern zu warten.

Ein solch einfacher Ansatz hätte eine Reihe von Schwächen. Zunächst einmal müsste für die Veröffentlichung ein Kanal gewählt werden, der nicht einfach kompromittiert werden kann. Einträge bei *twitter*, *justpaste.it*, *archive.org* oder ähnlichen Plattformen können jedoch leicht gefälscht werden. Da sich eine Bitcoinadresse überdies schwer merken lässt, wäre die Fälschung auch wenig offensichtlich. Al Qaida (bzw. AQAP) hat in Inspire einen ***pk*** bekannt gegeben, der zur Kommunikation mit der Redaktion genutzt werden soll.[99] Genauso könnten dschihadistische Gruppen auch Signaturen zur Fälschungssicherheit einsetzen. Dazu liegen dem Autoren jedoch keine Anhaltspunkte vor. Überdies steht zu bezweifeln, dass alle Adressaten eine solche Signatur erkennen oder nachprüfen könnten.

97 Siehe Internetpräsenz von Dark Wallet unter https://www.darkwallet.is/ (Stand 07.05.2016).
98 Vgl. Amin 2014 (b) [5] S. 2. Zu Silk Road im Zusammenhang. mit Bitcoin siehe Narayanan et al. 2016 [42] S. 205ff.
99 Siehe beispielsweise *Inspire* 1 (2010) [1] S. 65.

Ein weiteres Problem wäre die einfache Nachvollziehbarkeit in der Blockchain.[100] Dies würde die Identifikation der Akteure erleichtern und es sehr schwer machen, die Bitcoins unbemerkt zu verwerten. Auch viele andere Attacken würden bei Kenntnis einer öffentlichen Adresse erleichtert werden.

Sinnvoller erscheint die doppelte oder dreifache Verwendung sogenannter *Mixing Services*: Zu Einen seitens des Senders, um seine von einem Tauschdienst auf einer nicht anonymen Wallet erhaltenen Coins auf eine andere anonyme, ihm gehörende Wallet zu übertragen, und einmal seitens des Empfängers, um die mit der öffentlichen Adresse in Verbindung stehenden Coins an unbekannte eigene Adressen für die spätere Nutzbarmachung zu übertragen. Auch die eigentliche Transaktion könnte über einen Mixing Service erfolgen. Eine Verwendung mehrerer Mixing Services in Kombination könnte die Sicherheit weiter erhöhen. Mixing Services sind kurz gesagt Dienste, die viele Transaktionswünsche sammeln und dann aus den Wünschen Transaktionen generieren, die möglichst keine zutreffenden Rückschlüsse auf die Transaktionswünsche zulassen. Es gibt mehrere Möglichkeiten, dies technisch zu realisieren, teils über zentrale Webanwendungen, teils über speziell angepasste Bitcoin-Software. Für alle Mixing Services ist es jedoch ungünstig, wenn nur *eine* Empfangsadresse angegeben werden kann. Daher ist die Verwendung für die eigentliche Transaktion nicht sehr sinnvoll.[101]

Eine weitere Möglichkeit wäre das Verbreiten der Empfangsadresse auf nicht öffentlichem Wege, beispielsweise erst auf Anfrage über verschlüsselte Messenger. In diesem Fall könnte für jede Anfrage eine neue Adresse verwendet werden. Wenn eine Behörde eine solche Adresse abfängt, kann sie davon nicht so einfach auf weitere Empfangsadressen oder andere Sender schließen. Wie in Kapitel 5.1 gezeigt wird, ist eine Zuordnung weiterer Verbindungen über eine intelligente Analyse der Blockchain jedoch durchaus möglich. Hier liegt einer der Punkte, die gegen die Verwendung von Kryptowährungen zur Finanzierung des Dschihadismus sprechen: Ein einzelner unvorsichtiger Nutzer könnte wesentlich zur Entanonymisierung anderer Nutzer beitragen, indem er z.B. auf Mixing Services verzichtet, eine einzelne Senderadresse für Transaktionen an verschiedene Empfangsadressen nutzt, oder eine Empfangsadresse an seine

100 Siehe Kapitel 5.1.

101 Zu Mixing Services im Allgemeinen siehe Narayanan et al. 2016 [42] S. 177-185. Ein aktuelles Konzept für fortgeschrittene Mixing Services stellen Heilman et al. 2016 [22] vor. Zu Maßnahmen gegen Mixing Services siehe auch Kapitel 5.1 und die dortigen Hinweise.

Gesinnungsgenossen weitergibt, obwohl diese nur für die einmalige Verwendung gedacht war.[102] Es scheint daher aus Sicht des terroristischen Empfängers vernünftiger, die Verwaltung der Transaktionen selbst zu übernehmen.

4.2 Szenario: Off-Chain-Transaktionen

Um dies umzusetzen, könnte der Empfänger den Sender beispielsweise eine vorgefertigte Transaktion signieren lassen. Er könnte sich auch auf beliebigem Wege den Text einer Transaktion schicken lassen, deren Signatur lediglich die UTXOs entsperrt, aber beliebige Outputs erlaubt. Diese Transaktion könnte er dann nach seinem Bedarf vervollständigen. Er könnte sich aber auch ganz einfach den ***sk*** einer Adresse übermitteln lassen. Solche Möglichkeiten bezeichnet man als *Off-Chain-Transaktionen*[103], da eine Übermittlung de facto (schon) stattfindet, obwohl (noch) keine in der Blockchain sichtbare Transaktion erzeugt wird.

Im einfachsten dieser Fälle muss ein ***sk*** ausgelesen oder die entsprechende Wallet-Datei kopiert werden, was je nach verwendeter Wallet unterschiedlich aufwändig ist. Unter Umständen sind Verschlüsselungen aufzuheben. Entsprechende Anleitungen könnten aber leicht verbreitet werden. Die manuelle Erzeugung ganzer Transaktionen zum Off-Chain-Versand erfordert jedoch fortgeschrittene Kenntnisse. Bisherige Off-Chain-Lösungen basieren auf einer *trusted third party*, die eine entsprechende Anwendung (z.B. webbasiert im Rahmen einer Online-Wallet) zur Verfügung stellt. Da aber gerade keine dritte Partei Einfluss nehmen können soll, sind solche Lösungen nicht gut nutzbar. Außerdem wäre ein Betrug seitens der trusted third party erheblich.[104]

Off-Chain-Transaktionen erschweren eine Entdeckung auf Basis der Blockchain oder auf Basis von P2P-Netzwerkangriffen erheblich. Um solche Transaktionen zu entdecken, bleibt die gezielte Überwachung verdächtiger Sympathisanten auf der Senderseite, sowie die Suche nach verdächtigem Einsatz von Bitcoins auf der Empfängerseite.

---

102 Vgl. Brantly 2014 [11] S. 4.

103 In den benutzten Einführungen taucht dieser Begriff nicht auf. Die Bezeichnung ist übernommen aus der weit verbreiteten Bitcoin-Dokumentaion *Bitcoin Wiki:* https://en.bitcoin.it/wiki/Off-Chain_Transactions (Stand 07.05.2016), ähnliche Bezeichnung auch im Titel von Heilman et al. 2016 [22].

104 Vgl. den Abschnitt über Online-Wallets in Narayanan et al. 2016 [42] S. 112ff.

4.3 Verwertung von Kryptowährungen

Bisher wurde davon ausgegangen, dass der Sender der zu spendenden Kryptowährung diese Coins auf einem beliebigen Wege erhalten hat. Da diese Wege für die Terrorismusfinanzierung nicht spezifisch sind, spielen sie in diesem Kapitel keine Rolle.

Anders sieht es mit der Verwertung seitens des Empfängers aus. Zum Einen besteht ein Bedarf an bestimmten nicht gegenständlichen Werten wie Infrastruktur, Protektion, Fachwissen, Dienstleistungen. Zum Anderen benötigen dschihadistische Gruppen ganz gewöhnliche Versorgungsmittel. Hinzu kommen spezielle Gegenstände der Ausrüstung und diverser militärischer Bedarf. ISIS muss darüber hinaus ein Staatswesen aufrecht erhalten.

Selbst Bitcoin als die verbreitetste Kryptowährung lässt sich jedoch nur eingeschränkt zur Bezahlung von Waren und Dienstleistungen einsetzen. Verbreitet ist Bitcoin bei der Bezahlung mancher Dienstleistungen, besonders in westlichen Staaten, überdies in manchen Internetshops und im Online-Schwarzmarkt[105]. Es ist denkbar, dass Bitcoin geeignet ist, um bei Händlern der organisierten Kriminalität militärische und andere Ausrüstung einzukaufen. Für den Bedarf des täglichen Lebens, die Versorgung der Kämpfer und die Aufrechterhaltung eines Staatswesens müsste jedoch ein Tausch in harte Werte oder in stabile Fiat-Währungen erfolgen. Ein solcher Tausch benötigt einen Partner, der gegen den Erhalt der Bitcoins eine Transaktion der benötigten Werte in die Wege leitet. Infrage kommen hier ganz herkömmliche Tauschdienste, die dann auf eine unauffällige Bankverbindung überweisen. Unter Einbeziehung von Money Service Businesses (sofern diese Bitcoins annehmen), sind kompliziertere Szenarien denkbar, die den Weg des Geldes verschleiern. Schließlich wäre es auch möglich, dass ein Hawaladar oder eine andere Person oder Gruppierung mit entsprechenden Wertbeständen Bitcoins annimmt.

Neu aufkommende Konzepte des Fundraising bzw. Crowdfunding zu terroristischen Zwecken[106] könnten auch Bitcoin-Transaktionen mit einbeziehen. Einzelne Sympathisanten mit speziellen Kenntnissen könnten verschiedene kleinere Geldquellen zunächst bündeln. Diese könnten aus gewöhnlichen Bitcoin-Transaktionen oder Off-Chain-Transaktionen bestehen,

105 Vgl. Narayanan et al. 2016 [42] S. 205ff.

106 Eine Methode, die bislang unbedeutend scheint, jedoch mit Sorge betrachtet wird: vgl. FATF 2015 (a) [18] S. 24f., FATF 2015 (b) [19] S. 30ff., Normark / Ranstorp 2015 [45] S. 20ff.

aber auch aus der Übermittlung von Gutscheincodes (Prepaid-Karten) oder Kreditkarten-PINs, möglicherweise auch aus herkömmlichen Überweisungen. Solch kleine Beträge fallen in der Regel nicht auf. Die gesammelten Beträge könnten in einem zweiten Schritt gebündelt und transferiert werden, wobei die Kombination verschiedener Transfertechniken zur Verschleierung eingesetzt werden könnte. Zum schnellen und wiederholten Transfer solch hoher Beträge zwecks Verschleierung scheint Bitcoin gut geeignet. Die derart „gewaschenen“ Spenden könnten letztlich in Beträgen mittlerer Höhe über Hawala in das Zielland transferiert werden.

