

Jean-Daniel Schmid / Alexander Schmid

Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen

Die Autoren geben in ihrem Beitrag einen ersten Überblick über die sich im Zusammenhang mit der virtuellen Währung «Bitcoin» stellenden rechtlichen Fragen. Dabei konzentrieren sie sich auf öffentlich-rechtliche und strafrechtliche Fragestellungen.

Rechtsgebiet(e): Öffentliches Recht; Strafrecht

Jean-Daniel Schmid / Alexander Schmid

Inhaltsübersicht

- I. Einleitung
- II. Grundlagen
 1. Funktionsweise von Bitcoin
 2. Anonymität
 3. Verwendungsmöglichkeiten
 4. Weitere Eigenheiten
 - 4.1. Erwerb der Währungseinheiten durch Erschaffung oder Tausch
 - 4.2. Volatilität der Währungseinheit
 5. Zwischenfazit
- III. Rechtliche Problemfelder
 1. Vorbemerkungen
 2. Öffentliches Recht
 - 2.1. Zulässigkeit der Schaffung und Nutzung elektronischen Gelds
 - 2.1.1. Bargeldmonopol
 - 2.1.2. Lotterierechtliche Regulierung
 - 2.2. Zwangsvollstreckungsrecht
 - 2.2.1. Hypothetischer Fall als Ausgangssachverhalt
 - 2.2.2. Analyse
 - 2.3. Weitere Problemfelder
 3. Strafrecht
 - 3.1. Erschaffung des Systems Bitcoin und autonome Erzeugung einzelner Bitcoins
 - 3.2. Verwendung von Bitcoins
 - 3.3. Umwandlung Geld/Bitcoins
 - 3.4. Fälschung von Bitcoins
 - 3.5. Unrechtmässige Entwendung von Bitcoins
 - 3.6. Verwendung unrechtmässig entworfener Bitcoins
 - 3.7. Geldwäscherei
- IV. Fazit

I. Einleitung

[Rz 1] Leser in¹ und ausländischer² Zeitungen, Zeitschriften und digitaler Medien wurden in vergangener Zeit vermehrt mit dem Begriff «*Bitcoin*» konfrontiert. Dabei handelt es sich um eine besondere Form elektronischen Gelds³. In diesem Zusammenhang war vom «*gefährlichsten Open-Source-Projekt*»⁴, von «*Anarcho-Geld*»⁵, welches unter anderem von Hackern und Kriminellen eingesetzt werde, und ähnlichem die Rede. Daneben hat sich mit Paul Krugman selbst ein Wirtschaftsnobelpreisträger hierzu geäussert⁶. Im Ausland

haben Angehörige der Legislative von diesem Phänomen Kenntnis erlangt⁷ und es verdichten sich die Anzeichen, dass sich selbst der US-amerikanische Geheimdienst für Bitcoin interessiert⁸. Schliesslich sind am Horizont erste diesbezügliche Gerichtsverfahren und regulatorische Entscheidungen erkennbar⁹.

[Rz 2] Im Hinblick auf das System Bitcoin bestehen zweifellos zahlreiche rechtliche Fragen¹⁰. In der hiesigen¹¹ Literatur hat eine entsprechende Analyse soweit erkennbar bisher nicht stattgefunden¹². Im Folgenden unternehmen die Autoren deshalb den Versuch, diese Lücke zumindest teilweise zu schliessen. Dabei sollen einerseits der technische Hintergrund des Systems sowie dessen wesentliche Eigenheiten kurz erläutert werden. Andererseits schaffen die Autoren eine erste Auslegeordnung möglicher rechtlicher Fragestellungen und führen eine Analyse gewisser dieser Fragen im Lichte des schweizerischen Rechts durch.

[Rz 3] Der erste Teil dieses Beitrags beschäftigt sich mit der Funktionsweise von Bitcoin. Im Anschluss wird ein Überblick über mögliche rechtliche Problemfelder gegeben und eine erste diesbezügliche Analyse durchgeführt. Hierbei gehen die Autoren zuerst auf öffentlich-rechtliche, sodann auf strafrechtliche Aspekte ein¹³. Im letzten Teil wird ein Fazit gezogen.

¹ Siehe statt aller etwa NZZ ONLINE, «Gefährlichstes Open-Source Projekt», http://www.nzz.ch/nachrichten/digital/bitcoin_1.10929007.html (besucht am 5. Mai 2012).

² Siehe statt vieler etwa THE NEW YORK TIMES, Speed Bumps on the Road to Virtual Cash, 4. Juli 2011, B3 (online abrufbar unter: <http://www.nytimes.com/2011/07/04/business/media/04link.html?pagewanted=all> [besucht am 5. Mai 2012]).

³ Die dazugehörigen Einheiten lauten «*Bitcoins*». Zum Ganzen nachstehend Kap. II.

⁴ NZZ ONLINE (Fn. 1).

⁵ DIE ZEIT, Anarcho-Geld, 30. Juni 2011 (online abrufbar unter: <http://www.zeit.de/2011/27/Internet-Bitcoins/komplettansicht> [besucht am 5. Mai 2012]).

⁶ Vgl. KRUGMAN PAUL, Golden Cyberfetters, The New York Times Blog, <http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/> (besucht am 5. Mai 2012).

⁷ Statt vieler THE INDEPENDENT, Hack attack pushes Bitcoin to the brink, <http://www.independent.co.uk/news/business/news/hack-attack-pushes-bitcoin-to-the-brink-2300384.html> (besucht am 5. Mai 2012). Darüber hinaus ist allgemein ein gewisses Grundinteresse an Bitcoin erkennbar. Dies wird bereits dadurch deutlich, dass eine Abfrage mittels Google (Suchbegriff «*Bitcoin*») über 13'000'000 Ergebnisse zu Tage fördert (Suche durchgeführt am 5. Mai 2012).

⁸ Siehe die Bemerkungen bei WALLACE BENJAMIN, The Rise and Fall of Bitcoin, Wired Dezember 2011 (19.12), S. 99–112, insb. S. 104.

⁹ Siehe hierzu die Bemerkungen in Fn. 97.

¹⁰ Siehe etwa die Bemerkungen der Electronic Frontier Foundation, einer Vereinigung, die sich für die Rechte in der digitalen Welt stark macht (ELECTRONIC FRONTIER FOUNDATION, EFF and Bitcoin, <http://www.eff.org/deeplinks/2011/06/eff-and-bitcoin> [besucht am 5. Mai 2012]). Bei der Recherche zum vorliegenden Thema fällt zudem auf, dass es zahlreiche Blogs gibt, welche sich mit entsprechenden juristischen Fragen auseinandersetzen. Siehe statt aller etwa NELSON JOHN WILLIAM, Why Bitcoin isn't a Security under Federal Securities Law, <http://www.lextechnologiae.com/2011/06/26/why-bitcoin-isnt-a-security-under-federal-securities-law/> (besucht am 5. Mai 2012) sowie TECHNOLLAMA, Is Bitcoin legal?, <http://www.technollama.co.uk/is-bitcoin-legal> (besucht am 5. Mai 2012). Daneben sind erste juristische Publikationen erschienen (dazu nachstehend Fn. 11).

¹¹ Im Ausland sind erste Abhandlungen bereits erschienen. Zu nennen ist namentlich GRINBERG REUBEN, Bitcoin: An Innovative Alternative Digital Currency, Hastings Sci. & Tech. L.J. 2011 (Vol. 4), S. 159–208. Vgl. daneben insb. ELIAS MATTHEW, Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy, abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769 (besucht am 5. Mai 2012).

¹² Anders verhält es sich mit anderen Formen elektronischen Gelds. Siehe umfassend dazu WEBER ROLF H., Elektronisches Geld, Zürich 1999.

¹³ Auf eine Analyse privatrechtlicher Fragestellungen wird vorliegend verzichtet. Diesbezüglich ist darauf hinzuweisen, dass sich auch die

[Rz 4] Der vorliegende Beitrag bezweckt, eine juristische Diskussion über Bitcoin anzuregen. Eine vollständige Behandlung oder auch bloss Nennung aller denkbarer Problemfelder wird damit explizit nicht angestrebt. Ebenso kann vorliegend auf nicht-juristische, namentlich etwa ökonomische¹⁴, Aspekte, wenn überhaupt, lediglich punktuell eingegangen werden. Schliesslich ist zu bemerken, dass nicht ausgeschlossen werden kann, dass Bitcoin bald wieder von der Bildfläche verschwinden wird¹⁵. Die nachfolgende Analyse erscheint jedoch gleichwohl bereits im Hinblick darauf sinnvoll, dass das Prinzip, welches hinter Bitcoin steht, auch in Zukunft bei anderen allfälligen Folgesystemen zur Anwendung gelangen könnte.

II. Grundlagen¹⁶

1. Funktionsweise von Bitcoin

[Rz 5] Softwaresysteme, welche elektronisches Geld¹⁷ bereitstellen, müssen verschiedene grundsätzliche Hürden überwinden. Die wichtigsten Probleme stellen die Fälschung der Zahlungsmittel und die Verhinderung der mehrfachen Nutzung einer Zahlungsmittelinheit durch einen Nutzer (sog. «Double-Spending») dar. Diese Probleme können unterschiedlich gelöst werden, wobei die typische Lösung in der Registrierung aller Zahlungsmittelinheiten und der damit durchgeführten Transaktionen in einer zentralen Datenbank besteht, welche von einem unabhängigen Dritten geführt wird.¹⁸

[Rz 6] Bitcoin basiert dagegen auf der Idee, elektronisches Geld bereitzustellen, ohne sich auf eine Drittpartei verlassen zu müssen, welche eine zentrale Datenbank mit allen

Transaktionen führt¹⁹. Insoweit handelt es sich um ein Mehrweg-Token-System²⁰. Um den vorstehend angesprochenen Hindernissen zu begegnen, bedient sich Bitcoin eines Peer-to-Peer-Netzwerks²¹, in welchem ein Register aller Transaktionen gespeichert wird²².

[Rz 7] Vereinfacht dargestellt²³ funktioniert dies wie folgt: Jeder Nutzer des Bitcoin-Systems betreibt auf seinem Rechner eine spezielle Open-Source²⁴-Software (den sog. «Bitcoin-Client»), welche mit dem Einloggen einen Teil des Bitcoin-Netzwerks bildet²⁵. Informationen zu den mit Bitcoin durchgeführten Transaktionen werden sodann im Bitcoin-Netzwerk, d.h. auf den Rechnern der Bitcoin-Nutzer, dezentral gespeichert²⁶. Um einer Manipulation – welche bereits aufgrund der dezentralen Datenhaltung erschwert würde²⁷ – entgegenzuwirken, bedient sich das System kryptographischer Methoden²⁸.

[Rz 8] Die dem Benutzer zur Verfügung stehenden

ausländische Literatur bisweilen primär mit öffentlich- und strafrechtlichen Aspekten auseinandersetzt. Soweit Bitcoin nachhaltig bedeutsam wird, was derzeit schwer abzuschätzen ist, wäre eine Auseinandersetzung mit privatrechtlichen Fragen dagegen zwingend geboten.

¹⁴ Siehe dazu etwa THE ECONOMIST, Bits and bobs, Bitcoin has got geeks excited. What about economists?, 16. Juni 2011 (online abrufbar unter: <http://www.economist.com/node/18836780> [besucht am 5. Mai 2012]). Daneben KRUGMAN (Fn. 6), *passim*.

¹⁵ Zurückhaltend optimistisch betreffend der Zukunft von Bitcoin etwa GRINBERG REUBEN, bitcoin – Today Techies, Tomorrow the world?, The Milken Institute Review 1. Quartal 2012, S. 22–31, online abrufbar unter: http://www.milkeninstitute.org/publications/review/2012_1/22-31MR53.pdf (besucht am 5. Mai 2012), S. 31.