Sollten Kryptowährungen dergestalt in Kombination mit anderen Techniken eingesetzt werden, könnten Sanktionen gegen herkömmliche Finanzinstrumente umgekehrt auch die Verwertung von Kryptowährungen erschweren.

5 Identifikation der Akteure und Gegenmaßnahmen

Ausgehend von den beschriebenen Szenarien sollen nun einige Ansätze behandelt werden, mit deren Hilfe Ermittlungsbehörden Handlungen entdecken, unterbinden oder aufklären können. Diese können teils sehr generell angewandt werden, nutzen teils aber auch sehr spezifische Schwächen aus. Es ist wahrscheinlich, dass sich durch neu aufkommende Kryptowährungen, durch Änderungen einzelner Protokolle bzw. einzelner Implementierungen oder auch nur durch verändertes Nutzerverhalten, einige Strategien als nicht mehr gängig oder überarbeitungsbedürftig erweisen. Daher sollten neue Erscheinungen, aber auch schon kleine Veränderungen sorgfältig beobachtet werden.

Von den möglichen Strategien kann hier nur eine kleine Auswahl näher beschrieben werden. Letztlich wird eine Kombination vieler Ansätze den größten Erfolg versprechen. Die Entwicklung einer solch umfassenden Strategie steht noch aus.

In Punkt 5.1 wird zunächst an einer systemspezifischen Eigenheit angesetzt, der Öffentlichkeit der Blockchain.

In Punkt 5.2 werden zwei Angriffe auf Basis der Kommunikation im P2P-Netzwerk beschrieben. Die Verwendung einer P2P-Infrastruktur ist für Kryptowährungen zwar nicht spezifisch, aber immanent.

Es folgen in Punkt 5.3 übersichtsartig einige Angriffe, die ebenfalls an einem Punkt ansetzen, der nicht spezifisch, aber immanent ist: die Verwendung von Kryptographie.

In Punkt 5.4 wird ein Blick auf weitere Ansätze geworfen, die oftmals nicht speziell auf Kryptowährungen zugeschnitten sind, aber auch hier in Erwägung gezogen werden sollten.

Da nur die Angriffe in den Punkten 5.1 und 5.2 ausführlicher erläutert werden, folgt eine tabellarische Aufstellung von Ermittlungsansätzen nach aktuellem Stand, die als Grundlage für weitere Recherche dienen kann. Insbesondere die im Vorfeld wichtigen Ansätze zur Entdeckung verdächtiger Aktionen werden im Folgenden nicht näher erläutert, können und sollten zum Teil aber auch vom nicht weiter spezialisierten Sachbearbeiter in Angriff genommen werden.

Die nachstehende (zweiseitige) Tabelle zeigt eine Übersicht über mögliche Ermittlungsansätze, von denen die ersten drei im Folgenden näher erläutert werden. Grün hervorgehoben sind die Anhaltspunkte, deren Auftreten den einzelnen Angriff nahelegen könnte. Rot hervorgehoben sind die möglichen Erfolge.

Arbeits)name	Ausgenutzte Schwäche	Vorgehens-weise	Anhaltspunkte; Erfordernisse	Mögliche Erfolge
Blockchain-analyse	sytem-spezifische Öffentlichkeit der Blockchain	Recherche auf speziellen Webseiten / mittels Tools, *s.u.*	Verdächtige *Transaktionen*; Verfügbarkeit spezieller Tools	*Zuordnung* von Transaktionen, Personen, Firmen, Protokollen
Zuordnung Transaktion zu IP	Details der Kommunikation im P2P-Netzwerk	Aufbau vieler Verbindungen, Besetzung von responsible nodes, *s.u.*	Verdächtige *IP-Adressen*; Verfügbarkeit von Rechnern und Bandbreite	*Zuordnung* von Transaktionen, Zuordnung von Sendern zu IP-Adressen
Bloomfilter-Sammlung	Details der Kommunikation im P2P-Netzwerk, Verhalten der Implemen-tierungen	Aufbau vieler Verbindungen, Besetzung von entry nodes, *s.u.*	Verdächtige *IP-Adressen* oder *Transaktionen*; Verfügbarkeit von Rechnern und Bandbreite	*Zuordnung* von Empfangsadre ssen zu IP-Adressen
Beobachtung sozialer Medien	(teilweise) einfache Zugänglichkeit	Recherche auf Webseiten, Anlegen von Accounts	Allgemeine *Verdachts-momente*; /	*Entdeckung* verdächtiger Aktivitäten
Internet-recherche	Öffentlichkeit bestimter Bereich des Internets	Recherche auf Webseiten nach Verknüp-fungen von Bitcoinadresse und Identität	Verdächtige *Identitäten* oder *Transaktionen*; Verfügbarkeit von Recherche-tools	*Zuordnung* von Transaktionen zu Identitäten
Offline-Aufklärung / -Überwachung	/	offen / verdeckt (diverse Möglichkeiten)	Verdächtige *Identitäten*, *Vorgänge*; /	*Entdeckung* verdächtiger Aktivitäten
Online-Überwachung	Sicherheits-lücken in Software oder Netzwerk	Mitschneiden von Kommuni-kation, Auslesen von Daten	Verdächtige *Identitäten / IP-Adressen*; Verfügbarkeit spezieller Tools	*Entdeckung* verdächtiger Aktivitäten, weitere Ermittlungen
Online-Beschlag-nahme	Sicherheits-lücken in Software oder Netzwerk	Auslesen der ***sk*** und Transfer der Coins auf Behörden-wallets	Verdächtige *Identitäten / IP-Adressen*; Verfügbarkeit spezieller Tools	*Entzug* der Zugriffs-möglichkeit auf die Coins
Offline-Beschlag-nahme	Mangelnde Verschlüs-selung	Auslesen der ***sk*** und Transfer der Coins auf Behörden-wallets	Verdächtige *Identitäten*; Zugang zu laufendem oder unverschlüs-seltem System	*Entzug* der Zugriffs-möglichkeit auf die Coins

Tabelle 1(Beginn): Übersicht über mögliche Ermittlungsansätze.

Arbeits)name	Ausgenutzte Schwäche	Vorgehens-weise	Anhaltspunkte; Erfordernisse	Mögliche Erfolge
Offline-Beschlag-nahme	Mangelnde Verschlüs-selung	Auslesen der ***sk*** und Transfer der Coins auf Behörden-wallets	Verdächtige *Identitäten*; Zugang zu laufendem oder unverschlüs-seltem System	*Entzug* der Zugriffs-möglichkeit auf die Coins
Software-analyse	(teils) offener Quellcode	Untersuchung der genutzten Implemen-tierungen auf Eigenheiten und Schwach-stellen	/ ; Verfügbarkeit von Quellcode oder Dokumen-tationen, spezielle IT-Kenntnisse	*Ermöglichung* des Entwurfs von Angriffen
Infiltrierung des P2P-Netzwerkes	Struktur des P2P-Netzwerkes, fehlerhafte Implemen-tierungen	Besetzung von entry nodes (auf noch ungeklärte Weise)	Verdächtige *IP-Adressen*; spezielle IT-Kenntnisse	Diverse *Zuordnungen*, *Ermöglichung* weiterer Angriffe
Kryptoanalyse	Unzulängliche mathematische Grundlagen	Brechen der verwendeten Hashs, Signaturen, Verschlüs-selung	/ ; Exklusives Wissen über mathematische Vorgänge, enorme Rechenkapazität	*Entzug* der Zugriffs-möglichkeit auf die Coins; *Zugriff* auf Kommuni-kation
Passwort-ermittlung	Schwache Passwörter	Brute-Force-Angriffe, Wörterbuch-angriffe, Auslesen	Verdächtige *Accounts* oder *Dateien*; Nutzung verbreiteter Tools	*Zugriff* auf verschlüsselte Daten, *Zugriff* auf Accounts
Key-Recovery-Attacken	Unsichere Passwort-verwaltung	Berechnen der weiteren Schlüssel aus bekannten Schlüsseln	Verdächtige *Wallets;* Kenntnis einzelner Schlüssel	*Entzug* der Zugriffs-möglichkeit auf die Coins
Angriffe auf Server	Sicherheits-lücken in Software oder Netzwerk	Auslesen von Daten, Mitschneiden und Mani-pulation von Kommunikation	Verdächtige *Identitäten, Dienste*, Vorgänge; spezielle IT-Kenntnisse	*Zugriff* auf Accounts, Netzwerke und Mixing Services
Zusammen-arbeit mit Anbietern	/	Befragungen, Instruktionen, Ersuchen	Anhaltspunkte für Einbindung in verdächtige *Aktivitäten*; /	*Zuordnung* von Transaktionen zu Identitäten

Tabelle 1 (Fortsetzung): Übersicht über mögliche Ermittlungsansätze.

5.1 Ansatz an systemspezifischen Schwächen

Die Zugriffsmöglichkeit dritter Parteien auf Identitäten, Konten und Transaktionen bei Verwendung herkömmlicher Finanzinstrumente war einer der Punkte, die durch die Einführung von Bitcoins entschärft werden sollten.[107] Wer sich nur selbst um die Sicherheit seiner Schlüssel kümmert, darf sich – so der Wunsch - darauf verlassen können, dass niemand seine Transaktionen verändern oder unbefugte Transaktionen initiieren kann. Es gibt Angriffsszenarien, die auch das infrage stellen, die aber von einer gewaltigen Rechenleistung oder Übermacht im Netzwerk ausgehen und daher bei einer so viel genutzten Währung wie Bitcoin als nicht durchführbar gelten.[108] Die Dezentralisierung von Kryptowährungen ist eine bewusste Antwort auf zentrale Kontrolle und trägt viel zur Sicherheit, auch und gerade gegenüber staatlichen Organen bei. Sie bringt es allerdings unweigerlich mit sich, dass alle Transaktionen für alle einsehbar gespeichert werden müssen. Diese Blockchain ermöglicht umfangreiche Recherchen, die eine Offenlegung der Identitäten hinter den Transaktionen ermöglichen können.

Eine korrekte Kopie der Blockchain erhält man unter Verwendung der Bitcoin-Referenz-Wallet *Bitcoin Core*. In aller Regel wird aber auch der Abruf über die gängigen Webseiten eine korrekte Blockchain zur Verfügung stellen. Die Größe der Blockchain beträgt aktuell (Mai 2016) knapp 70 GB.[109]

Für diese Bachelorarbeit wurden zwei gängige Analyseseiten aufgerufen, *blockchain.info* und *oxt.me*. Beide erlauben Recherchen nach Adressen, öffentlichen Schlüsseln, Transaktionen und Blöcken. Beide bieten auch Visualisierungen der Transaktionen an, die beispielhaft am Ende dieses Kapitels eingefügt sind. *oxt.me* hält eine Reihe statistischer Auswertungsmöglichkeiten bereit, *blockchain.info* erlaubt Einsicht in die kompletten Rohdaten. Für die polizeiliche Arbeit wäre es allerdings sinnvoll, ein speziell programmiertes Tool zur Verfügung zu haben, das je nach Bedarf erweiterbar ist und das die Einbindung interner Datenbanken ermöglicht, in denen beispielsweise Bitcoinadressen bestimmten IP-Adressen oder Personen zugeordnet sind. Eine solche Zuordnung könnte probabilistisch anhand der Erkenntnisse aus der Blockchainanalyse oder aus anderen

107 Vgl. das Papier zur Vorstellung von Bitcoin: Nakamoto 2008 [41] S. 1, 5.

108 Insbesondere eine 51%-Attacke wäre bei Bitcoin schwerer durchführbar als bei weniger verbreiteten Währungen. Siehe zu dem Thema Antonopoulos 2015 [6] S. 213ff. und Narayanan et al. 2016 [42] S. 71f., ferner Mahlmann / Schindelhauer 2007 [34] S. 202-205.

109 Einzusehen auf https://blockchain.info/de/charts/blocks-size

Quellen erfolgen. Auch andere Möglichkeiten der Auswertung und Recherche sollten unterstützt werden. Zum Beispiel könnten anhand der Höhe der transaction fee Rückschlüsse auf die verwendete Software möglich sein. Auch könnten bestimmte Adressen bestimmten Tauschdiensten zugeordnet werden.[110] Auch Mixing Services wären möglicherweise über sorgfältige Analyse erkennbar. Aufgrund der Unübersichtlichkeit der Blockchain stößt die manuelle Recherche mittels *blockchain.info* und dergleichen hier schnell an ihre Grenzen. Ein spezialisiertes Programm und die Pflege von Datenbanken könnte die Qualität der Ermittlungen entscheidend voranbringen. *blockchain.info* hält in Form der *taint analysis* bereits eine probabilistische Zuordnung von Adressen zueinander bereit. Diese Methode könnte noch verfeinert und erweitert werden. Insbesondere ist eine Verknüpfung von Erkenntnissen aus der Blockchain mit Erkenntnissen aus anderen Angriffen und Ermittlungen wünschenswert.

Die Blockchain enthält keine Namen und keine IP-Adressen, sondern ist lediglich ein Verzeichnis der Transaktionen.[111] Zuordnungen von Adressen zur selben Wallet sind anhand verschiedener Anhaltspunkte möglich:[112]

Bei mehreren Inputs ist die Wahrscheinlichkeit sehr hoch, dass es sich um UTXOs derselben Wallet handelt, da die gängige Wallet-Software nur diesen Fall unterstützt. Ausnahmen sind unter Verwendung spezieller Protokolle möglich (sogenannte Mixing Services, siehe unten).

Existieren zwei Outputs, ist einer davon wahrscheinlich eine Change-Adresse der Wallet des Senders. Diese ist entweder eine bereits verwendete Adresse des Senders oder eine völlig neu generierte Adresse. Gerade wenn auch die Adresse des Empfängers völlig neu generiert ist, lässt sich jedoch schwer entscheiden, welches die Change-Adresse ist. Anhaltspunkt könnte die Höhe des Outputs sein. Existiert bei mehreren Inputs ein Input oder eine Summe von Inputs, die höher ist als der niedrigere Output, aber kleiner als der höhere Output, handelt es sich beim niedrigeren Output wahrscheinlich um den Change. Andernfalls würden gängige Wallet-Implementierungen nur den einen Input bzw. die entsprechende Summe verwenden. Allerdings könnten Wallets auch so programmiert werden, dass sie wahllos Inputs zusammenwürfeln. Dieses Verhalten sollte beobachtet werden.

110 Ein Beispiel für solche Zuordnungen findet sich in Narayanan et al. 2016 [42] S. 172-176, Abbildung von S. 175 aus Meiklejohn et al. 2013 [36] S. 23.

111 Auf *blockchain.info* angegebene IP-Adressen sind nicht die Urheber der Transaktion.

112 Zu den Möglichkeiten der Zuordnung vgl. Nick 2015 [44] S. 5-8, Narayanan et al. 2016 [42] S. 170-176.

Mit 3 beginnende Adressen deuten auf irgendeine Art von Spezialisierung hin, z.B. Firmen, Tauschdienste, etc. Um Coins von einer 3er-Adresse aus zu überweisen, sind spezielle Scripts erforderlich (siehe Kapitel 3.2).

Die Verwendung von mehr als zwei Outputs deutet ebenfalls auf die Verwendung einer speziellen Software (bzw. manuelle Erstellung der Transaktion hin), in diesem Fall seitens des Senders. Verbreitete Bitcoin-Software generiert ohne Change einen und mit Change zwei Outputs.

Ein einzelner Output deutet auf eine Spende oder einen Rücktausch gegen Fiat-Währungen hin. In anderen Fällen würde in aller Regel ein Change generiert werden, da UTXOs auf Inputebene nicht geteilt werden können und komplett in die Transaktion einfließen müssen.

Eine runde Höhe von Bitcoins oder immer dieselbe Höhe weisen auf Tauschdienste oder Mixing Services hin. Mixing Services könnten Standardhöhen nutzen, um Recherchen über das Transaktionsvolumen zu erschweren.[113] Mindestens ein Tauschdienst nutzt Sammeladressen, füllt diese auf bestimmte Höhen auf und generiert dann mehrere Outputs.[114]

Weitere Regelmäßigkeiten sind denkbar und es wäre lohnenswert, hier weiter zu recherchieren. Insbesondere die Identifikation der einzelnen Tauschdienste wäre wünschenswert.

Immer wieder ist nun schon der Begriff des Mixing Service aufgetaucht. Mixing Services sind, solange erweiterte Lösungen wie Zerocash nicht implementiert sind, gängige Verfahren zur Verschleierung von Geldflüssen und stellen ein großes Hindernis bei Analysen der Blockchain dar. Mixing Services sind auch deswegen ein wichtiges Thema, weil in vielen Fällen ihre Nutzung keine besonderen Ansprüche an die Teilnehmer stellt (sie müssen lediglich eine Reihe gewöhnlicher Adressen und Transaktionen generieren). Zu einer genaueren Untersuchung der verschiedenen Mixing Services wäre eine gezielte Forschung notwendig, die auch eine größere Anzahl von Testüberweisungen beinhalten würde. Eine solche Forschung würde in diesem Rahmen zu weit führen, wäre aber ein lohnendes und drängendes Projekt im Rahmen einer Bachelor- oder vielleicht Masterarbeit.[115]

113 In Narayanan et al. 2016 [42] S. 181 wird allerdings festgestellt, dass aktuelle Mixing Services sich nicht so verhalten. Das würde wiederum die Analyse nach Höhe des Transaktionsvolumens erleichtern.

114 So festgestellt bei der Rückverfolgung der Coins des Autoren. Für eine Generalisierung müsste weiter recherchiert werden.

115 Eine Untersuchung zu dem Thema liegt vor: Möser et al. 2013 [38]. Eine Einführung bieten Narayanan et al. 2016 [42] S. 177-185.

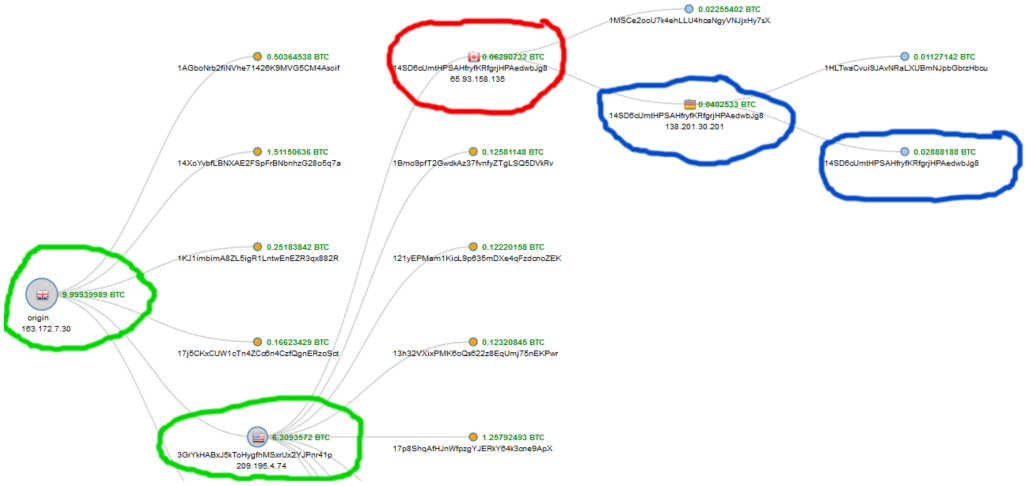

***Abbildung 2: (Screenshot)**:* Beispiel der Visualisierung auf *blockchain.info*: Rot markiert die Empfangsadresse des Autors mit der Wallet *Multibit Classic* unter Nutzung des Tauschdienstes *bit4coin*. Diese Adresse taucht (blau markiert) zweimal als change-Adresse auf. Bei den anderen Outputs handelt es sich um andere Wallets des Autoren. Grün markiert sind Adressen des Tauschdiensts. Diese beginnen mit dem Präfix 3 und haben mehrere fremde Outputs. Weitere Recherchen offenbaren außerdem Regelmäßigkeit im Gesamtvolumen ihrer Transaktionen. Die IP-Adressen zeigen, über welchen Server die Transaktion an *blockchain.info* geleitet wurde. Ein besser lesbarer Originalscreenshot findet sich samt Datum im digitalen Anhang.