¹⁶ Neben den nachfolgend erwähnten Quellen ist insb. auf das BITCOIN WIKI zu verweisen (https://en.bitcoin.it/wiki/Main_Page [besucht am 5. Mai 2012]), wo sich zahlreiche weitergehende Informationen finden lassen.

¹⁷ Da sich hinsichtlich des Begriffs des elektronischen Gelds noch keine einheitliche Umschreibung herausgebildet hat, wird im Folgenden auf eine entsprechende präzise Definition verzichtet. Siehe dazu WEBER ROLF H., E-Commerce und Recht, 2. Aufl., Zürich/Basel/Genf 2010, S. 592.

¹⁸ WALLACE (Fn. 8), S. 99 f. Ähnliches methodisches Vorgehen bei ELIAS (Fn. 11), S. 5.

¹⁹ WALLACE (Fn. 8), S. 99 f.

²⁰ Zum Begriff und den Eigenheiten solcher Systeme siehe WEBER (Fn. 12), S. 57 f. und WEBER (Fn. 17), S. 595 f.

²¹ Bei einem Peer-to-Peer-Netzwerk handelt es sich um ein Netzwerk von Systemen, in welchem jedes sowohl als Client als auch als Server für die anderen Systeme des Netzwerks fungiert. Dabei existiert kein zentraler Server, welcher die Netzwerkteilnehmer verbindet (sog. «hub and spoke»-Topologie) – die Netzwerkteilnehmer sind vielmehr direkt untereinander verbunden.

²² GRINBERG (Fn. 15), S. 24; WALLACE (Fn. 8), S. 99 f. Anschaulich zur Speicherung ferner NOIZAT PIERRE, Bitcoin: A Universal Complementary Currency?, ParisTech Review, <http://www.paristechreview.com/2012/01/20/bitcoin-universal-complementary-currency/> (besucht am 5. Mai 2012).

²³ Genauere technische Einzelheiten zum System lassen sich in einem Grundlagenpapier, welches von seinem Erfinder, Satoshi Nakamoto, stammt, entnehmen. Vgl. NAKAMOTO SATOSHI, Bitcoin: A Peer-to-Peer Electronic Cash System, <http://bitcoin.org/bitcoin.pdf> (besucht am 5. Mai 2012). Es ist anzumerken, dass anzunehmen ist, dass es sich bei diesem Namen um ein Pseudonym handelt. Vgl. dazu insb. WALLACE (Fn. 8), S. 99–102, S. 109 sowie S. 112 und GRINBERG (Fn. 11), S. 162 sowie ausführlich zur möglichen Identität des Erschaffers DAVIS JOSHUA, The Crypto-Currency, The New Yorker, 10. Oktober 2011, S. 62–70.

²⁴ Der Begriff «Open Source» bezeichnet ein Vertriebs- und Lizenzierungsmodell für Software, welches sich insbesondere dadurch auszeichnet, dass die Software als Quellcode bzw. der Quellcode mit der kompilierten Software ausgeliefert wird und es dem Lizenznehmer (je nach verwendetem Lizenzmodell unter gewissen Bedingungen und Einschränkungen) freisteht, den Quellcode der Software zu verändern und zur Herstellung Werke zweiter Hand zu verwenden. Hierzu statt vieler ELIAS (Fn. 11), S. 1.

²⁵ GRINBERG (Fn. 11), S. 162 f.; GRINBERG (Fn. 15), S. 24 f.; WALLACE (Fn. 8), S. 104. Alternativ kann der Benutzer Bitcoin ohne eigenständige Nutzung eines Clients verwenden, indem er sich spezifischer Webseiten bedient, welche diese Dienstleistung anbieten. Dazu GRINBERG (Fn. 11), S. 162 f.

²⁶ GRINBERG (Fn. 15), S. 24

²⁷ In diesem Sinn auch GRINBERG (Fn. 15), S. 24.

²⁸ Zum Ganzen insb. GRINBERG (Fn. 15), S. 24 f. und S. 29; GRINBERG (Fn. 11), S. 180 f. und anschaulich NOIZAT (Fn. 22). Die zum Einsatz gelangende Technologie dürfte sich auch noch für andere Verwendungszwecke nutzbar machen lassen. Vgl. dazu ARON JACOB, Bitcoin rises again, New Scientist 14. Januar 2012, S. 20.

(Währungs-)Einheiten (sog. Bitcoins) werden durch eine simple Information verkörpert, die im Regelfall auf dem Computer des Verwenders in einer Datei gespeichert wird²⁹.

2. Anonymität

[Rz 9] Zum Versand und zum Empfang von Bitcoin-Zahlungen benötigt der Nutzer eine Bitcoin-Adresse³⁰, welche kostenlos erstellt werden kann³¹. Diese Adressen stellen eindeutige Adressen im Bitcoin-Netzwerk dar, haben aber grundsätzlich keinen Bezug zur Identität des Nutzers oder seinen anderen physischen oder virtuellen Adressen³². Bitcoin bietet daher auf der Ebene der Transaktionen – trotz der Publikation aller Transaktionen im Bitcoin-Netzwerk, die der Publizität von Börsentransaktionen ähnelt³³ – eine mit Bargeld zu vergleichende Anonymität³⁴; im Netzwerk ist bekannt, dass eine klar spezifizierte Transaktion zwischen zwei Adressen stattgefunden hat – wer hinter diesen Adressen steckt, weiss das Netzwerk aber nicht³⁵.

[Rz 10] Dies heisst aber nicht, dass die Verwendung von Bitcoins tatsächlich völlig anonym ist: Sobald eine Bitcoin-Adresse mit der Identität eines Nutzers verknüpft werden kann – z.B. weil der Nutzer eine Bestellung einer physischen Sache an eine Postadresse mit Bitcoin bezahlt hat oder weil der Nutzer unter Angabe seiner Bitcoin-Adresse in einem öffentlichen Forum Beiträge veröffentlicht – ist die Anonymität faktisch aufgehoben³⁶.

3. Verwendungsmöglichkeiten

[Rz 11] Bitcoins können nicht nur (wie zu vermuten wäre) zur Bezahlung von Online-Dienstleistungen oder zum Kauf von Produkten über das Internet benutzt werden³⁷. Es existieren

im Ausland bspw. Restaurants³⁸ und Hotels³⁹, welche Bitcoins als Zahlungsmittel akzeptieren. Es ist davon auszugehen, dass Bitcoins daneben auch für zwielichtigere Zwecke eingesetzt werden⁴⁰.

4. Weitere Eigenheiten

4.1. Erwerb der Währungseinheiten durch Erschaffung oder Tausch

[Rz 12] Das von Bitcoin verwendete Peer-to-Peer-Netzwerk stellt u.a. die Integrität des Systems als Ganzes sicher. Zugleich werden hierdurch periodisch zusätzliche Bitcoins (sog. «Mining») erschaffen.⁴¹ Mit anderen Worten kann jeder, der den Bitcoin-Client verwendet, theoretisch zusätzliche Währungseinheiten erschaffen und anschliessend verwenden⁴². Diese Erschaffung zusätzlicher Währungseinheiten wird aufgrund bewusst im System angelegter ansteigender Komplexität zusehends langsamer bzw. rechenintensiver⁴³. Die derzeit im Umlauf befindliche Anzahl an Bitcoins beträgt ca. 8.9 Mio.⁴⁴ und wird im Jahr 2030 bereits in der Nähe des Maximums von 21 Mio. Bitcoins liegen⁴⁵.

[Rz 13] Die mit diesem System verbundene Zielsetzung besteht einerseits darin, einen Anreiz dafür zu schaffen, den Bitcoin-Client zu verwenden und hierdurch die Integrität des Systems zu unterstützen. Andererseits stellt es einen Weg dar, um die Währungseinheiten überhaupt zu verteilen, zumal es an einem zentralen Herausgeber der Währungseinheit mangelt.⁴⁶

[Rz 14] Bitcoins lassen sich damit auf zwei Arten erwerben: Einerseits durch die eigenständige Erschaffung – wobei diese Variante für Einzelpersonen kaum noch von Bedeutung sein dürfte⁴⁷ – andererseits durch Tausch. Der Tausch kann hierbei nicht bloss durch einen Austausch mit Gütern⁴⁸ erfolgen; vielmehr haben sich bereits viele Plattformen entwickelt,

²⁹ Die Bitcoins können jedoch auch anderweitig, z.B. auf einem Webserver, gespeichert werden. Siehe zum Ganzen GRINBERG (Fn. 11), S. 162 f. und S. 180; WALLACE (Fn. 8), S. 104 und S. 107.

³⁰ Diese Adresse besteht im Fingerprint eines zu einem asymmetrischen Schlüsselpaar gehörenden öffentlichen Schlüssels; eine Bitcoin-Adresse sieht beispielsweise wie folgt aus: 75tWpb8K1S7NmH4Zx6rewF9WQrcZv245W. Siehe dazu auch GRINBERG (Fn. 15), S. 25 f.

³¹ Ein Benutzer kann dabei auch mehrere Adressen erstellen. Hierzu auch GRINBERG (Fn. 11), S. 164 f.

³² In diesem Sinn GRINBERG (Fn. 15), S. 25 f.

³³ NAKAMOTO (Fn. 23), S. 6 und daneben ELIAS (Fn. 11), S. 7.

³⁴ GRINBERG (Fn. 15), S. 25 f. Ähnlich auch DAVIS (Fn. 23), S. 70.

³⁵ GRINBERG (Fn. 11), S. 164 und S. 179; GRINBERG (Fn. 15), S. 30. Vgl. ferner ELIAS (Fn. 11), S. 7. Die Transaktionen können z.B. mittels des Bitcoin Block Explorers nachvollzogen werden, vgl. <http://blockexplorer.com> (besucht am 5. Mai 2012).

³⁶ Siehe zur ganzen Problematik GRINBERG (Fn. 15), S. 30; GRINBERG (Fn. 11), S. 179; WALLACE (Fn. 8), S. 110.

³⁷ Eine Liste mit Händlern, welche Bitcoins akzeptieren, findet sich unter <https://en.bitcoin.it/wiki/Trade> (besucht am 5. Mai 2012). Vgl. zum Ganzen ferner GRINBERG (Fn. 15), S. 27; GRINBERG (Fn. 11), S. 165 f.

³⁸ NEW YORK MAGAZINE, I Spent a Coin (and I Liked It) – How I Bought Lunch With Bitcoins, http://nymag.com/daily/intel/2011/06/i_spent_a_coin_and_i_liked_it.html (besucht am 5. Mai 2012).

³⁹ DAVIS (Fn. 23), S. 66 ff.

⁴⁰ Dazu Kap. III.3.7.

⁴¹ ELIAS (Fn. 11), S. 6 f.; GRINBERG (Fn. 15), S. 24 f.; GRINBERG (Fn. 11), S. 163; WALLACE (Fn. 8), S. 100 und S. 104.

⁴² GRINBERG (Fn. 11), S. 167.

⁴³ GRINBERG (Fn. 11), S. 163 f. und S. 167 m.w.H.; WALLACE (Fn. 8), S. 100.

⁴⁴ Vgl. BITCOIN CHARTS, Bitcoin Network, abrufbar unter <http://bitcoincharts.com/bitcoin/> (besucht am 5. Mai 2012).

⁴⁵ GRINBERG (Fn. 15), S. 25; GRINBERG (Fn. 11), S. 163. Vgl. ferner auch DAVIS (Fn. 23), S. 62. Da sich Bitcoins bis auf die 8. Dezimalstelle aufteilen lassen (GRINBERG (Fn. 11), S. 163) dürfte alleine aus der Begrenzung der maximalen Anzahl an Bitcoins kein Nachteil entstehen.

⁴⁶ NAKAMOTO (Fn. 23), S. 4.

⁴⁷ Siehe die Bemerkungen bei GRINBERG (Fn. 11), S. 167; GRINBERG (Fn. 15), S. 26 f.

⁴⁸ Dazu vorstehend Kap. II.3.

welche den Austausch gegen andere (echte) Währungen erlauben⁴⁹.

4.2. Volatilität der Währungseinheit

[Rz 15] In faktischer Hinsicht ist schliesslich auf die wertmässige Volatilität der Bitcoins aufmerksam zu machen: Bitcoins lassen sich wie dargelegt in andere Währungen konvertieren. Der Wechselkurs der Bitcoins schwankt seit der Begründung des Systems massiv: Im Frühjahr 2010 wurden Bitcoins zu einem Wechselkurs von weniger als 0.01 USD/Bitcoin gehandelt⁵⁰. Im Juni 2011 stieg der Kurs auf rund 30 USD/Bitcoin⁵¹ um im Oktober 2011 auf einen Kurs von 2 USD/Bitcoin zu fallen⁵² und zwischenzeitlich auf wieder über 5 USD/Bitcoin zu steigen⁵³. Der Wert aller sich im Umlauf befindlicher Bitcoins beträgt z.Z. etwa knapp 50 Mio. USD⁵⁴.

5. Zwischenfazit

[Rz 16] Im Ergebnis lässt sich Bitcoin als digitale, dezentralisierte und teilweise anonyme elektronische Währung⁵⁵ qualifizieren, die einen effektiven Verwendungszweck aufweist und deren Währungseinheiten (Bitcoins) durch eigenständige Erschaffung oder Tausch erworben werden können und deren Wert einer hohen Volatilität unterliegt.

III. Rechtliche Problemfelder

1. Vorbemerkungen

[Rz 17] Aufgrund der Zielsetzung des vorliegend Beitrags soll nachfolgend auf einige rechtliche Fragestellungen im öffentlichen Recht und im Strafrecht, die sich im Zusammenhang mit Bitcoin stellen, hingewiesen und auf mögliche Lösungsansätze aufmerksam gemacht werden. Es ist dabei erneut festzuhalten, dass der vorliegende Beitrag einzig dazu dient, potentiell kritische Punkte anzusprechen und eine weitere juristische Diskussion und Auseinandersetzung zu fördern, ohne auf alle möglichen Fragen Antworten zu liefern. Nachfolgend wird zum Zweck der Diskussion stets unterstellt, dass schweizerisches materielles Recht zur Anwendung gelangt.

2. Öffentliches Recht

2.1. Zulässigkeit der Schaffung und Nutzung elektronischen Gelds

2.1.1. Bargeldmonopol

[Rz 18] Art. 99 Abs. 1 BV⁵⁶ erklärt das Geld- und Währungswesen zur Sache des Bundes und statuiert das ausschliessliche Recht des Bundes, Münzen und Banknoten auszugeben. Der Bund ist damit alleine berechtigt, die Währungseinheit und das gesetzliche Zahlungsmittel zu bestimmen (sog. Bargeldmonopol)⁵⁷. Vom verfassungsrechtlichen Geldbegriff und damit auch vom Bargeldmonopol nicht erfasst sind dagegen privat geschaffene Währungseinheiten⁵⁸. Der Verfassungsgeber hat hierunter insbesondere auch privat geschaffenes virtuelles Geld⁵⁹ verstanden⁶⁰. Im Ergebnis sind derartige Schöpfungen alleine dem Markt überlassen⁶¹.

[Rz 19] Es lässt sich somit festhalten, dass die Erschaffung von Bitcoin als System privat geschaffener Währungseinheit in Form elektronischen Gelds aus verfassungsrechtlicher Perspektive in der Schweiz – anders als möglicherweise⁶² in

⁴⁹ Hierzu GRINBERG (Fn. 11), S. 165 f.; GRINBERG (Fn. 15), S. 26 f. DAVIS (Fn. 23), S. 62 hält fest, dass zwischenzeitlich mehr als 40 derartiger Plattformen entstanden sind.

⁵⁰ GRINBERG (Fn. 11), S. 164; WALLACE (Fn. 8), S. 110.

⁵¹ GRINBERG (Fn. 11), S. 164; WALLACE (Fn. 8), S. 110.

⁵² GRINBERG (Fn. 11), S. 164.

⁵³ BITCOIN CHARTS (Fn. 44).

⁵⁴ BITCOIN CHARTS (Fn. 44).

⁵⁵ Angelehnt an GRINBERG (Fn. 11), S. 160.

⁵⁶ Bundesverfassung vom 18. April 1999 der Schweizerischen Eidgenossenschaft (SR 101).

⁵⁷ Botschaft vom 26. Mai 1999 zu einem Bundesgesetz über die Währung und die Zahlungsmittel (WZG), BBl 1999 7258 ff., S. 7261. Ausführlich VEIT MARC D./LEHNE JENS B., Kommentar zu Art. 99 BV, in: Ehrenzeller Bernhard/Mastronardi Philippe/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 2. Aufl., Zürich 2008, N 8 f. sowie WEBER (Fn. 17), S. 601 f.

⁵⁸ Botschaft vom 27. Mai 1998 über einen neuen Geld- und Währungsartikel in der Bundesverfassung, BBl 1998 4007 ff., S. 4029. In diesem Sinne VEIT/LEHNE (Fn. 57), Art. 99 N 9.

⁵⁹ In der Sprache des Verfassungsgebers sog. «Cybercash». Vorliegend wird am Begriff des «elektronischen Gelds» festgehalten (vorstehend Kap. II.).

⁶⁰ Botschaft vom 27. Mai 1998 über einen neuen Geld- und Währungsartikel in der Bundesverfassung (Fn. 58), S. 4029. Siehe auch Botschaft vom 26. Mai 1999 zu einem Bundesgesetz über die Währung und die Zahlungsmittel (WZG) (Fn. 57), S. 7271. Der Verfassungs- bzw. Gesetzgeber hat es dabei unterlassen, dieses Phänomen des virtuellen Geldes weitergehend zu konkretisieren.

⁶¹ VEIT/LEHNE (Fn. 57), Art. 99 N 9. Unter der Berücksichtigung der Kompetenzen der Nationalbank ebenso WEBER (Fn. 17), S. 602 f. Siehe ferner KUNZ MICHAEL, Jedem sein eigenes elektronisches Geld? Zur Frage nach dem Regulierungsbedarf, NZZ vom 9. Januar 1999, S. 27.

⁶² Die Rechtslage in den USA ist sowohl auf verfassungsrechtlicher als auch gesetzlicher Ebene umstritten. Siehe im Kontext von Bitcoin insbesondere GRINBERG (Fn. 11), S. 182–194 und allgemein zu elektronischen Währungseinheiten SMITH BRIAN W./WILSON RAMSEY J., How Best to Guide the Evolution of Electronic Currency Law, Am. U.L. Rev. 1997 (Vol. 46), S. 1105–1130, insb. S. 1109–1113 sowie TUCKER PETER C., The Digital Currency Doppelgänger: Regulatory Challenge or Harbinger of the New Economy?, Cardozo J. Int'l & Comp. L. 2009 (Vol. 17), S. 101–136, insb. S. 119 ff. Private (nicht-elektronische) Währungseinheiten sind in den USA vielerorts üblich und gelten dabei als zulässig, siehe GOOD BARBARA A., Private Money: Everything Old is New Again, Federal Reserve Bank of Cleveland Commentary, April 1998, <http://www.clevelandfed.org/research/commentary/1998/0401.pdf> (besucht am 5. Mai 2012).

den USA, wo die Erschaffung von privaten Währungseinheiten schon zu strafrechtlichen Konsequenzen führte⁶³ – zulässig sein dürfte. Zugleich ist zu bemerken, dass der Bund jederzeit gegen negative Entwicklungen, welche u.a. das Vertrauen in das staatliche Bargeld untergraben können, einschreiten kann⁶⁴. Die vorgenannte Zulässigkeit steht somit, wie dies auch bei anderen privat geschaffenen Währungseinheiten der Fall ist, unter dem ständigen Vorbehalt eines staatlichen Eingriffs.

2.1.2. Lotterierechtliche Regulierung

[Rz 20] Bitcoin sieht sich seit der Einführung regelmässig mit dem Vorwurf konfrontiert, ein unzulässiges Schneeballsystem⁶⁵ bzw. eine Lotterie darzustellen⁶⁶. Es erscheint daher geboten, auch aus dieser Perspektive erste Überlegungen zur Zulässigkeit dieses elektronischen Gelds anzustellen. Dabei ist im Folgenden auf die Lotterieregulierung einzugehen.

[Rz 21] Lotterien sind grundsätzlich verboten (Art. 1 Abs. 1 LG⁶⁷). Gewisse Ausnahmen bleiben vorbehalten (Art. 2 f., 5 ff. und 17 ff. LG). Das System Bitcoin lässt sich evidenterweise nicht als Lotterie qualifizieren, zumal es sich hierbei um keine Veranstaltung handelt, bei welcher gegen Leistung eines Einsatzes oder Abschluss eines Rechtsgeschäftes ein vermögensrechtlicher Gewinn in Aussicht gestellt wird, der im Wesentlichen vom Zufall abhängt⁶⁸. Dies gilt auch für die originäre Erschaffung der Bitcoins, die mit einer Lotterie verglichen wird⁶⁹, da auch in diesem Zusammenhang weder

ein eigentlicher Einsatz⁷⁰ noch der Abschluss eines Rechtsgeschäfts notwendig ist. Daneben stellt das System offensichtlich auch kein konzessionierungspflichtiges Glücksspiel (Art. 3 Abs. 1 SBG⁷¹) dar⁷².

[Rz 22] Der Bundesrat ist befugt, auf dem Verordnungsweg lotterieähnliche Unternehmungen den Bestimmungen des Lotterieggesetzes zu unterwerfen (Art. 56 Abs. 2 LG). Der Verordnungsgeber hat von dieser zulässigen Delegation u.a. im Rahmen von Art. 43 Ziff. 1 LV⁷³ Gebrauch gemacht⁷⁴. Demnach sind den Lotterien insbesondere Veranstaltungen, bei welchen Schneeballsysteme zur Anwendung gelangen, gleichgestellt. Eine solche Veranstaltung liegt dann vor, wenn «die Lieferung von Waren, die Ausrichtung von Prämien oder andere Leistungen zu Bedingungen in Aussicht gestellt werden, die für die Gegenpartei des Veranstalters nur dann einen Vorteil bedeuten, wenn es ihr gelingt, weitere Personen zum Abschluss gleicher Geschäfte zu veranlassen» (Art. 43 Ziff. 1 LV).

[Rz 23] Damit eine unzulässige lotterieähnliche Unternehmung vorliegt, muss die Veranstaltung neben den Voraussetzungen gemäss Art. 43 Ziff. 1 LV eine Ähnlichkeit zur Lotterie gemäss Art. 1 Abs. 2 LG aufweisen. Damit sind die Kriterien der (i) Leistung eines Einsatzes, der (ii) Inaussichtstellung eines Gewinns sowie der (iii) Planmässigkeit angesprochen, welche auch bei Lotterien anzutreffen sind. Im Gegensatz zur Lotterie zeichnet sich die lotterieähnliche Veranstaltung

⁶³ Angesprochen ist damit u.a. der sog. *Liberty Dollar* (ausführlich hierzu GRINBERG (Fn. 11), S. 191–194; andere Beispiele bei TUCKER (Fn. 62), S. 124 ff.). Der Herausgeber dieser physischen Währungseinheit wurde im Frühjahr 2011 für seine Handlungen schuldig gesprochen. Es ist jedoch zu bemerken, dass es sich hierbei insoweit um einen Spezialfall handelt, als dass der Liberty Dollar mit verschiedenen Merkmalen ausgestattet wurde, welche Ähnlichkeiten zur gesetzlichen Währung aufweisen (u.a. dem Zeichen «\$» und dem Wort «Dollar»). Siehe zum Ganzen DEPARTMENT OF JUSTICE, Defendant convicted of minting his own currency, <http://www.justice.gov/usao/ncw/press/nothaus.html> (besucht am 5. Mai 2012). Kritisch GRINBERG (Fn. 11), S. 191–194 und LIPSKY SETH, When Private Money Becomes a Felony Offense, Opinion, The Wall Street Journal Online, <http://online.wsj.com/article/SB10001424052748704425804576220383673608952.html> (besucht am 5. Mai 2012).