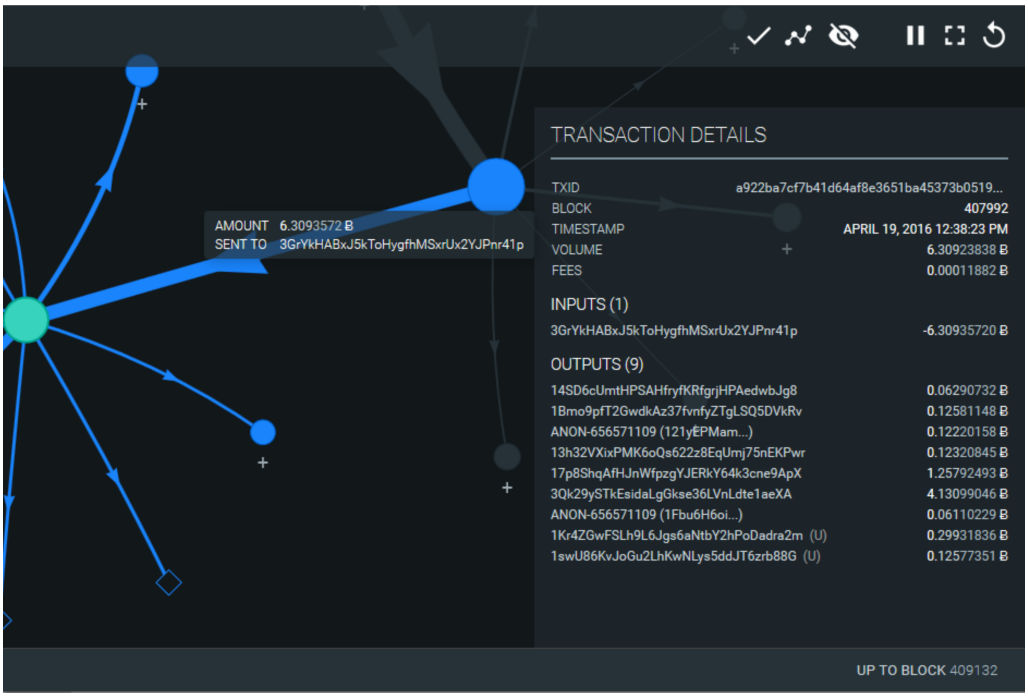

***Abbildung 2 (Screenshot)**:* Beispiel der Visualisierung auf *oxt.me*. Original- und ein weiterer Screenshot befinden sich im digitalen Anhang.

5.2 Ansatz an Schwächen der Netzwerkkommunikation

In Verbindung mit Analysen der Blockchain erscheinen zwei Angriffe vielversprechend, die Bitcoinadressen und IP-Adressen einander zuordnen. Beide nutzen Details bei der Kommunikation im P2P-Netzwerk aus. Es könnte daher nötig werden, sie bei Änderungen der Abläufe entsprechend anzupassen. Beiden Angriffen ist gemein, dass sie live ablaufen, relativ aufwändig sind und neben den erwünschten eine Menge an uninteressanten Ergebnissen liefern. Zur Ermittlung einer einzelnen Verbindung sind sie daher recht unökonomisch. Sinnvoller erscheint es, diese Techniken einzusetzen, um eine große Zahl an Zuordnungen zu finden, entweder weil man aufgrund von Blockchainanalysen bereits eine große Zahl an zu untersuchenden Adressen hat, oder um Datensätze für zukünftige Recherchen zu gewinnen.

Die erste Methode[116] richtet sich an solche Peers, die keine eingehenden Verbindungen akzeptieren, da ihr Netzwerkverkehr beispielsweise durch ein *NAT (Network Address Translation)* oder eine *Firewall* kontrolliert wird, ähnlich wie Unternehmen nach außen hin oft einen Pförtner oder einen Empfang vorschalten. Auf ihnen läuft keine veränderte andere Bitcoin-Software, dennoch ist es treffend, sie im Folgenden als ***Clients*** zu bezeichnen, wohingegen diejenigen Peers, die auch eingehende Verbindungen akzeptieren, als ***Server*** bezeichnet werden. Um einen Server zu identifizieren, kann versucht werden, mit ihm eine TCP-Verbindung an Port 8333 aufzubauen. Ein Port ist die Adresse einer Anwendung auf einem System, vergleichbar mit der Durchwahl eines Sachbearbeiters in einem Unternehmen. In aller Regel wird ein Server die Verbindung zulassen, ein Client hingegen nicht.

Clients verbinden sich standardmäßig mit 8 Peers (Servern), die in einer Sitzung nicht ausgetauscht werden, sofern sie erreichbar bleiben.[117] Diese Server werden im Folgenden als ***entry nodes*** bezeichnet. Ein Client wählt seine entry nodes zufällig aus einer Liste von Peers, die entweder aus einer vergangenen *getaddr-Anfrage* resultiert, oder die er sich von einem vertrauenswürdigen *seed node* (einem bekannten Standardserver) geben lässt. Um die Liste möglicher Peers aktuell zu halten, sendet ein Client regelmäßig getaddr-Anfragen, woraufhin seine Peers ihm eine zufällige Auswahl ihrer Listen zusenden. Sollte es trotz dieser Durchmischung

116 Der folgende Angriff folgt Biryukov et al. 2014 [9] bzw. Pustogarov 2015 [46] S. 71-87.

117 Für die genauen Abläufe in der P2P-Kommunkation vgl. Biryukov et al. 2014 [9] S. 3f., Antonopoulos 2015 [6] S. 144-149. Weitere Informationen bietet die Protokolldokumentation im Bitcoin Wiki: https://en.bitcoin.it/wiki/Protocol_documentation

gelingen, einen oder mehrere entry nodes eines Clients zielsicher zu besetzen, wären weitgehende Angriffe möglich. Eine genauere Untersuchung der Prozesse, wie ein Client entry nodes gewinnt, und ein Entwurf möglicher Angriffspunkte in einer weiteren Arbeit wären wünschenswert, auch da der weiter unten beschriebene Angriff auf Bloom Filter die Besetzung von entry nodes voraussetzt.

Hier wird jedoch davon ausgegangen, dass ein Angreifer die entry nodes nicht selbst besetzen kann. Hingegen beteiligt er sich mit einer möglichst großen Zahl an Peers (Clients oder Servern) am P2P-Netzwerk und baut zu jedem bekannten Server eine möglichst große Zahl an Verbindungen auf. Ein Server akzeptiert grundsätzlich viele Verbindungen von derselben IP, es könnte aber sinnvoll sein, verschiedene IP-Adressen zu verwenden, um den Angriff unauffälliger zu gestalten.

In einem ersten Schritt wird nun versucht, Zuordnungen zwischen anzugreifenden IP-Adressen und entry nodes zu erhalten. Dazu wird ausgenutzt, dass ein Client zu Beginn einer Sitzung eine *addr-message* an seine entry nodes schickt. Diese enthält seine IP-Adresse und soll den Peer im Netzwerk bekannt machen. Das ist zwar für einen reinen Client überflüssig, doch seitens der Bitcoin-Anwendung besteht keine Unterteilung in Clients und Server, sie ergibt sich nur de facto aus den Einstellungen des benutzten Computers. Die entry nodes leiten die addr-message nun an ein oder zwei ihrer Peers weiter. Diese Peers werden im Folgenden ***responsible*** nodes genannt. Sie werden anhand der Berechnung eines bestimmten Hash-Wertes (u.a. aus weiterzuleitender Adresse und einem Wert für den infrage kommenden responsible node) ausgewählt. Für jeden verbundenen Peer und jede weiterzuleitende Adresse wird ein solcher Hash berechnet, eine Liste erstellt und sortiert. Der oberste oder die obersten beiden Einträge werden als responsible nodes festgelegt. Diese responsible nodes leiten die addr-message nun wiederum an ihre entsprechenden responsible nodes weiter, und so fort. Auf diese Weise wird die Adresse nach und nach über viele Verbindungen verbreitet. Ist die addr-message bereits durch eine Verbindung gelaufen, wird sie nicht erneut darüber gesendet.

Der Angreifer versucht nun, addr-mesages von den entry nodes zu erhalten. Er geht davon aus, dass die Peers, die ihm als erste die addr-message weiterleiten, wahscheinlich die entry nodes sind. Im Idealfall erhält er eine addr-message von 8 verschiedenen entry nodes und kann so entry nodes und IP einander zuordnen. Die Wahrscheinlichkeit, dass mehrere Peers denselben

Satz an entry nodes benutzen, ist äußerst gering, *Biryukov et al.* zeigen in ihrer Arbeit, dass bereits drei entry nodes mit hoher Treffsicherheit eine Identifikation ermöglichen.[118]

Der Ansatz hat eine Schwäche: Wenn ein Angreifer selbst nicht für alle entry nodes die responsible nodes besetzt hat, wird er die addr-message auch von Peers erfahren, die nicht entry nodes sind. Um diese addr-mesages nun aber möglichst *nur* von den entry nodes und nicht von zufälligen anderen Peers zu erhalten, muss verhindert werden, dass andere Peers die addr-message weiterverbreiten. Dazu kann der Angreifer die IPs, die ihn interessieren, *im Vorfeld* des Angriffs bereits selbst im Netzwerk verbreiten, sprich: eine Reihe an addr-messages mit der IP-Adresse des Opfers verschicken. Das wird dazu führen, dass die addr-message, die der angegriffene Client später an seine entry nodes schickt, nicht ein zweites Mal an die selben responsible nodes geleitet wird. Wenn der Angreifer aber durch Zufall einen dieser responsible nodes besetzen konnte, wird er die addr-message erhalten.

Die Besetzung eines responsible nodes erfolgt, indem viele Verbindungen mit ihm aufgebaut werden. Jede dieser Verbindungen führt zu einem anderen Hash-Wert in der Liste. Mit einer gewissen Wahrscheinlichkeit wird einer dieser Werte schließlich die Liste anführen.

Es ist möglich, dass der Angreifer bereits bei seiner eigenen Verbreitung der addr-message zufällig responsible node eines entry nodes war. In dem Fall wird die spätere addr-message nicht an ihn gesendet werden. Daher sollten beim Zeitpunkt seiner eigenen Verbreitung der addr-messages nur wenige Verbindungen von seiner Seite bestehen. Die Verbindungen, von denen er zu diesem Zeitpunkt Weiterleitungen seiner eigenen addr-message erhält, sollten abgebaut und ersetzt werden. Eine genaue Empfehlung über Ablauf des Aufbaus und Anzahl der Verbindungen kann hier nicht gegeben werden und müsste im Testbetrieb untersucht werden.

Bei einem sauber ausgeführten Angriff erhält der Angreifer drei oder mehr wahrscheinliche entry nodes zu einer Reihe von IP-Adressen, zum Teil aber auch weniger. Der Angriff basiert auf einer Reihe zufälliger Ereignisse und hat keine 100-prozentige Treffsicherheit. Man benötigt bereits *im Vorfeld* einen Satz anzugreifender IP-Adressen aus beliebiger Quelle. IP-Adressen können auch erhalten werden, indem der Angreifer getaddr-Messages an seine Peers sendet. Doch wenn die Clients dieser IP-Adressen bereits die Verbindungen

118 Vgl. Biryukov et al. 2014 [9] S. 6.

zu ihren entry nodes aufgebaut haben, senden sie zunächst keine addr-Messages mehr. In diesem Fall müsste abgewartet werden, bis das Opfer eine neue Sitzung startet, oder bis nach einer gewissen Zeit eine neue addr-Message gesendet wird.

In einem zweiten Schritt beobachtet der Angreifer die Verbreitung von Transaktionen. Wenn der angegriffene Client eine Transaktion abschließt, sendet er diese in zwei Schritten an seine entry nodes: Zunächst schickt er eine *inv-message* (für *inventory)*, die unter anderem die Identifikationsnummer (einen Hash) der Transaktion erhält. Der empfangende Peer prüft, ob ihm die ID schon bekannt ist und führt weitere Prüfungen durch. Wenn die inv-message diese Prüfungen besteht, wird über eine *getdata-message* die eigentliche Transaktion angefordert, die wiederum in einer *tx-message* verschickt wird. Die entry nodes senden nun wiederum ihren verbundenen Peers eine inv-message, diese prüfen, senden eine getdata-message zurück, und so weiter. Anders als bei den addr-messages werden hier keine responsible nodes festgelegt. Aufgrund der Prüfungen ergibt sich eine signifikante Zeitverzögerung, sodass man wiederum davon ausgehen kann, dass von den entry nodes eine Transaktion schneller erhalten wird als von anderen Peers. In diesem Fall kann ein Angreifer zwar nicht im Vorfeld schon inv- und tx-messages versenden, um die Verbreitung über Nicht-entry-nodes auszuschließen. Er kann aber anhand der zeitlichen Verzögerung eine Wahrscheinlichkeit festlegen. Dazu müssen lediglich Verbindungen zu sämtlichen Servern aufgebaut werden. Erhält der Angreifer eine Transaktion von einem oder mehreren Peers sehr früh und von anderen Peers deutlich später, handelt es sich bei den frühen Peers wahrscheinlich um entry nodes. Es gibt Mechanismen, die zu einer zufälligen Verzögerung führen, doch es angenommen werden, dass unter den ersten 10 Peers, die eine Transaktion an den Angreifer weiterleiten, mit hoher Wahrscheinlichkeit drei entry nodes sind. [119]

Wenn ein Angreifer bereits nach bestimmten IP-Adressen sucht und deren entry nodes kennt, könnte er natürlich auch gezielt nur deren Transaktionen herausfiltern. Allerdings leiten diese entry nodes auch andere Transaktionen früher oder später weiter, sodass dieser Ansatz nicht gangbar ist.

Die Zuordnung von Transaktionen (bzw. der in ihrem Input genannten public keys) zu IP-Adressen der Sender erfolgt in einem dritten Schritt über den Abgleich der entry nodes aus Schritt 1 (Auswertung der addr-Messages nach

119 Vgl. Biryukov et al. 2014 [9] S. 7.

entry nodes) und Schritt 2 (Auswertung der inv- / tx-Messages nach entry nodes). Bereits bei einem gemeinsamen entry node lässt sich eine (hier noch geringe) Wahrscheinlichkeit festlegen, die mit der Zahl der gemeinsamen entry nodes stark ansteigt.

Wenn verschiedene Transaktionen über dieselben entry nodes laufen, stammen diese wahrscheinlich von derselben IP und aus derselben Sitzung (auch wenn diese IP vielleicht in Schritt 1 nicht ermittelt werden konnte). Auch das kann bereits eine wichtige Erkenntnis sein.

Eine mehrfache oder kontinuierliche Durchführung dieses Angriffs kann die Wahrscheinlichkeiten erhöhen, obwohl sich in jeder Sitzung die entry nodes ändern. Denn in Verbindung mit anderen Analysen, wie z.B. Auswertung der Blockchain, ergeben sich möglicherweise weitere Zuordnungen. Daher kann dieser Angriff sinnvoll für eine große Anzahl an IP-Adressen und über einen längeren Zeitraum durchgeführt werden. Selbst Zuordnungen mit nur einer geringen Wahrscheinlichkeit sollten gespeichert und mit Erkenntnissen aus anderen Quellen oder weiteren Durchläufen verknüpft werden.

Der eben beschriebene Angriff setzt auf Seiten des Senders einer Transaktion an. Es ist zwar prinzipiell möglich, eine Transaktion über Umwege ins Netzwerk zu bringen,[120] in aller Regel ergibt sich aber der beschriebene angreifbare Ablauf. Es besteht insbesondere die Möglichkeit, Dienste wie Tor oder VPN zur **Verschleierung der IP-Adresse** zu verwenden. *Biryukov et al.* schlagen vor, ersteres zu unterbinden, indem im Vorfeld des Angriffes über möglichst viele *Tor-exit-nodes* derart gestaltete Nachrichten an die Bitcoin-Server geschickt werden, dass diese einen bestimmten Angriff vermuten und die IP-Adressen der Tor-exit-nodes sperren.[121] Das Problem der Nutzung solcher Anonymisierungsdienste, die prinzipiell unabhängig vom Bitcoin-Protokoll sind, in Verbindung mit Bitcoin bzw. anderen Kryptowährungen, muss hier außen vor bleiben, könnte aber in einem Aufsatz im Umfang einer Masterarbeit umfassend erläutert werden. Generell ist zu sagen, dass die üblichen Anonymisierungsdienste nicht speziell auf P2P-Netzwerke zugeschnitten sind und dass bereits Angriffe im P2P-Netzwerk entwickelt wurden, die bestimmte Eigenschaften ausnutzen, für die Tor etc. nicht konzipiert sind.[122]

120 *Transaction remote release*, vorgestellt in ShenTu / Yu 2015 [49].
121 Vgl. Biryukov et al. 2014 [9] S. 4f., ausführlicher Pustogarov 2015 [46] S. 87ff.
122 Vgl. Pustogarov 2015 [46] S. 87-97, ferner Manils et al. 2010 [35].

Auch **auf Seiten des Empfängers** einer Transaktion ist ein Angriff möglich. Allerdings muss ein Empfänger keinen verräterischen Datenverkehr initiieren, um eine Transaktion zu empfangen. Zum einen erhält er, als Server wie als Client, von seinen Peers diejenigen Transaktionen, die gerade im Netzwerk verbreitet werden über die ganz normalen inv- und tx-messages. Diese Transaktionen sind in diesem Moment noch nicht von den Minern bestätigt und mit Unsicherheit behaftet. Die bestätigten Transaktionen erhält der Empfänger dann einfach aus der Blockchain.

Allerdings laden immer mehr Nutzer aus Gründen der Bandbreite und des Speicherplatzes nicht die gesamte Blockchain herunter. Sie benutzen eine etwas modifizierte Software, einen sogenannten ***SPV-Client***.[123]Ein SPV-Client lädt nicht alle Blöcke der Blockchain herunter, sondern nur alle Header, und fragt ansonsten im Netzwerk nach den Transaktionen, die für seine Wallet relevant sind. Er lädt insbesondere die kompletten Daten dieser Transaktionen mit ihrem jeweiligen *merkle tree* herunter. Der merkle tree einer Transaktion ermöglicht in Zusammenspiel mit dem Header eines Blockes den Beweis, dass die Transaktion in diesem Block vorhanden ist.[124]

Ein SPV-Client kann bei der Verifizierung von Transaktionen und der Verteilung der Blockchain im Netzwerk keinen Beitrag leisten und läuft daher stets als reiner Client.

Ein SPV-Client muss also notwendigerweise seinen entry nodes offenbaren, welche Transaktionen für seine Wallet relevant sind. Hat ein Angreifer einen entry node unter Kontrolle, kann er einfach die Empfangsadresse(n) der angefragten Transaktionen mit der IP-Adresse des SPV-Clients verknüpfen.

Um dies zu erschweren, setzt der SPV-Client sogenannte ***Bloom Filter*** ein.[125] Die Funktionsweise von Bloom Filtern lässt sich mit folgendem Vergleich recht treffend beschreiben: Ein Gast möchte vom Gastgeber im Vorfeld einer Feier wissen, ob eine bestimmte Person (möglicherweise die Angebetete) auch auf die Feier kommt. Um seine noch heimliche Liebe nicht offenzulegen, könnte der Gast ganz generell fragen, wer denn alles kommt. Das entspräche dem Verhalten eines full node, der die gesamte Blockchain herunterlädt. Er könnte aber auch fragen, wer von den Gästen weiblich, blond, ledig, zwischen 25 und

123 Zu SPV-Clients vgl. Antonopoulos 2015 [6] S. 149ff. Die Grundlage für SPV-Clients ist die Bibliothek *BitcoinJ*, online dokumentiert unter https://bitcoinj.github.io/ (Stand 07.05.2016).