⁶⁴ Botschaft vom 27. Mai 1998 über einen neuen Geld- und Währungsartikel in der Bundesverfassung (Fn. 58), S. 4032.

⁶⁵ DAVIS (Fn. 23), S. 62; GRINBERG (Fn. 15), S. 22 und S. 28; WALLACE (Fn. 8), S. 110. Siehe ferner die entsprechenden Hinweise u.a. bei SPIEGEL ONLINE, Angreifer pulverisiert Online-Kurs, <http://www.spiegel.de/netzwelt/web/0,1518,769361,00.html> (besucht am 5. Mai 2012) sowie ALLOWAY TRACY, A currency trader's take on Bitcoin, Financial Times, Alphaville, <http://ftalphaville.ft.com/blog/2011/06/27/602966/a-currency-traders-take-on-bitcoin/> (besucht am 5. Mai 2012).

⁶⁶ DAVIS (Fn. 23), S. 62.

⁶⁷ Bundesgesetz vom 8. Juni 1923 betreffend die Lotterien und die gewerbmässigen Wetten (SR 935.51).

⁶⁸ Hierbei handelt es sich im Wesentlichen um die Legaldefinition einer Lotterie gemäss Art. 1 Abs. 2 LG.

⁶⁹ Hierzu DAVIS (Fn. 23), S. 62.

⁷⁰ Als Einsatz gilt in lotterierechtlicher Hinsicht derjenige Vermögenswert, den der Einleger als Gegenleistung für die Teilnahme an der jeweiligen Veranstaltung erbringen muss. Der Einsatz kann dabei in einer anderen Leistung von Vermögenswert verborgen sein (hierzu insb. BGE 123 IV 175, 178 f. E. 2a); 125 IV 213, 215 E. 1 b/aa)). Die Möglichkeit der originären bzw. autonomen Erschaffung von Bitcoins dient als Anreiz dafür, die Software einzusetzen, welche die Integrität des Systems gewährleistet und das System Bitcoin erst ermöglicht (vorstehend Kap. II.4.1.). Das diesbezügliche Zurverfügungstellen von Rechenleistung lässt sich zumindest *prima facie* kaum unmittelbar unter den Begriff des Einsatzes subsumieren. Es ist jedoch zuzugestehen, dass dieses Zurverfügungstellen einen Vermögenswert beinhaltet, da eine derartige Dienstleistung im Regelfall gegen Entgelt erbracht wird. Aus dieser Perspektive liesse sich im Zusammenhang mit dieser Tatbestandsvoraussetzung bei grosszügiger Auslegung potentiell auch ein anderes Resultat vertreten. Hierauf wird im Folgenden nicht mehr speziell hingewiesen. Siehe zu dieser Tatbestandsvoraussetzung im Allgemeinen insb. FIOILKA GERHARD, «Big Brother»: zwischen Menschenwürde und Lotterieggesetzgebung, Fernsehgewinnspiele mit langfristiger Kandidatenbindung im schweizerischen Lotterierecht, AJP 2000, S. 813–820, insb. S. 817 f.m.w.H.

⁷¹ Bundesgesetz vom 18. Dezember 1998 über Glücksspiele und Spielbanken (Spielbankengesetz, SBG) (SR 935.52).

⁷² Da dies ziemlich offensichtlich erscheint, wird nachfolgend auf die Spielbankengesetzgebung nicht mehr eingegangen.

⁷³ Verordnung vom 27. Mai 1924 zum Bundesgesetz betreffend die Lotterien und die gewerbmässigen Wetten (LV) (SR 935.511).

⁷⁴ Siehe dazu insbesondere BGE 123 IV 225, 226 ff. E. 1 f. sowie die Bemerkungen bei FIOILKA GERHARD, Bundesgericht, Kassationshof, 15. Dezember 1997 i.S.J.c. Staatsanwaltschaft des Kantons Basel-Landschaft, BGE 123 IV 225 ff., Nichtigkeitsbeschwerde, AJP 1998, S. 846–852, insb. S. 850–852. Siehe zu Art. 56 Abs. 2 LG ferner BGE 123 IV 175.

jedoch dadurch aus, dass der in Aussicht gestellte Gewinn nicht allein vom Zufall, sondern von weiteren Eigenheiten abhängig gemacht wird.⁷⁵

[Rz 24] Die Qualifikation des Systems Bitcoin als Schneeballsystem und damit als unzulässige lotterieähnliche Unternehmung erscheint im Lichte der vorgenannten Definitionen in mehrfacher Hinsicht zweifelhaft: Das System ist wie dargelegt so ausgestaltet, dass es keinen eigentlichen Emittenten des elektronischen Gelds gibt⁷⁶. Ein eigentlicher «Veranstalter» ist damit nicht auszumachen. Selbst wenn – entgegen dem Wortlaut von Art. 43 Ziff. 1 LV – die Qualifikation einer Veranstaltung als lotterieähnliche Unternehmung eine klare Abgrenzung zwischen einem Veranstalter und der Gegenpartei des Veranstalters gemäss bundesgerichtlicher Rechtsprechung nicht erfordert⁷⁷, so erscheint die vorgenannte Eigenheit des Systems des gänzlichen Fehlens eines eigentlichen Emittenten nahezulegen, dass keine Veranstaltung vorliegt.

[Rz 25] Es liesse sich jedoch – unter grosszügiger Ausweitung des Begriffs des Veranstalters und der Veranstaltung – auch gegenteilig argumentieren, dass der Aufbau des Systems Bitcoin an und für sich eine Veranstaltung darstellt und dass der Erschaffer des Systems der eigentliche Veranstalter ist. Wie es sich damit verhält, braucht vorliegend jedoch nicht abschliessend geklärt zu werden, zumal andere Aspekte vorliegen, welche gegen die Annahme eines unzulässigen Schneeballsystems sprechen. Namentlich ist u.a. im Hinblick auf Art. 43 Ziff. 1 LV festzuhalten, dass betreffend die Partizipation am System Bitcoin (z.B. Verwendung von Bitcoins als Zahlungsmittel) in vermögensrechtlicher Hinsicht – wenn überhaupt – einzig in Aussicht gestellt wird, dass keine oder geringfügigere Gebühren anfallen, als dies bei einer Bezahlung mit anderen Zahlungsmöglichkeiten der Fall ist⁷⁸. Es erscheint fraglich, ob ein solcher Vorteil unter Art. 43 Ziff. 1 LV subsumiert werden kann. Aufgrund des Zwecks der Lotteriegesetzgebung (Bekämpfung der unerwünschten wirtschaftlichen und sonstigen Folgen der Lotterien⁷⁹) kann zudem davon ausgegangen werden, dass der Gesetzgeber nicht derartige Vorteile als «Gewinn» gemäss Art. 1 Abs. 2 LG im Auge gehabt hat. Das Kriterium der Inaussichtstellung eines Gewinns und die Tatbestandsvoraussetzung der

Lotterieähnlichkeit wird somit nicht erfüllt, weshalb auch unter diesem Gesichtspunkt keine lotterieähnliche Unternehmung vorliegt. Schliesslich dürften diese Vorteile nicht unmittelbar davon abhängen, dass weitere Personen zur Partizipation am System bewegt werden, was zusätzlich gegen die Qualifikation als Schneeballsystem gemäss Art. 43 Ziff. 1 LV spricht.

[Rz 26] Aus alledem folgt, dass bereits bei bloss summarischer Prüfung davon auszugehen ist, dass das System Bitcoin an und für sich⁸⁰ kaum als unzulässiges Schneeballsystem und damit als unzulässige lotterieähnliche Unternehmung zu qualifizieren ist, was nicht allein in lotterierechtlicher Hinsicht von Bedeutung sein dürfte⁸¹. Es erübrigt sich daher, an dieser Stelle auf die weiteren dargelegten Tatbestandsvoraussetzungen einzugehen.

2.2. Zwangsvollstreckungsrecht

2.2.1. Hypothetischer Fall als Ausgangssachverhalt

[Rz 27] Für die nachfolgenden Überlegungen wird von folgendem Sachverhalt ausgegangen: Zwei Personen vereinbaren, dass die eine Person (Veräusserer) der anderen Person (Erwerber) das Eigentum an einem Fahrnisgegenstand verschafft, wofür der Erwerber den Veräusserer in Bitcoins «bezahlt». Es ist zu prüfen, wie der Veräusserer die Bitcoins eintreiben kann, soweit der Erwerber diese nicht fristgerecht zur Verfügung stellt.

2.2.2. Analyse

[Rz 28] Bitcoins stellen nach dem Vorgesagten elektronisches Geld dar⁸². Intuitiv würde die Eintreibung mittels Schuldbetreibung naheliegen, da auf diesem Weg Zwangsvollstreckungen durchgeführt werden, welche auf eine Geldzahlung gerichtet sind (Art. 38 Abs. 1 SchKG⁸³).

[Rz 29] Ob Bitcoins unter die genannte Bestimmung fallen, ergibt sich nicht ohne weiteres aus dem Gesetzeswortlaut. Abzustellen ist vielmehr auf die Behandlung anderer Zahlungsmittel, welche ähnliche Eigenschaften wie Geld aufweisen ohne selbst Geld i.e.S. darzustellen: Es ist insoweit

⁷⁵ Siehe zum Ganzen grundlegend BGE 123 IV 225, 228 ff. E. 2b)-d) und FIOCCA (Fn. 74), S. 850–852. Bestätigt u.a. in BGE 132 IV 76, 78 ff. E. 3.1. f.

⁷⁶ Vorstehend Kap. II.

⁷⁷ BGE 132 IV 76, 84 E. 4.2.4.

⁷⁸ «Compared to other alternatives, Bitcoins have a number of advantages: [...] the fees are much lower» (siehe die Einführung unter <http://www.weusecoins.com> [besucht am 5. Mai 2012]). Anders verhält es sich potentiell in Bezug auf die Möglichkeit der originären Erschaffung von Bitcoins (dazu vorstehend Kap. II.4.1.).

⁷⁹ Siehe die wiederholten Bemerkungen in der Botschaft vom 13. August 1918 zum Entwurfe eines Bundesgesetzes betreffend die Lotterien und lotterieähnlichen Unternehmungen, BBl 1918 IV 333 ff., u.a. S. 333, S. 335 und S. 339 f.

⁸⁰ Es ist jedoch nicht auszuschliessen, dass Bitcoins dazu verwendet werden, Schneeballsysteme aufzubauen bzw. durchzuführen (z.B. Schenkkreise, in welchen anstelle von Geld Bitcoins verwendet werden; in diese Richtung geht etwa der «Bitcoin randomizer», <http://fxnet.bitlex.org/> [besucht am 5. Mai 2012]).

⁸¹ Vgl. auch Art. 3 Abs. 1 lit. r des Bundesgesetzes vom 19. Dezember 1986 gegen den unlauteren Wettbewerb (UWG) (SR 241), wonach unlauter insbesondere derjenige handelt, der «jemandem die Lieferung von Waren, die Ausrichtung von Prämien oder andere Leistungen zu Bedingungen in Aussicht stellt, die für diesen hauptsächlich durch die Anwerbung weiterer Personen einen Vorteil bedeuten und weniger durch den Verkauf oder Verbrauch von Waren oder Leistungen (Schneeball-, Lawinen- oder Pyramidensystem)». Es ist somit eine deutliche Ähnlichkeit zur Definition gemäss Art. 43 Ziff. 1 LV auszumachen.

⁸² Vorstehend Kap. II.

⁸³ Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG) (SR 281.1).

anerkannt, dass Forderungen, die auf WIR-Geld⁸⁴ lauten, im Regelfall nicht auf dem Schuldbetreibungsweg durchgesetzt werden können.⁸⁵ Dies ist darauf zurückzuführen, dass im Betreibungsbegehren die Forderungssumme «*in gesetzlicher Schweizerwährung*» anzugeben ist (Art. 67 Abs. 1 Ziff. 3 SchKG)⁸⁶, wobei WIR-Geld gerade keine gesetzliche Währung darstellt⁸⁷. Eine Betreibung auf Zahlung eines Betrags in Schweizer Franken wäre jedoch möglich, wenn eine diesbezügliche Umrechnung aufgrund eines objektivierbaren Umrechnungskurses oder aufgrund Parteivereinbarung erfolgen könnte.⁸⁸ Gleiches gilt insb. wenn ein gerichtliches Urteil die Umrechnung bestimmt.⁸⁹ Sind diese Voraussetzungen nicht erfüllt, erfolgt die Durchsetzung auf dem Weg der Realexekution gemäss Art. 335 ff. ZPO^{90, 91}

[Rz 30] Vorstehende Überlegungen dürften auch für auf Bitcoins lautende Forderungen gelten: Bitcoins stellen nach dem Vorgesagten gerade kein gesetzliches Zahlungsmittel

dar.⁹² Damit handelt es sich um keine «*gesetzliche Schweizerwährung*» i.S.v. Art. 67 Abs. 1 Ziff. 3 SchKG. Die Zulässigkeit einer Betreibung wäre entsprechend davon abhängig, dass eine Umrechnung gestützt auf einen objektivierbaren Umrechnungskurs erfolgen könnte.⁹³ Wie dargelegt unterliegen Bitcoins einer grossen Volatilität.⁹⁴ Daneben gibt es für Bitcoins eine Vielzahl von Handelsplätzen.⁹⁵ Es erscheint bereits aufgrund dessen mehr als zweifelhaft, dass ein objektivierbarer Umrechnungskurs festgestellt werden kann. Aus diesem Grund dürfte eine Vollstreckung betreffend Bitcoins – zumindest in einer ersten Phase⁹⁶ – nicht mittels Betreibung sondern mittels Realexekution vorzunehmen sein.

2.3. Weitere Problemfelder

[Rz 31] Neben den bereits angesprochenen Problemfeldern dürften zahlreiche weitere öffentlich-rechtliche Aspekte auszumachen sein, welche im Zusammenhang mit dem System Bitcoin einer vertieften Analyse bedürfen. Zu nennen sind etwa das Bankenaufsichts-⁹⁷, das Geldwäschereiaufsichts-⁹⁸,

⁸⁴ Die WIR Wirtschaftsring-Genossenschaft (heute WIR Bank Genossenschaft) hat in den Dreissigerjahren des letzten Jahrhunderts zum Zweck der Selbsthilfe ein System der Kreditgewährung auf der Grundlage bilateraler Verrechnung erschaffen (hierzu statt vieler SCHRANER MARIUS, Die Erfüllung der Obligation, Art. 68–96 OR, Zürcher Kommentar, Bd. 5, Teilbd. V 1e, 3. Aufl., Zürich 2000, Art. 84 N 18). Bei der korrespondierenden Währungseinheit, dem WIR-Geld, welches in der Praxis rege Verwendung findet (hierzu WEBER ROLF H., Artikel 68-96, Berner Kommentar, Bd. VI/1./4., 2. Aufl., Bern 2005, Art. 84 N 57), handelt es sich insb. nicht um Geld im Rechtssinne, sondern um eine Forderung sui generis (so das Urteil des Bundesgerichts 2A.602/2002 vom 23. Juli 2003, E. 3.1.2.1).

⁸⁵ BGE 94 III 74, S. 76 f. E. 3; Urteil des Bundesgerichts 5C.268/2002 vom 14. Februar 2003, E. 2.3; Urteil der Obergerichtskommission OW vom 17. Juni 2005 (publ. in BISchK 2007, S. 143–145 = AbR OW 2004/2005, Nr. 22), E. 1a). Daneben auch Urteil des Obergerichts BL vom 20. Februar 1996 (publ. in BISchK 1997, S. 189 f.); Urteil des Bezirksgerichts Höfe vom 9. Oktober 1970 (publ. in EGV-SZ 1970, S. 57–59), E. 2b). Vgl. aus der Literatur ACCOCELLA DOMENICO, Kommentar zu Art. 38 SchKG, in: Staehelin Adrian/Bauer Thomas/Staehelin Daniel (Hrsg.), Bundesgesetz über Schuldbetreibung und Konkurs I, Basler Kommentar, Basel 2010, N 11; AMONN KURT/WALTHER FRIDOLIN, Schuldbetreibungs- und Konkursrecht, 8. Aufl., Bern 2008, § 7 N 2; GILLIÉRON PIERRE-ROBERT, Commentaire de la loi fédérale sur la poursuite pour dettes et la faillite, Articles 1-88, Lausanne 1999, Art. 38 N 20; RÜETSCHI DAVID/STAUBER DEMIAN, Die Durchsetzung von Fremdwährungsforderungen in der Praxis, BISchK 2006, S. 41–60, insb. S. 48 Fn. 44.

⁸⁶ Aus Art. 38 Abs. 1 SchKG ergibt sich diese Anforderung dagegen nicht (statt vieler JENT-SØRENSEN INGRID, Kommentar zu Art. 38 SchKG, in: Hunzler Daniel (Hrsg.), SchKG, Kurzkommentar, Basel 2009, N 5).

⁸⁷ In diesem Sinn BGE 94 III 74, S. 76 E. 3. Expliziter Urteil des Bundesgerichts vom 14. Februar 2003 (Fn. 85), E. 2.3. In diesem Sinn ferner statt vieler GILLIÉRON (Fn. 85), Art. 38 N 20.

⁸⁸ Urteil der Obergerichtskommission OW vom 17. Juni 2005 (Fn. 85), E. 1a). In diesem Sinn auch ACCOCELLA (Fn. 85), Art. 38 N 11. Diese Möglichkeit bleibt im Urteil des Bundesgerichts vom 14. Februar 2003 (Fn. 85), E. 2.3 unerwähnt.

⁸⁹ BGE 94 III 74, S. 76 E. 3; Urteil der Obergerichtskommission OW vom 17. Juni 2005 (Fn. 85), E. 1a). Aus der Literatur statt vieler ACCOCELLA (Fn. 85), Art. 38 N 11.

⁹⁰ Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (Zivilprozessordnung, ZPO) (SR 272).

⁹¹ Statt vieler ACCOCELLA (Fn. 85), Art. 38 N 11.

⁹² Vorstehend Kap. III.2.1.1.

⁹³ Daneben wäre auch eine Parteivereinbarung ausreichend; gemäss Ausgangssachverhalt liegt eine solche jedoch nicht vor.

⁹⁴ Vorstehend Kap. II.4.2.

⁹⁵ Vorstehend Kap. II.4.1.

⁹⁶ Im Rahmen der Realvollstreckung kann die Umwandlung in eine Geldschuld verlangt werden (Art. 345 Abs. 1 lit. b ZPO), welche sich im Anschluss auf dem Betreibungsweg vollstrecken lässt.

⁹⁷ Beispielsweise lässt sich die Frage aufwerfen, ob die Ausgabe elektronischen Gelds als Geldsurrogat einer bankengesetzlichen Bewilligung bedarf (verneinend etwa WEBER (Fn. 17), S. 603 f.; KUNZ (Fn. 61), S. 27 sowie LYNEDJIAN MARC, La monnaie électronique – Quelques aspects juridiques, SZW 2000, S. 169–176, insb. S. 174; siehe ferner schon WEBER (Fn. 12), S. 88 ff.). Diesbezüglich gilt es im Hinblick auf die Besonderheit von Bitcoin erneut festzuhalten, dass ein eigentlicher (zentraler) Emittent so wieso nicht besteht. Bankenaufsichtsrechtliche Fragen dürften sich auch etwa beim Betrieb einer «Bitcoin-Bank» stellen. Derartige Dienstleistungen werden im Ausland bereits erbracht (vgl. etwa «flexcoin», <http://www.flexcoin.com/> [«the bitcoin bank»]; besucht am 5. Mai 2012). Beachtlich erscheint, dass in Frankreich ein erster Entscheid des Regulators, d.h. der französischen Nationalbank, ergangen zu sein scheint, welcher Unternehmen betrifft, welche im Zusammenhang mit Bitcoin den Tausch in andere (reale) Währungen erlauben (vgl. hierzu Mt.Gox, All EUR transactions will be temporarily suspended within Europe, with immediate effect, <https://support.mtgox.com/entries/20568322-all-eur-transactions-will-be-temporarily-suspended-within-europe-with-immediate-effect> [besucht am 5. Mai 2012]). In diesem Zusammenhang werden auch erste zivilrechtliche Streitigkeiten ausgetragen, da sich gewisse Geschäftsbanken weigern, derartigen Unternehmen Konten zur Abwicklung von diesbezüglichen Transaktionen zur Verfügung zu stellen, da diese Transaktionen bewilligungspflichtigen Unternehmen vorbehalten seien (vgl. dazu Ordonnance de refere du Tribunal de Commerce de Creteil vom 11. August 2011 i.S.S.M.v.C.I. [Nr. 2011R00309]; Ordonnance de refere du Tribunal de Commerce de Creteil vom 31. August 2011 i.S.S.M.v.C.I. [Nr. 2011R00323]; Arrêt du Cour d'Appel de Paris vom 26. August 2011 i.S.C.I.v.S.M. [Nr. 11/15269]).

⁹⁸ Namentlich ist zu prüfen, ob sich im Zusammenhang mit der Geldwäschereibekämpfung Bewilligungspflichten ableiten lassen (bejahend für elektronisches Geld im Allgemeinen WEBER (Fn. 17), S. 605).

das Börsen⁹⁹, das Datenschutz¹⁰⁰ und das Steuerrecht. Aufgrund der Zielsetzung dieses Beitrags wird auf diese Aspekte vorliegend nicht eingegangen.

3. Strafrecht

3.1. Erschaffung des Systems Bitcoin und autonome Erzeugung einzelner Bitcoins

[Rz 32] Die Erschaffung des Systems Bitcoin und die Erzeugung einzelner Bitcoins¹⁰¹ an sich dürfte nicht strafbar sein. Namentlich verstösst dieses Verhalten *nicht* gegen das Währungsrecht, da dieses lediglich das gesetzliche Zahlungsmittel erfasst¹⁰². Die entsprechende strafrechtliche Bestimmung (Art. 11 WZG¹⁰³) ist damit nicht anwendbar. Ebenfalls *nicht* betroffen sind die lotterierechtlichen Strafbestimmungen (Art. 38 ff. LG), da keine Lotterie und keine lotterieähnliche Unternehmung vorliegt¹⁰⁴. Schliesslich sind auch die Geldfälschungsdelikte (Art. 240 ff. StGB¹⁰⁵) nicht einschlägig, da diese Delikte lediglich in- und ausländische, staatlich als Wertträger beglaubigte, mit einem gesetzlichen Kurs versehene Zahlungsmittel betreffen¹⁰⁶, was bei Bitcoins gerade nicht der Fall ist¹⁰⁷.