124 Zu merkle trees vgl. Antonopoulos 2015 [6] S. 166-173, Narayanan et al. 2016 [42] S. 34ff.

125 Zu Bloom Filtern vgl. Antonopoulos 2015 [6] S. 152ff.

30 Jahre alt ist und an der philosophischen Fakultät studiert. Je spezifischer eine Frage, desto weniger wertlose Antworten erhält er, aber desto höher ist auch das Risiko, dass der Gastgeber sich seinen Teil dazu denken kann.

Ein Bloom Filter hat genau diese Eigenschaften. Technisch gesehen besteht er aus einer Reihe von Bits, die mit Nullen gefüllt sind. Nun berechnet ein SPV-Client mithilfe eines zufälligen Startwertes aus jeder seiner Empfangsadressen einen Hashwert. Der Startwert bleibt dabei für alle Adressen im Filter gleich. Die verwendete Funktion ist so gestaltet, dass ihr Ergebnis immer eine Zahl ist, die maximal so groß ist, wie der Bloom Filter Felder hat. Für jedes Ergebnis wird in das korrespondierende Bitfeld eine 1 eingetragen. Die Reihe von Bits sendet der SPV-Client seinen entry nodes. Diese berechnen nun für die Empfangsadressen der ihnen vorliegenden Transaktionen die entsprechenden Werte. Wenn einer dieser Werte auch zu einer 1 führen würde an einer Stelle, an der im Bloom-Filter eine 1 steht, wird die Transaktion (samt merkle tree) gesendet.

Neben erhöhter Anonymität haben Bloom Filter unter anderem auch den Vorteil, nur sehr wenig Daten zu enthalten und damit den Netzwerkverkehr im Vergleich zu einer kompletten Liste der Empfangsadressen kaum zu belasten. Es werden notwendigerweise auch überflüssige Transaktionen angefragt, wenn ihr Hash-Wert zufällig ebenfalls ins Raster passt. Die meisten überflüssigen Transaktionen werden jedoch herausgefiltert. Ein Bloom-Filter kann zur Verschleierung noch zusätzliche Einsen enthalten, vorhandenen Einsen dürfen aber nicht getilgt werden. Je mehr überflüssige Ergebnisse (sogenannte *false positives*) er liefert, desto höhere Anonymität gewährleistet ein Filter; die Wahrscheinlichkeit, dass eine Adresse ins Raster passt, obwohl sie nicht in der Eingabe enthalten war, wird als *false positive rate* bezeichnet.

Wie die Arbeiten von *Gervais et al.*[126] und *Nick*[127] zeigen, erlaubt die derzeitige Implementierung von Bloom Filtern jedoch weitgehende Rückschlüsse auf die zugrunde liegenden Adressen. Die entsprechenden Probleme scheinen so einfach nicht zu beheben sein. Denn damit Bloom Filter funktionieren, sind derzeit einige problematisch Verhaltensweisen nötig.[128] Insbesondere ist es äußerst gefährlich, wenn Bloom Filter sowohl public key als auch Bitcoinadresse (also dessen Hash) als Eingabe enthalten, da dies einem Angreifer ermöglicht, alle false positives herauszufiltern und auszuschließen,

126 Vgl. Gervais et al. 2014 [20], besonders S: 4-7.
127 Vgl. Nick 2015 [44], besonders S. 11.
128 Vgl. ebd. den Verweis auf die Antwort eines BitcoinJ -Entwicklers zu der Problematik: https://groups.google.com/forum/#!msg/bitcoinj/Ys13qkTwcNg/9qxnhwnkeoIJ

bei denen nur einer der Werte passt. Hierzu muss natürlich dem Angreifer der public key bekannt sein, was nicht grundsätzlich der Fall ist, wohl aber bei Adressen, die bereits als Sendeadressen verwendet wurden. Problematisch ist auch, dass die gängigen Implementierungen zunächst einen sehr kleinen Bloom Filter bilden und diesen bei Bedarf erweitern und neu absenden. Selbst bei unterschiedlichem Startwert lassen sich Adressen und öffentlice Schlüssel darauf testen, ob sie in beide Filter passen. Problematisch ist auch, dass bei einem Neustart des SPV-Clients (auf Smartphones keineswegs unwahrscheinlich) auch ein neuer Bloomfilter gebildet wird. Ein entry node kann über den Vergleich verschiedener Bloomfilter von derselben IP-Adresse weitgehende Rückschlüsse ziehen.

Die genauen Abläufe bei der Bildung eines Bloom-Filters sollten für die einzelnen Implementierungen unter Beobachtung bleiben. Um hier einen Angriff durchzuführen, müssen Bloom-Filter samt zugehörigen IP-Adressen einfach gesammelt werden. Ein Problem könnten Anonymisierungsdienste darstellen. Eine weitere Hürde stellt die Besetzung von entry nodes dar, denn in dem beschriebenen Szenario können nur die entry nodes sowohl die IP als auch den Bloom Filter abfangen. Möglich bliebe die zufällige Besetzung durch Aufbau vieler Verbindungen über einen längeren Zeitraum mit anschließendem Filtern der relevanten Daten. Die tiefergreifende Bearbeitung des Problems der Besetzung von entry nodes wurde bereits weiter oben angeregt.

5.3 Ansatz an kryptographischen Schwächen

Kryptowährungen basieren notwendigerweise auf kryptographischen Konzepten. Angriffe auf dieser Ebene könnten sehr weitreichende Folgen haben. Würde es einem Angreifer gelingen, die Signatur einer Transaktion (das unlocking script) zu fälschen, könnte er ohne weiteres fremde Coins ausgeben. Allerdings gilt die von Bitcoin und anderen Währungen verwendete asymmetrische Verschlüsselung aktuell als sehr sicher. Es ist bei Bitcoin hingegen problemtisch, dass der SHA-256-Algorithmus für fast alle Hash-Berechnungen eingesetzt wird. Sollte ein Angriff auf diesen Algorithmus entwickelt werden, könnte das weitreichende Folgen haben[129]. Tatsächlich konnten einige früher verbreitete Hash-Algorithmen bereits erfolgreich kompromittiert werden.[130]

129 Vgl. Giechaskiel et al. 2016 [21] S. 6-9.
130 z.B. MD5: vgl. Schmeh 2013 [47] S. 241.

Ein großes Sicherheitsproblem stellt die Schlüsselverwaltung dar. Grundsätzlich sind die Schlüssel einfach in einer Datei unter einem bekannten Pfad auf der Festplatte des Rechners gespeichert. Diese Datei kann wie jede Datei aufgrund technischer Pannen verloren gehen. Da Schlüssel Zufallszahlen sind, können sie dann nicht mehr wiederhergestellt werden, was einem Verlust der von ihnen zu entsperrenden Bitcoins gleichkommt. Es existiert überdies Malware, die gezielt Schlüsseldateien ausliest.[131] Daher gibt es diverse Konzepte und sogar eigene Hardware zur Sicherung der Schlüssel.[132] Eine Möglichkeit stellt das Anlegen von Backups auf separater Hardware, in der Cloud, oder gar auf einem simplen Ausdruck dar. Daten auf der Festplatte des Rechners und in der Cloud sollten zum Schutz vor Angriffen außerdem verschlüsselt werden.

Einen anderen Ansatz bieten *Hierarchical Deterministic Wallets (HD-Wallets)*.[133] Sie benötigen nur einen geheimen Masterkey (***msk***), aus dem sämtliche Schlüssel jederzeit generiert werden können. Aus diesem privaten Masterkey lässt sich überdies ein „öffentlicher" Masterkey (***mpk***) erzeugen, mit dessen Hilfe öffentliche Schlüssel generiert werden können. Die privaten Schlüssel dazu können dann später auf einem abgeschirmten System mithilfe des privaten Masterkey erzeugt werden. Allerdings lassen sich sämtliche Schlüssel zurückrechnen, sollten gewisse Schlüsselkombinationen bekannt werden (insbesondere bei Kenntnis der Kombination beliebiger ***sk*** plus ***mpk***, weswegen auch dieser geheim bleiben sollte).[134] Für die Polizei ist dieser Ansatz im Einzelfall schwierig nutzbar. Es sollte aber die Entwicklung solcher Wallets weiter beobachtet und auf Schwächen untersucht werden, da möglicherweise über das Ausspähen eines unsicher generierten oder schlecht gesicherten Masterkey sehr weitreichende Angriffe ermöglicht werden.

Eine für weitere kryptographische Schwäche stellen Passwörter dar. Wie oben erwähnt, dürften Wallet-Dateien oder Backups in vielen Fällen sicherheitshalber verschlüsselt werden. Dabei werden die Daten meist mit einem Schlüssel fester (und sicherer) Länge verschlüsselt, der wiederum aus einem Passwort generiert wird. Es wird jedoch beobachtet, dass viele Menschen aus Gründen der Bequemlichkeit solche Passwörter verwenden, die mit geringer Leistung unter Verwendung frei zugänglicher Tools offengelegt werden können. Unter Kenntnis der Verfahren, mit denen der Schlüssel aus

131 Vgl. Barber et al. 2012 [7] S. 407.
132 Vgl. Antonopoulos 2015 [6] S. 237.
133 Vgl. ebd. S. 89-97, Narayanan et al. 2016 [42] S. 104-107.
134 Solche Angriffe werden beschrieben in Courtois et al. [13] 2014.

dem Passwort generiert wurde, sind daher die bekannten Angriffe vielversprechend.[135] Sollte ein Passwort gar nur den Zugang zur Cloud oder zu einer Online-Wallet schützen und diese selbst unverschlüsselt sein (eine reine Authentifikation), wäre es unter Umständen sogar noch einfacher, die sensiblen Daten auszulesen. Daher sollten die Mechanismen, mit denen Verschlüsselung und Zugangskontrolle stattfindet, für die einzelnen Anwendungen analysiert werden und abrufbar sein.

5.4 Weitere Ansätze

Neben den beschriebenen Angriffen ergeben sich weitere Möglichkeiten an verschiedenen Ansätzen. Bei einer Kontrolle des gesamten Netzwerkverkehrs eines Verdächtigen durch physischen Zugriff (auf Router / Verteiler / beim Internetanbieter) oder über Malware (*sniffing*) sind weitreichende Angriffe möglich. Besonders problematisch ist, dass die Kommunikation im P2P-Netzwerk von Bitcoin nicht verschlüsselt ist. Ähnlich umfassende Szenarien ermöglicht die verdeckte Installation von Keyloggern und ähnlichen Tools. Auf diese Weise könnten sogar Ende-zu-Ende-verschlüsselte Off-Chain-Transaktionen entdeckt werden. Die Durchführbarkeit solcher Angriffe hängt vom Betriebssystem und der installierten Software ab und kann hier nicht weiter thematisiert werden. Da Dschihadisten die Verwendung von Android-Smartphones in Verbindung mit Ende-zu-Ende-Verschlüsselung empfehlen,[136] wäre eine Auseinandersetzung mit Angriffsmöglichkeiten besonders auf solche Smartphones lohnenswert, würde aber mindestens eine weitere Bachelorarbeit in Anspruch nehmen.

Auch der Zugriff auf Bitcoin-Server, Server von Online-Wallets, Server von Mixing Services etc. sollte in Erwägung gezogen werden.

Neben diesen Ansatzpunkten auf IT-Ebene sind auch Angriffe zu erwägen, die simple Schwierigkeiten bei Erwerb oder Verwertung ausnutzen. Oft wird ein Zusammenspiel der IT-Ermittlungen mit anderen Ermittlungen nötig sein. Bei Einkauf von Waren oder Dienstleistungen im Inland sollten Anbieter entsprechender Waren oder Dienstleistungen zur Zusammenarbeit bewegt werden. Bitcoin-Tauschdienste könnten dazu bewegt werden, bei anonymen Käufen (z.B. mittels Paysafecard) die Empfangsadresse, geloggte IP-Adressen auf der zum Kauf benutzten Webseite, E-Mailadresse o.ä. an die

135 z.B. Wörterbuchangriffe, Brute-Force-Angriffe.
136 Vgl. *Hijrah* 2015 [28] S. 47.

Behörden zu geben. Die Durchführung von Durchsuchungen kann ebenfalls wichtige Erkenntnisse liefern – sofern den Durchführenden bewusst ist, welche Anzeichen auf die Nutzung von Kryptowährungen hindeuten und wie damit umgegangen werden kann.

6 Zusammenfassung und Ausblick

In den vorangegangen Kapiteln wurde untersucht, inwiefern Kryptowährungen eine Rolle bei der Finanzierung des islamistischen Terrorismus spielen oder in der Zukunft spielen könnten.

Festzuhalten ist, dass die aktuellen dschihadistischen Entwicklungen in vielen islamischen Ländern, besonders aber im Einflussbereich von ISIS, auch auf die westlichen Demokratien ausstrahlen. Diese spielen eine Rolle als Adressaten von Anschlägen und Propaganda, aber auch als Basis für die Rekrutierung von Kämpfern und die Erwirtschaftung finanzieller Mittel.

Das Abschneiden von Geldquellen kann ein probates Mittel zur Bekämpfung des islamistischen Terrorismus sein, und sollte auch dann verfolgt werden, wenn nur einzelne, scheinbar unbedeutende Quellen, abgeschnitten werden können.

Auch in Europa werden Finanzmittel zur Unterstützung des islamistischen Terrorismus erwirtschaftet. Diese werden auf vielfältigen Wegen transferiert und nutzbar gemacht.

Bislang ist nicht belegt, dass auch Kryptowährungen zum Transfer eingesetzt werden. Es spricht jedoch einiges dafür, dass dies in Zukunft der Fall sein könnte.

Die Nutzung von Bitcoin, möglicherweise in Verbindung mit verschiedenen Anonymisierungstechniken, scheint in dieser Hinsicht das wahrscheinlichste Szenario. Dabei sind gewöhnliche Transaktionen ebenso denkbar wie Off-Chain-Transaktionen oder spezialisierte Lösungen, auch in Verbindung mit anderen Transfertechniken.

Bitcoin-Transaktionen bieten eine Reihe von Angriffspunkten, die es erlauben, Transaktionen und Akteure einander zuzuordnen. Neben der Analyse in der Blockchain sind besonders Angriffe auf das zugrunde liegende P2P-Netzwerk vielversprechend. Daneben existieren diverse weitere Angriffspunkte.

Aufgabe der Polizei ist es, im Zusammenspiel mit weiteren Behörden und Spezialisten, übergreifende Konzepte zur Entdeckung entsprechender Transaktionen und zur Identifikation der Akteure zu entwickeln. Dies erfordert insbesondere Ermittlungen innerhalb der islamistischen Szene und in sozialen Netzwerken, die Verfügbarmachung spezieller informationstechnischer Einsatzmittel, die Schulung von Personal und die Klärung rechtlicher Fragen.

All diese Ermittlungen können prinzipiell auch zu anderen Zwecken genutzt werden: Zur Aufdeckung weiterer Finanzierungsmodelle und dschihadistischer Netzwerke einerseits; für Ermittlungen in den Bereichen Geldwäsche, Betrug, Ransomware etc. andererseits.

Für die Entwicklung solcher Konzepte sollten einige Fragen beantwortet werden, die in dieser Arbeit nicht nah genug behandelt werden konnten:

Wie sind die dschihadistischen Netzwerke in Europa aufgebaut, wie gestalten sich die Verknüpfungen untereinander und in den arabischen Raum? Wie verändern sich diese Beziehungen durch die Nutzung sozialer Medien und die einfache Verfügbarkeit fortgeschrittener Verschlüsselung in gängigen Kommunikationsanwendungen?

Wie erfolgt die Erwirtschaftung finanzieller Mittel für den Dschihadismus in Europa, wie werden diese Mittel genutzt und auf welchen Wegen werden sie an ihren Bestimmungsort transferiert?

Darüber hinaus sollten einige Untersuchungen informationstechnischer Natur erfolgen:

- Analyse der genutzten Bitcoin-Software, Protokolle und Techniken auf Schwachpunkte und sicherheitsrelevante Änderungen,
- Analyse des P2P-Netzwerkes, insbesondere mit Zielrichtung Besetzung von seed nodes und entry nodes,
- Untersuchung der Nutzung von Mixing Services,

- Untersuchung der Nutzung von IP-Anonymisierung im Zusammenspiel mit Kryptowährungen,
- Untersuchung der Übertragbarkeit der Angriffe auf andere Kryptowährungen.

Außerdem ist eine Zusammenarbeit mit Betreibern von Tauschdiensten, Online-Wallets, Cloud-Diensten und dergleichen anzustreben.

Die Umsetzung dieser Maßnahmen erfordert hohe Anstrengungen seitens der zuständigen Behörden, ist aber eine notwendige Antwort auf die drängenden Herausforderungen dieser Tage.

Literaturangaben

Sofern im Folgenden nicht explizit anders angegeben, wurden sämtliche hier aufgeführte URLs zuletzt am 04.05.2016 abgerufen.

[1] Al Qaida (2010): *Inspire* 1. https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf

[2] Al Qaida (2013): *Inspire* 10. http://azelin.files.wordpress.com/2013/03/inspire-magazine-issue-10.pdf

[3] Al Qaida (2015): *Inspire* 14. https://azelin.files.wordpress.com/2015/09/inspire-magazine-14.pdf

[4] Ali Shukri Amin (2014a): *Remaining Anonymous Online*, Blogeintrag vom 20.08.2014. https://alkhilafaharidat.wordpress.com/2014/08/20/remaining-anonymous-online/

[5] Ali Shukri Amin (2014b): *Bitcoin wa Sadaqat alJihad. Bitcoin and the Charity of Violent Physical Struggle*, Blogeintrag etwa vom 7.08.2014. https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf

[6] Andreas M. Antonopoulos (^{2}2015): *Mastering Bitcoin. Unlocking Digital Cryptocurrencies*, Sebastopol (USA): O'Reilly Media.

[7] Simon Barber / Xavier Boyen / Elaine Shi / Ersin Uzun (2012): „Bitter to better - how to make bitcoin a better currency“, in: *Lecture Notes in Computer Science* 7397, S. 399-414. http://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.pdf

[8] Eli Ben-Sasson / Alessandro Chiesa / Christina Garman / Matthew Green / Ian Miers / Eran Tromer / Madars Virza (2014): *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 IEEE Symposium on Security and Privacy, S: 459 – 474. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956581

[9] Alex Biryukov / Dmitry Khovratovich / Ivan Pustogarov (2014): *Deanonymisation of clients in Bitcoin P2P network*, CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM New York, NY, USA , S. 15-29. http://arxiv.org/pdf/1405.7418.pdf

[10] Jarret M. Brachman / William F. McCants (2006): *Stealing Al-Qua'ida's Playbook*, Combating Terrorism Center At West Point. https://www.ctc.usma.edu/v2/wp-content/uploads/2010/06/Stealing-Al-Qaidas-Playbook.pdf

[11] Aaron Brantly (2014): "Financing Terror Bit by Bit", in: *CTC Sentinel* Vol7. Issue10, S. 1-5. https://www.ctc.usma.edu/v2/wp-content/uploads/2014/10/CTCSentinel-Vol7Iss101.pdf

[12] Bundeskriminalamt (BKA), Bundesamt für Verfassungsschutz (BfV), Hessisches Informations- und Kompetenzzentrum gegen Extremismus (HKE) (2015): *Analyse der Radikalisierungshintergründe und -verläufe der Personen, die aus islamistischer Motivation aus Deutschland in Richtung Syrien oder Irak ausgereist sind. Fortschreibung 2015.* www.bka.de/nn_193924/SharedDocs/Downloads/DE/Publikationen/PublikationsreihenSonstigeVeroeffentlichungen/2015AnalyseRadikalisierungsgruendeSyrienIrakAusreisende,templateId=raw,property=publicationFile.pdf/2015AnalyseRadikalisierungsgruendeSyrienIrakAusreisende.pdf