3.2. Verwendung von Bitcoins

[Rz 33] Wie bereits dargelegt¹⁰⁸ werden Bitcoins nicht von der Lotterieregulierung erfasst. Lotterierechtliche Strafbestimmungen (Art. 38 ff. LG) sind damit auch im Bereich der Verwendung von Bitcoins (beispielsweise als Zahlungsmittel) nicht anwendbar¹⁰⁹. Gleiches gilt für die

währungsrechtsrechtliche Strafbestimmung (Art. 11 WZG)¹¹⁰. Die Verwendung von Bitcoins dürfte damit im Allgemeinen nicht strafbar sein.

3.3. Umwandlung Geld/Bitcoins

[Rz 34] Es wurde bereits erwähnt, dass sich Geld in Bitcoins umwandeln lässt. Ebenso lassen sich Bitcoins zu Geld umwandeln.¹¹¹ Derartige Handlungen dürften aus lotterierechtlicher und währungsrechtlicher Sicht unproblematisch und damit nicht strafbar sein¹¹².

3.4. Fälschung von Bitcoins

[Rz 35] Bitcoins gelten aufgrund ihrer Ausgestaltung als weitgehend fälschungssicher¹¹³. Gleichwohl lässt sich nicht zuletzt im Hinblick darauf, dass sich vorgenannte Annahme im Laufe der Zeit als falsch herausstellen könnte, die Frage aufwerfen, wie eine derartige Fälschung strafrechtlich zu beurteilen wäre. Geldfälschungsdelikte scheiden wie dargelegt¹¹⁴ aus. Gleiches gilt für den Straftatbestand der Warenfälschung (Art. 155 StGB), da als Waren lediglich bewegliche Sachen in Frage kommen¹¹⁵.

[Rz 36] Prüfwert erscheint die Anwendbarkeit der Urkundendelikte (Art. 251 ff. StGB). Aufzeichnungen auf Bild- und Datenträgern werden traditionellen Urkunden gleichgestellt, soweit sie dem identischen Zweck dienen (Art. 110 Abs. 4 StGB) (sog. «Computerurkunde»). Damit Aufzeichnungen auf Bild- und Datenträgern geschützt werden, müssen vorab die traditionellen Voraussetzungen der Schrifturkunde¹¹⁶ erfüllt sein (menschliche Gedankenäusserung, Beständigkeit, Beweisbestimm- und -geeignetheit, Erkennbarkeit des Ausstellers)¹¹⁷.

[Rz 37] Hinsichtlich der vorgenannten Voraussetzungen

⁹⁹ Prüfwert wäre etwa die Frage, inwieweit «Bitcoin-Börsen», welche bereits heute bestehen (zu nennen ist insb. «Mt. Gox», <https://mtgox.com/> [besucht am 5. Mai 2012]; vgl. daneben vorstehend Kap. II.4.1.), bei einem Betrieb in der Schweiz börsenrechtlich zu erfassen wären.

¹⁰⁰ Siehe dazu im Allgemeinen etwa WEBER (Fn. 12), S. 139 ff.

¹⁰¹ Gemeint ist hierbei die autonome Erzeugung einzelner Bitcoins (siehe dazu vorstehend Kap. II.4.1.).

¹⁰² Vorstehend Kap. III.2.1.1.

¹⁰³ Bundesgesetz vom 22. Dezember 1999 über die Währung und die Zahlungsmittel (WZG) (SR 941.10).

¹⁰⁴ Vorstehend Kap. III.2.1.2.

¹⁰⁵ Schweizerisches Strafrechtbuch vom 21. Dezember 1937 (SR 311).

¹⁰⁶ Grundlegend BGE 78 I 225 und BGE 82 IV 198. Siehe ferner statt aller in diesem Sinn DONATSCH ANDREAS/WOHLERS WOLFGANG, Strafrecht IV, 4. Aufl., Zürich/Basel/Genf 2011, S. 108 f. m.w.H. Im Ergebnis ebenso zum softwarebasierten elektronischen Geld im Allgemeinen WEBER (Fn. 12), S. 135.

¹⁰⁷ Vorstehend Kap. II.

¹⁰⁸ Vorstehend Kap. III.2.1.2.

¹⁰⁹ Damit muss nicht geprüft werden, ab welchem Zeitpunkt eine strafbare Beteiligung an einer unerlaubten Lotterie bzw. einer unerlaubten lotterieähnlichen Unternehmung vorliegt. Siehe hierzu etwa BGE 132 IV 76, 85 ff. E. 5.

¹¹⁰ Vorstehend Kap. III.3.1.

¹¹¹ Vorstehend Kap. II.4.1.

¹¹² Siehe zur Begründung vorstehend Kap. III.3.1. f.

¹¹³ Vorstehend Kap. II.1. und daneben auch ELIAS (Fn. 11), S. 5; GRINBERG (Fn. 15), S. 25.

¹¹⁴ Vorstehend Kap. III.3.1.

¹¹⁵ Statt vieler TRECHSEL STEFAN ET AL., Schweizerisches Strafrechtbuch, Praxiskommentar, Zürich 2008, Art. 155 N 3.

¹¹⁶ Siehe zu diesen ausführlich etwa DONATSCH/WOHLERS (Fn. 106), S. 141 ff.

¹¹⁷ Botschaft vom 24. April 1991 über die Änderung des Schweizerischen Strafrechtbuches und des Militärstrafgesetzes sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung, BBl 1991 II 969 ff., S. 993. Siehe ferner statt aller differenziert SCHMID NIKLAUS, Computer- sowie Check- und Kreditkarten-Kriminalität, Zürich 1994, Art. 110 Ziff. 5 StGB N 56 ff. und daneben BOOG MARKUS, Kommentar zu Art. 110 Abs. 4 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Strafrecht I, Basler Kommentar, 2. Aufl., Basel 2007, N 68; TRECHSEL ET AL. (Fn. 115), Vorbemerkungen vor Art. 251 ff. N 19. Kritisch dazu etwa KUNZ KARL-LUDWIG, Grundstrukturen des neuen Vermögens- und Urkundenstrafrechts, ZBJV 1996, S. 189–210, S. 201. Offener STRATENWERTH GÜNTER/WOHLERS WOLFGANG, Schweizerisches Strafrechtbuch, Handkommentar, 2. Aufl., Bern 2009, Art. 110 N 14.

stellen sich bei Bitcoins hauptsächlich zwei Probleme. Erstens ist zu prüfen, ob Bitcoins bzw. die damit in Zusammenhang stehenden Aufzeichnungen¹¹⁸ als menschliche Gedankenäusserungen qualifiziert werden können. Im Zusammenhang mit Computerurkunden ist hierbei darauf abzustellen, ob der Inhaber der Datenverarbeitungsanlage den Willen aufweist, sich die automatisierten Gedankengänge zu Eigen zu machen und sich die Ergebnisse als eigene Erklärungen zurechnen zu lassen¹¹⁹. Bei elektronischem Geld, d.h. auch den Bitcoins, kann diese Voraussetzung bejaht werden¹²⁰. Zweitens bedarf die Frage der Erkennbarkeit des Ausstellers einer vertieften Analyse. Diesbezüglich gelten im Vergleich zur traditionellen Schrifturkunde herabgesetzte Anforderungen¹²¹. Gleichwohl ist es zumindest notwendig, dass sich aus den Umständen ergibt, aus welcher Datenverarbeitungsanlage die Daten stammen bzw. wem sie zuzurechnen sind¹²². Nach dem Vorgesagten zeichnen sich Bitcoins insbesondere durch ihren hohen Grad an Anonymität aus¹²³. Eine Zurechnung zu einer bestimmten Person bzw. Datenverarbeitungsanlage ist aus diesem Grund alleine aufgrund der Bitcoins selbst *nicht* möglich bzw. nur soweit weitere *äussere* Anhaltspunkte beachtet werden. Bei Schrifturkunden gilt die Tatbestandsvoraussetzung der Erkennbarkeit des Ausstellers etwa dann als nicht erfüllt, wenn der Aussteller lediglich aufgrund äusserer Umstände (z.B. Analyse der Schrift) ermittelbar ist¹²⁴. Im Hinblick darauf erscheint es unter Berücksichtigung der angesprochenen Eigenheiten von Bitcoin zumindest zweifelhaft, entsprechende Daten als Urkunde i.S.v. Art. 110 Abs. 4 StGB zu qualifizieren. Die Anwendbarkeit der Urkundendelikte entfällt damit¹²⁵. Die Fälschung von Bitcoins wäre somit auch unter diesem Gesichtspunkt straflos¹²⁶.

3.5. Unrechtmässige Entwendung von Bitcoins

[Rz 38] Bitcoins haben kürzlich für Schlagzeilen gesorgt,

da diese verschiedentlich «gestohlen» wurden¹²⁷. In technischer Hinsicht ist zu bemerken, dass die Informationen, die notwendig sind, um Bitcoins zu verwenden, in einer Datei (bis vor kurzem unverschlüsselt¹²⁸) abgespeichert werden¹²⁹. Wer Zugriff auf die entsprechenden Daten besitzt und das zugehörige Passwort kennt, kann somit die entsprechenden Bitcoins verwenden¹³⁰. Diese technische Lösung, welche wie dargelegt bis vor kurzem nicht einmal eine Verschlüsselung aufwies, hat denn auch schon Tüftler dazu bewogen, Programme (sog. «Malware») zu programmieren, welche gezielt nach der entsprechenden Datei suchen und die Daten an eine andere (unberechtigte) Person senden¹³¹.

[Rz 39] In strafrechtlicher Hinsicht gilt es zu bemerken, dass die Entwendung der Bitcoins, die sich auf dem Weg der Entwendung der vorgenannten Daten erzielen lässt, im Regelfall¹³² keinen Diebstahl i.S.v. Art. 139 StGB darstellt, da als entsprechendes Tatobjekt lediglich bewegliche Sachen, d.h. körperlich fassbare Gegenstände, in Frage kommen, wozu Daten gerade nicht zählen¹³³. Diverse weitere Delikte scheiden ebenfalls aus diesem Grund aus¹³⁴. Einschlägig könnten dagegen die sog. «Computer-Delikte» sein. Die Entwendung

¹¹⁸ Siehe zu den technischen Aspekten vorstehend Kap. II.1.

¹¹⁹ Statt vieler SCHMID (Fn. 117), Art. 110 Ziff. 5 StGB N 58. Anders BOOG (Fn. 117), Art. 110 Abs. 4 N 74, wobei darauf abgestellt wird, ob der Erklärende die Informations- oder Aussageherrschaft inne hat.

¹²⁰ WEBER (Fn. 12), S. 134.

¹²¹ Statt vieler SCHMID (Fn. 117), Art. 110 Ziff. 5 StGB N 63 ff., insb. N 65.

¹²² Statt vieler SCHMID (Fn. 117), Art. 110 Ziff. 5 StGB N 65 und daneben BOOG (Fn. 117), Art. 110 Abs. 4 N 78 sowie etwa VEST HANS, Probleme des Urkundenstrafrechts, AJP 2003, S. 883–891, insb. S. 889 f.

¹²³ Vorstehend Kap. II.2.

¹²⁴ Selbige Überlegungen gelten bei Zeichenurkunden. Siehe zum Ganzen statt vieler BOOG (Fn. 117), Art. 110 Abs. 4 N 43 und N 61.

¹²⁵ Anders für elektronisches Geld, welches nicht die Eigenheiten der Bitcoins aufweist, WEBER (Fn. 12), S. 134 f.

¹²⁶ Anders zu beurteilen sein könnte die Verwendung gefälschter Bitcoins. Dieser Aspekt wäre mutmasslich unter dem Aspekt des Betrugs (Art. 146 StGB) bzw. des betrügerischen Missbrauchs einer Datenverarbeitungsanlage (Art. 147 StGB) zu prüfen. Aufgrund der derzeitigen Unwahrscheinlichkeit der Fälschung von Bitcoins wird auf diesen Aspekt an dieser Stelle nicht vertieft eingegangen.