[13] Nicolas T. Courtois / Pinar Emirdag / Filippo Valsorda (2014): *Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events*, veröffentlicht im Cryptology ePrint Archive 2014. https://eprint.iacr.org/2014/848.pdf

[14] Audrey Kurth Cronin (2015): „ISIS Is Not a Terrorist Group. Why Counterterrorism Won't Stop the Latest Jihadist Threat“, in: *Foreign Affairs* 94, S. 87-98. http://heinonline.org/HOL/Page?handle=hein.journals/fora94&div=43&g_sent=1&collection=journals

[15] Department of Justice (2015): *Virginia Teen Pleads Guilty to Providing Material Support to ISIL. Seventeen-year-old Facilitated Travel to Syria for 18-year-old Prince William County, Virginia, Resident,* Pressemeldung vom 11.06.2015, Office of Public Affairs. http://www.investigativeproject.org/documents/case_docs/2739.pdf

[16] Evan Duffield / Kyle Hagan (2014): *Darkcoin: PeertoPeer CryptoCurrency with Anonymous Blockchain Transactions and an Improved ProofofWork System.* https://www.dash.org/wp-content/uploads/2014/09/DarkcoinWhitepaper.pdf

[17] FATF (2013): *The role of Hawala and other similar service providers in money laundering and terrorist financing,* FATF, Paris. www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html

[18] FATF (2015a), *Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL),* FATF. www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html

[19] FATF (2015b): *Emerging Terrorist Financing Risks,* FATF, Paris. www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

[20] Arthur Gervais / Ghassan O. Karame / Damian Gruber / Srdjan Capkun (2014): *On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients*, Eidgenössische Technische Hochschule Zürich, NEC Laboratories Europe, veröffentlich im Cryptology ePrint Archive 2014. https://eprint.iacr.org/2014/763.pdf

[21] Ilias Giechaskiel / Cas Cremers / Kasper B. Rasmussen (2016): *On Bitcoin Security in the Presence of Broken Crypto Primitives*, University of Oxford, veröffentlicht im Cryptology ePrint Archive 2016. http://eprint.iacr.org/2016/167.pdf

[22] Ethan Heilman / Foteini Baldimtsi / Sharon Goldberg (2016): *Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions*, Boston University, veröffentlicht im Cryptology ePrint Archive 2016. https://eprint.iacr.org/2016/056.pdf

[23] Carla E. Humud / Robert Pirog / Liana Rosen (2015): *Islamic State Financing and U.S. Policy Approaches*, Congressional Research Service Report 7-5700. https://www.fas.org/sgp/crs/terror/R43980.pdf

[24] ISIS (2014): *The Revived Caliphate*. https://archive.org/download/EbookTheRevivedCaliphate2014/Ebook-The-REVIVED-CALIPHATE-2014.pdf

[25] ISIS (2014): *Dabiq* 1. https://azelin.files.wordpress.com/2014/07/islamic-state-22dc481biq-magazine-122.pdf

[26] ISIS (2014): Dabiq 4. https://azelin.files.wordpress.com/2015/02/the-islamic-state-e2809cdc481biq-magazine-422.pdf

[27] ISIS (2015): *Dabiq* 12. https://azelin.files.wordpress.com/2015/11/the-islamic-state-e2809cdc481biq-magazine-12e280b3.pdf

[28] ISIS (2015): *Hijrah to the Islamic State*. https://ia800300.us.archive.org/33/items/GuideBookHijrah2015-ToTheIslamicState/7-Hijrah2015-ToTheIslamicState.pdf

[29] ISIS (2015): *The Islamic State. https://archive.org/download/TheIslamicState2015-FullEbook/TheIslamicState2015FullEbook.pdf*

[30] ISIS (2016): *Dabiq* 13. https://azelin.files.wordpress.com/2016/01/the-islamic-state-e2809cdacc84biq-magazine-13e280b3.pdf

[31] ISIS (2016): *Dabiq* 14. https://azelin.files.wordpress.com/2016/04/the-islamic-state-22dacc84biq-magazine-1422.pdf

[32] ISIS-Sympathisanten (2016): *Report über den 26.04.2016*, arabischsprachiger Online-Eintrag unter https://justpaste.it/topb, aufgerufen am 27.04.2016, mittlerweile gelöscht, im digitalen Anhang als pdf beigefügt.

[33] Matthew Levitt (2014): *Terrorist Financing and the Islamic State*, Testimony submitted to the House Committee on Financial Services November 13, 2014, The Washington Institute for Near East Policy. http://www.washingtoninstitute.org/uploads/Documents/testimony/LevittTestimony20141113.pdf

[34] Peter Mahlmann / Christian Schindelhauer (2007): *Peer-to-Peer-Netzwerke*, Heidelberg: Springer.

[35] Pere Manils / Abdelberi Chaaban / Stevens Le Blond / Mohamed Ali Kaafar / Claude Castelluccia / Arnaud Legout / Walid Dabbous (2010): *Compromising Tor Anonymity Exploiting P2P Information Leakage*. http://arxiv.org/pdf/1004.1461.pdf

[36] Sarah Meiklejohn / Marjori Pomarole / Grant Jordan / Kirill Levchenko / Damon McCoy / Geoff Voelker / Stefan Savage (2013): *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, Proceedings of the 2013 conference on Internet measurement conference. http://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf

[37] Ian Miers / Christina Garman / Matthew Green / Aviel D. Rubin (2013): *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*, 2013 IEEE Symposium on Security and Privacy, S. 397 – 411. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6547123

[38] Malte Möser / Rainer Böhme / Dominic Breuker (2013) : *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*, 2013 eCrime Researchers Summit (eCRS), S. 1-14. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6805780

[39] Imam Muslim Ibn Al-Hadschdschadsch (2014): *Sahih Muslim*, zusammengestellt von Imam 'Abdu-l-Qawi Al-Mundiri, übersetzt von Fadlallah Ksiks, herausgegeben von Mohammed Amine Ramdani, Düsseldorf: Islamische Bibliothek.

[40] Abu Bakr Naji (2004): *The Management of Savagery. The Most Critical Stage Through Which the Umma Will Pass*, übersetzt von William F. McCants 2006. https://azelin.files.wordpress.com/2010/08/abu-bakr-naji-the-management-of-savagery-the-most-critical-stage-through-which-the-umma-will-pass.pdf

[41] Satoshi Nakamoto (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf

[42] Arvind Narayanan / Joseph Bonneau / Edward Felten / Andrew Miller / Steven Goldfeder (2016): *Bitcoin and Cryptocurrency Technologies*, elektronische Vorabveröffentlichung von Februar 2016, Printausgabe voraussichtlich im Jui 2016, Princeton: Princeton University Press. https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1

[43] Peter R. Neumann (2015): *Die neuen Dschihadisten. IS, Europa und die nächste Welle des Terrorismus*, Berlin: Ulstein.

[44] Jonas David Nick (2015): *Data-Driven De-Anonymization in Bitcoin*, Distributed Computing Group, Computer Engineering and Networks Laboratory, Eidgenössische Technische Hochschule Zürich. http://e-collection.library.ethz.ch/eserv/eth:48205/eth-48205-01.pdf?pid=eth:48205&dsID=eth-48205-01.pdf

[45] Magnus Normark / Magnus Ranstorp (2015): *Understanding Terrorist Finance. Modus Operandi and National CTF-Regimes*, Swedish Defense University Report, SEDU designation 46/2015. http://www.fi.se/upload/43_Utredningar/20_Rapporter/2016/Understanding_Terrorist_Finance_160315.pdf

[46] Ivan Pustogarov (2015): *Deanonymization techniques for Tor and Bitcoin*, Université du Luxembourg, Faculty of Sciences, Technology and Communication. http://publications.uni.lu/bitstream/10993/21798/1/phdthesis-pustogarov.pdf

[47] Klaus Schmeh ([5]2013): *Kryptographie. Verfahren, Protokolle, Infrastrukturen*, Heidelberg: dpunkt.verlag.

[48] Tilman Seidensticker (^{3}2015): *Islamismus. Geschichte, Vordenker, Organisationen*, Nördlingen: C.H.Beck.

[49] QingChun ShenTu / JianPing Yu (2015): *Transaction Remote Release (TRR): A New Anonymization Technology for Bitcoin*, Shenzhen University, ATR Defense Science & Technology Lab. https://arxiv.org/ftp/arxiv/papers/1509/1509.06160.pdf

[50] Muhammad al-'Ubaydi / Nelly Lahoud / Daniel Milton / Bryan Pryce (2014): *The Group That Calls Itself a State. Understanding the Evolution and Challenges of the Islamic State*, Combating Terrorism Center At West Point. https://www.ctc.usma.edu/v2/wp-content/uploads/2014/12/CTC-The-Group-That-Calls-Itself-A-State-December20141.pdf

[51] United States District Court for the Eastern District of Virginia / Alexandria Division (2015): *Statement of Facts*, Geständnis des Ali Shukri Amin. http://www.justice.gov/opa/file/477366/download

[52] Juan C. Zarate (2013): „The Coming Financial Wars", adaptiert aus: Juan C. Zarate (2013): *Treasury's War: The Unleashing of a New Era of Financial Warfare,* New York: Public Affairs Books. http://www.strategicstudiesinstitute.army.mil/pubs/parameters/issues/Winter_2013/9_Zarate.pdf

[53] Aiman az-Zawahiri (2005): *Letter to Abū Musʿab az-Zarqāwi, July 9, 2005,* bereitgestellt durch das Combating Terrorism Center At West Point. https://www.ctc.usma.edu/v2/wp-content/uploads/2013/10/Zawahiris-Letter-to-Zarqawi-Translation.pdf

Authentizitätserklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig, ohne fremde Hilfe und ausschließlich unter Benutzung der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die ich wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Quellen entnommen habe, sind als solche kenntlich gemacht, und alle Quellen, die aus dem World Wide Web entnommen oder in einer sonstigen digitalen Form verwendet wurden, sind der Arbeit in digitaler Form beigefügt. Ich bin mir bewusst, dass eine falsche Erklärung rechtliche Folgen haben wird.

Hann. Münden, 09.05.2016

_____ / Thomas Faelligen, PKA