¹²⁷ Siehe statt vieler etwa THE NEW YORK TIMES (Fn. 2), B3 sowie NZZ ONLINE, Virtuelle Währung bricht ein, http://www.nzz.ch/nachrichten/digital/bitcoins_mt_gox_1.10990274.html (besucht am 5. Mai 2012). In einem Fall habe der Diebstahl Bitcoins im Wert von rund 500'000 US-Dollar umfasst (siehe THE REGISTER, Man says he lost 0,000 in virtual currency heist, http://www.theregister.co.uk/2011/06/16/bitcoin_theft_claims/ [besucht am 5. Mai 2012]). Vgl. zum Ganzen ferner GRINBERG (Fn. 11), S. 180; WALLACE (Fn. 8), S. 107.

¹²⁸ Siehe die Bemerkungen bei THE GUARDIAN, Bitcoins: What are they and how do they work?, 23. Juni 2011 (online abrufbar unter: <http://www.guardian.co.uk/technology/2011/jun/22/bitcoins-how-do-they-work> [besucht am 5. Mai 2012]) sowie THE NEW YORK TIMES (Fn. 2), B3. Zwischenzeitlich ist eine Verschlüsselung eingeführt worden, welche die Verwendung eines Passworts erforderlich macht. Hierzu GRINBERG (Fn. 15), S. 29.

¹²⁹ Vorstehend Kap. II.1.

¹³⁰ In diesem Sinn auch GRINBERG (Fn. 15), S. 29.

¹³¹ Siehe SYMANTEC, Infostealer.Coinbit, http://www.symantec.com/security_response/writeup.jsp?docid=2011-061615-3651-99 (besucht am 5. Mai 2012) («Infostealer.Coinbit is a Trojan horse that attempts to steal Bitcoin wallets») sowie SYMANTEC, All your Bitcoins are ours, <http://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours> (besucht am 5. Mai 2012). Siehe ferner WALLACE (Fn. 8), S. 110.

¹³² Ausgenommen wäre derjenige Fall, in welchem eine Person den entsprechenden (fremden) physischen Datenträger (samt den Daten) entwendet, da es sich beim Datenträger um eine bewegliche Sache handelt (dazu BGE 128 IV 11 und DONATSCH ANDREAS, Strafrecht III, 9. Aufl., Zürich 2008, S. 82 und S. 134).

¹³³ Statt vieler DONATSCH (Fn. 132), S. 82 und S. 134. Ebenso für das elektronische Geld im Allgemeinen WEBER (Fn. 12), S. 128.

¹³⁴ Namentlich etwa unrechtmässige Aneignung (Art. 137 StGB) und Sachentziehung (Art. 141 StGB). Daneben ist auf weitere Delikte aufmerksam zu machen, welche aufgrund der Besonderheiten des elektronischen Gelds ebenso – offensichtlich – ausscheiden. Hierzu zählt namentlich der Straftatbestand des Check- und Kreditkartenmissbrauchs (Art. 148 StGB). Siehe zum Ausscheiden vorgenannter Delikte im Allgemeinen WEBER (Fn. 12), S. 128 f. und S. 131 f.

der Daten könnte durch Art. 143 StGB (unbefugte Datenbeschaffung) abgedeckt sein¹³⁵. Dabei wird u.a. vorausgesetzt, dass der Inhaber der Daten, d.h. der Verwender der Bitcoins, die Daten gegen den unbefugten Zugriff des Täters im Rahmen des Zumutbaren bzw. Üblichen geschützt hat.¹³⁶ Welche Anforderungen damit genau verlangt werden, ist umstritten¹³⁷. Es dürfte praxismässig jedoch genügen, wenn der Computer mittels gängiger Vorsichtsmassnahmen gegen allgemeine Bedrohungen (Passwörter, Firewall, Software) geschützt wird. Vorsichtsmassnahmen gegen die konkret eingetretene Bedrohung sind dagegen nicht notwendig.¹³⁸ Aus diesem Grund dürfte das bislang übliche¹³⁹ unverschlüsselte Speichern der für die Nutzung der Bitcoins notwendigen Daten – und damit das Unterlassen *spezifischer* Schutzmassnahmen gegen die Entwendung von Bitcoins – *nicht* automatisch dazu führen, dass die Anwendbarkeit von Art. 143 StGB entfällt.

[Rz 40] Das im Vorfeld potentiell erfolgende unerlaubte Eindringen in das System des Bitcoin-Inhabers wird durch Art. 143^{bis} StGB (unbefugtes Eindringen in ein Datenverarbeitungssystem) erfasst, soweit eine besondere Sicherung im vorgenannten Sinne vorliegt¹⁴⁰. Soweit im Anschluss effektiv eine unbefugte Datenbeschaffung begangen wird, tritt Art. 143^{bis} StGB hinter Art. 143 StGB zurück¹⁴¹. Eine allfällige Löschung der Daten wäre nach Art. 144^{bis} StGB (Datenbeschädigung) zu beurteilen, wobei ein besonderer Schutz gegen unbefugten Zugriff, im Gegensatz zu den anderen angesprochenen Delikten, nicht notwendig ist¹⁴².

[Rz 41] Im Ergebnis lässt sich festhalten, dass die eigentliche Entwendung von Bitcoins, soweit es um die angedrohte Strafe geht, vergleichbar zu ahnden ist wie der Diebstahl von Geld¹⁴³. Diese Gleichbehandlung gelangt jedoch lediglich

dann zum Zug, wenn die vorgenannten Delikte überhaupt zur Anwendung gelangen, was voraussetzt, dass der Inhaber der Bitcoins sein System adäquat gesichert hat.

3.6. Verwendung unrechtmässig entwendeter Bitcoins

[Rz 42] Die Verwendung unrechtmässig entwendeter Bitcoins als Zahlungsmittel könnte strafrechtlich in verschiedener Hinsicht relevant sein. Derjenige, der einen unrechtmässig entwendeten Bitcoin als Zahlungsmittel verwendet, dürfte die Gegenpartei regelmässig (zumindest implizit) darüber täuschen, am entsprechenden Bitcoin originär berechtigt zu sein. Soweit Personen oder Datenverarbeitungsanlagen getäuscht bzw. in der Datenverarbeitung beeinflusst werden, ist die Anwendbarkeit von Art. 146 StGB (Betrug) bzw. Art. 147 StGB (betrügerischer Missbrauch einer Datenverarbeitungsanlage) zu prüfen. Beide Delikte setzen eine Vermögensschädigung voraus¹⁴⁴. Zu denken wäre in diesem Kontext je nach den konkreten Umständen weiter an den Straftatbestand der Hehlerei (Art. 160 StGB). Tatobjekt dieses Tatbestands ist ausschliesslich eine körperliche Sache¹⁴⁵; da Bitcoins diese Voraussetzung nicht erfüllen, scheidet die Anwendung dieses Straftatbestands bereits aus diesem Grund aus.

[Rz 43] Es stellt sich die Frage, ob bei der genannten Ausgangslage im Hinblick auf die Straftatbestände des Betrugs und des betrügerischen Missbrauchs einer Datenverarbeitungsanlage eine Schädigung überhaupt eintreten kann. Verschiedene Aspekte sprechen dagegen. In faktischer Hinsicht ist zu beachten, dass sich Bitcoins durch ihre Anonymität auszeichnen¹⁴⁶. Es dürfte bereits aus diesem Grund in tatsächlicher Hinsicht regelmässig nicht leicht fallen, überhaupt festzustellen, welche individuelle Person effektiv (rechtlich) an den fraglichen Bitcoins berechtigt ist bzw. war. Selbst wenn eine derartige ursprüngliche Berechtigung festgestellt werden kann und sich im Einzelfall nachweisen lässt, dass eine unerlaubte Entwendung von Bitcoins stattgefunden hat und wem die Bitcoins eigentlich ursprünglich zustanden, erscheint es zweifelhaft, dass eine allfällig getäuschte Person eine Vermögensschädigung erleidet, wenn sie über die Berechtigung getäuscht wird und in der Folge ihre Leistung erbringt: Beim täuschenden Verkauf gestohlener Sachen wird die Tatbestandsvoraussetzung des Vermögensschadens dadurch erfüllt, dass die Sache nach objektiven Gesichtspunkten einen geringfügigeren Wert aufweist als der Käufer erwarten durfte, da die Sache mit sachenrechtlichen Herausgabeansprüchen belastet ist¹⁴⁷. Die Belastung mit derartigen Drittanprüchen erscheint bei unrechtmässig entwendeten Bitcoins zumindest zweifelhaft. Namentlich dürfte auf die

¹³⁵ Ebenso im Allgemeinen WEBER (Fn. 12), S. 130.

¹³⁶ Statt vieler allgemein SCHMID (Fn. 117), Art. 143 N 30 und daneben DONATSCH (Fn. 132), S. 174.

¹³⁷ Siehe für eine instruktive Übersicht verschiedener Auslegungen das Urteil des Obergerichts BE vom 13. November 2007 (publ. in forumpoenale 2008, S. 224–228), E. IV.2.b.

¹³⁸ Urteil des Obergerichts BE vom 13. November 2007 (Fn. 137), E. IV.2.b. Immerhin ist zu beachten, dass der Sicherheitsstandard auch vom Verwendungszweck abhängt. Bei PCs von Privatbenutzern mit vergleichsweise wenig sensitiven Daten ist daher ein anderer Standard anzulegen als bei einer Bank (SCHMID (Fn. 117), Art. 143 N 32). Der Standard dürfte aus diesem Grund jedoch erhöht sein, soweit der Benutzer besonders sensitive Daten speichert, d.h. z.B. Daten betreffend Bitcoins in einem besonders grossen Umfang.

¹³⁹ Siehe THE GUARDIAN (Fn. 128).

¹⁴⁰ Statt vieler DONATSCH (Fn. 132), S. 178.

¹⁴¹ Statt vieler TRECHSEL ET AL. (Fn. 115), Art. 143bis N 12.

¹⁴² TRECHSEL ET AL. (Fn. 115), Art. 144^{bis} N 2. Siehe zu Konkurrenzfragen DONATSCH (Fn. 132), S. 189. Eine Sachbeschädigung (Art. 144 StGB) wäre dagegen zu verneinen. Siehe dazu WEBER (Fn. 12), S. 130 f.

¹⁴³ Strafandrohung Diebstahl: Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe. Strafandrohung unbefugte Datenbeschaffung: Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe.

¹⁴⁴ Statt vieler DONATSCH (Fn. 132), S. 212 und S. 224.

¹⁴⁵ Grundlegend BGE 81 IV 156, S. 158 E. 1. Daneben statt vieler TRECHSEL ET AL. (Fn. 115), Art. 160 N 3 m.w.H.

¹⁴⁶ Vorstehend Kap. II.2.

¹⁴⁷ Statt vieler TRECHSEL ET AL. (Fn. 115), Art. 146 N 24 und DONATSCH (Fn. 132), S. 214 jeweils m.w.H.

Bitcoins das Besitzrecht nicht zur Anwendung gelangen¹⁴⁸. Eine Belastung mit (besitzrechtlichen) Ansprüchen scheidet daher aus, was dazu führt, dass die verwendeten unrechtmässig entwendeten Bitcoins über keinen geringfügigeren Wert verfügen als erwartet werden durfte. Aus diesen Gründen dürfte die Annahme einer Vermögensschädigung zu verwerfen sein, weshalb die Verwendung unrechtmässig erlangter Bitcoins zumindest unter dem Gesichtspunkt der vorgenannten Straftatbestände straflos sein dürfte¹⁴⁹.

3.7. Geldwäscherei

[Rz 44] Bitcoins zeichnen sich nach dem Vorgesagten insbesondere dadurch aus, dass sie eine hohe Anonymität gewährleisten¹⁵⁰. Während alle Bitcoin-Transaktionen (Transfer von Bitcoins von einem Benutzer zu einem anderen Benutzer) grundsätzlich¹⁵¹ vollständig transparent und allgemein einsehbar und damit auch nachvollziehbar sind, werden die Inhaber der Bitcoins in den öffentlich zugänglichen Daten, welche die Nachvollziehbarkeit der Transaktionen ermöglichen, lediglich durch eine Nummer bzw. einen Code repräsentiert.¹⁵² Die Inhaber der Bitcoins sind aus diesem Grund grundsätzlich anonym, da dieser Code nicht ohne weitere Informationen direkt einer individuellen Person zugeordnet

werden kann.¹⁵³ Hinzu kommt, dass sich echtes Geld zumindest derzeit faktisch¹⁵⁴ noch vollständig anonym in Bitcoins umwandeln lässt¹⁵⁵.

[Rz 45] Es darf davon ausgegangen werden, dass diese Form des elektronischen Gelds gerade aufgrund der Anonymität auch für zweifelhafte Aktivitäten verwendet wird¹⁵⁶. Die Kombination der vorgenannten Eigenheiten – Anonymität und potentielle Verwendung für bzw. im Zusammenhang mit illegalen Aktivitäten – legt die Prüfung der Anwendbarkeit des Straftatbestands der Geldwäscherei (Art. 305^{bis} StGB) nahe¹⁵⁷. Der Straftatbestand setzt unter anderem voraus, dass eine Handlung vorgenommen wird, «*die geeignet ist, die Ermittlung der Herkunft, die Auffindung oder die Einziehung von Vermögenswerten zu vereiteln*». Die entsprechende Handlung muss typischerweise geeignet sein, die Einziehung zumindest zu gefährden¹⁵⁸. Im Hinblick auf die angesprochenen Eigenheiten von Bitcoin muss davon ausgegangen werden, dass gewisse Handlungen im Zusammenhang mit Bitcoin (z.B. die Umwandlung von Bargeld in Bitcoins¹⁵⁹; nicht per se dagegen die Annahme von Bitcoins

¹⁴⁸ Entsprechende Bestimmungen stellen auf das Vorliegen einer Sache ab. Daten lassen sich gemäss h.L. nicht unter diesen Begriff subsumieren (statt vieler HÜRLIMANN-KAUP BETTINA/SCHMID JÖRG, Sachenrecht, 3. Aufl., Zürich 2009, N 7).

¹⁴⁹ Zu einer anderen Ansicht könnte gelangt werden, soweit der Argumentation in BGE 121 IV 26, 28 E. 2d) (betreffend täuschende Veräußerung einer ertrogenen Sache) gefolgt würde, wonach es genüge, wenn hinsichtlich der Herausgabe des Gegenstands eine unsichere Zivilrechtslage bestehe, welche für den Dritterwerber ein erhebliches Risiko berge, in eine zivilrechtliche Auseinandersetzung verstrickt zu werden und den Gegenstand herausgeben zu müssen. Eine derartige unsichere Zivilrechtslage könnte im Fall von entwendeten Bitcoins ggf. bejaht werden.

¹⁵⁰ Vorstehend Kap. II.2.

¹⁵¹ Es ist darauf hinzuweisen, dass bereits Dienstleistungen angeboten werden, welche darauf abzielen, diese Transparenz faktisch zu begrenzen (sog. «Mixing services»). Die Funktionsweise lässt sich an einem einfachen Beispiel illustrieren: A möchte B Bitcoins übertragen (z.B. als Gegenleistung für die Übertragung einer gewissen, möglicherweise illegalen, Ware). A und B möchten wechselseitig nicht miteinander in Verbindung gebracht werden. Um dies sicherzustellen, verwenden sie (ggf. gegen ein Entgelt) den Service Z. A überträgt Z die Bitcoins; A hat bei Z sodann ein Guthaben in der Höhe der genannten Bitcoins und erhält einen Zugangscode, der einmal zum Bezug von Bitcoins in entsprechender Höhe verwendet werden kann. A teilt B den Zugangscode mit und B bezieht bei Z Bitcoins im Umfang des Guthabens von A. Die entsprechenden Bitcoins stammen dabei jedoch nicht von A selbst, sondern von anderen Benutzern, die die Dienstleistung von Z ebenfalls benutzen möchten und Bitcoins an Z übertragen. Wirtschaftlich findet damit eine Übertragung von Bitcoins von A zu B statt. Diese Übertragung ist jedoch nicht direkt transparent bzw. nachvollziehbar (Beispiel angelehnt an BITCOIN WEEKLY, The Battle is On – Silk Road vs. Government, and Bitcoin Anonymity, <http://bitcoinweekly.com/articles/the-battle-is-on-silk-road-vs-government-and-bitcoin-anonymity> [besucht am 5. Mai 2012]).

¹⁵² Vorstehend Kap. II.2.

¹⁵³ Vorstehend Kap. II.2.

¹⁵⁴ Ob ein derartiges (faktisch derzeit im Ausland erfolgreiches) Vorgehen nach dem anwendbaren Recht rechtlich zulässig ist, muss an dieser Stelle offen bleiben.

¹⁵⁵ Als Beispiel lässt sich der Service «Mt. Gox» anführen, welcher (in begrenztem Umfang) die (anonyme) postalische Einsendung von US-Dollar zwecks Umwandlung in Bitcoins zulässt (vgl. BITCOIN MORPHEUS, How to buy Mt Gox USD with cash in the mail, http://bitcoinmorpheus.tumblr.com/how_to_buy_mt_gox_usd_with_cash_in_the_mail [besucht am 5. Mai 2012]).

¹⁵⁶ Hinzuweisen ist insb. auf «Silk Road». Hierbei handelt es sich um einen nicht leicht zugänglichen Online-Marktplatz, auf welchem insbesondere illegale Waren und Dienstleistungen ausgetauscht werden können. Als Zahlungsmittel dienen hierbei aufgrund der Anonymität Bitcoins (siehe dazu statt vieler DIE ZEIT (Fn. 5); DAVIS (Fn. 23), 66 ff.; GRINBERG (Fn. 15), S. 28). Daneben ist der Sachverhalt, der dem Urteil des Landgerichts Düsseldorf vom 22. März 2011 (publ. in ZUM [= Zeitschrift für Urheber- und Medienrecht] 2011, S. 675–679) betreffend Erpressung, zu Grunde liegt, interessant: Der Erpresser hat zur Verschleierung seiner Identität ein Zahlungsmittel gewählt, mittels welchem sich Zahlungsvorgänge weitgehend anonymisieren lassen (es wurden dabei jedoch nicht Bitcoins eingesetzt). Siehe hierzu auch GERCKE MARCO, Die Entwicklung des Internetstrafrechts 2010/2011, ZUM 2011, S. 609–623, insb. S. 619 f. m.w.H., wobei auch ein Bezug zu Bitcoins hergestellt wird. Schliesslich scheinen auch Anarchisten für Bitcoin Verwendung zu finden (vgl. BBC, Five charged over «plot to blow up Ohio bridge», <http://www.bbc.co.uk/news/world-us-canada-17913139> [besucht am 5. Mai 2012] und die diesbezügliche eidesstattliche Erklärung eines Ermittlers, http://www.cbsnews.com/htdocs/pdf/Wright_complaint_affadavit_050112.pdf [besucht am 5. Mai 2012], S. 6 N 27, wonach Anarchisten, die die Sprengung einer Brücke geplant hätten, darüber gesprochen hätten, Bitcoin für finanzielle Transaktionen zu verwenden um keine Spuren zu hinterlassen).

¹⁵⁷ Ähnlich auch GRINBERG (Fn. 11), S. 204. Im Zusammenhang mit «Silk Road» (siehe dazu vorstehend Fn. 156) wurden Bitcoins von us-amerikanischen Politikern bereits als «an online form of money laundering used to disguise the source of money» qualifiziert (siehe etwa THE INDEPENDENT (Fn. 7)).

¹⁵⁸ Statt vieler TRECHSEL ET AL. (Fn. 115), Art. 305^{bis} N 17.

¹⁵⁹ Dies aufgrund der Überlegung, dass auch das Wechseln von normalem

als Gegenleistung¹⁶⁰) in den Anwendungsbereich des Geldwäschereistraftatbestands fallen könnten. Zu berücksichtigen ist dabei insbesondere, dass traditionell bereits jeder Transfer von kontaminierten Geldwerten ins Ausland als Geldwäschereihandlung qualifiziert wird, da die Einziehung hierdurch erschwert wird¹⁶¹.

IV. Fazit

[Rz 46] Bitcoin ist eine neuartige, digitale, dezentralisierte und teilweise anonyme elektronische Währung, die seit ihrer Entstehung auf reges Interesse gestossen ist. Sie kann effektiv verwendet werden und ihre Währungseinheiten, welche wertmässig einer hohen Volatilität ausgesetzt sind, können durch eigenständige Erschaffung oder Tausch erworben werden.

[Rz 47] Diese neuartige Währung wirft – unabhängig davon, ob sie längerfristig Bestand haben wird, was sich derzeit nicht verlässlich abschätzen lässt – vielfältige rechtliche Fragen auf. Bereits eine erste Analyse zeigt, dass Bitcoin in währungsrechtlicher Hinsicht grundsätzlich zulässig ist. Dies gilt auch unter Berücksichtigung des Lotterierechts, obwohl fälschlicherweise regelmässig der Vorwurf erhoben wird, Bitcoin stelle eine unzulässige Lotterie bzw. ein Schneeballsystem dar. Darüber hinaus wäre eine allfällige Zwangsvollstreckung betreffend einer Forderung, die auf Bitcoins lautet, auf dem Realvollstreckungs- und nicht dem Betreibungsweg zu vollstrecken.

[Rz 48] In strafrechtlicher Hinsicht deuten erste Überlegungen und Erkenntnisse darauf hin, dass sowohl die Erschaffung des Systems an sich als auch die Erzeugung einzelner Bitcoins nicht strafbar ist. Selbiges gilt grundsätzlich für die Verwendung und den Tausch von Bitcoins, wobei nicht auszuschliessen ist, dass der Tausch einer staatlichen Währung in Bitcoin sowie die dafür nötigen Dienstleistungen unter dem Gesichtspunkt des Geldwäschereitratbestandes problematisch sein können. Die wenig wahrscheinliche Fälschung von Bitcoins stellt klarerweise kein Geldfälschungsdelikt dar. Auch das Vorliegen eines Urkundendelikts dürfte zu verneinen sein. Die unrechtmässige Entwendung von Bitcoins wäre primär als unbefugte Datenbeschaffung und nicht als Diebstahl zu qualifizieren. Die Verwendung unrechtmässig erlangter Bitcoins erfüllt ebenfalls keinen Straftatbestand.

Jean-Daniel Schmid, M.A. HSG (Rechtswissenschaft), Fischbach-Göslikon, Rechtsanwalt, Doktorand an der Universität St. Gallen. Alexander Schmid, M.A. HSG (Rechtswissenschaft), Unterengstringen, Rechtsanwalt bei *epartners Rechtsanwälte* in Zürich (www.epartners.ch).

Die Autoren danken Herrn Reuben Grinberg, M.Sc. (Computer Science), J.D. (Yale) für die wertvollen Hinweise.

* * *

Geld den Straftatbestand der Geldwäscherei erfüllen kann (vgl. etwa BGE 122 IV 211, 215 f. E. 2c); Urteil des Bundesgerichts 6B_321/2010 vom 25. August 2010, E. 3.1).

¹⁶⁰ Die Annahme von kontaminierten Geldwerten ist für sich allein noch keine tatbestandsmässige Geldwäschereihandlung (Urteil des Bundesgerichts 6S.595/1999 vom 24. Januar 2000, E. 2d/aa); ferner statt vieler DONATSCH/WOHLERS (Fn. 106), S. 481).

¹⁶¹ Statt vieler TRECHSEL ET AL. (Fn. 115), Art. 305^{bis} N 18.