SCHWEIZERISCHE BANKRECHTSTAGUNG 2018

Institut für Bankrecht, Universität Bern

Unautorisierte Zahlungen mit virtuellen Währungen?

Martin Hess / Stephanie Lienhard

In: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018

ISBN 978-3-7190-4138-0

Unautorisierte Zahlungen mit virtuellen Währungen?

Martin Hess/Stephanie Lienhard, Zürich*

Inhaltsverzeichnis

* Dr. iur. Martin Hess, Rechtsanwalt, Partner bei Wenger & Vieli. MLaw Stephanie Lienhard, Rechtsanwältin.

I. Einleitung

Ende der 1. Maiwoche 2018 gab es gemäss Coinmarketcap[1] 1'614 virtuelle Währungen. Deren Marktkapitalisierung betrug zu diesem Zeitpunkt USD 457'141'660'679.[2]

Bitcoin (BTC) – die erste und bekannteste virtuelle Währung – war ursprünglich als Zahlungsmittel geschaffen worden.[3] In der Praxis sieht die Nutzung als Zahlungsmittel heute folgendermassen aus:

– Die Stadt Zug entschied im Mai 2016 als erste staatliche Institution weltweit, Bitcoin in begrenztem Umfang (bis CHF 200) als Zahlungsmittel zu akzeptieren.[4] Bei der Einwohnerkontrolle der Stadt Zug wurden von Mai 2016 bis Februar 2018 rund 50 Transaktionen mit Bitcoin beglichen. Das Zuger Handelsregisteramt akzeptiert seit November 2017, dass Dienstleistungen mit Bitcoin und Ether bezahlt werden können.[5] Bis Februar 2018 gab es nur drei Zahlungen in Höhe von gesamthaft 1'890 Franken, die beim Handelsregisteramt mit Bitcoin und Ether beglichen wurden. Zudem akzeptiert das Amt, dass bei der Gründung von Aktiengesellschaften und GmbH das Kapital mit Kryptowährungen liberiert werden kann. Kryptowährungen gelten ebenso als Sacheinlage wie beispielsweise Autos oder Mobiliar.[6]

---

1 Coinmarketcap ist ein Dienstleister, der alle gehandelten virtuellen Währungen auflistet: <https://coinmarketcap.com/>.

2 Vgl. <https://coinmarketcap.com/de/all/views/all/>.

3 NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System.

4 <http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/newsarchiv/?action=showinfo&info_id=351680>.

5 <https://www.zg.ch/behoerden/volkswirtschaftsdirektion/handelsregisteramt/aktuell/handelsregisteramt-zug-akzeptiert-kryptowaehrungen-bitcoin-und-ether-als-zahlungsmittel>.

6 Neue Zürcher Zeitung (NZZ) vom 10. Februar 2018, «Die Bitcoinblase platzt – im Zuger Crypto Valley wachsen die Bedenken», <https://www.nzz.ch/schweiz/die-bitcoin-blase-platzt-im-zuger-crypto-valley-wachsen-die-bedenken-ld.1354992>.

– Pro Tag werden in Deutschland 70 Mio. Zahlungen getätigt, weltweit mit Bitcoin nur ca. 300'000.[7]

Folglich finden virtuelle Währungen wie Bitcoin und Ether in der Regel keine Verwendung als Zahlungsmittel, sondern sind Anlage- und Spekulationsinstrumente. Demzufolge sind Transaktionen in virtuellen Währungen häufig, Zahlungen nicht.

II. Geld und Währungen

1. Grundlagen der geltenden Geld- und Währungsordnung

Die Währungshoheit, d.h. die Kompetenz, Regeln betreffend das Geld- und Währungswesen zu erlassen, liegt in der Regel in staatlichen Händen, in der Schweiz beim Bund.[8]

Der Begriff des «Geldes» ist unscharf. Gemäss der allgemeinen Geldtheorie hat Geld drei Funktionen. Geld ist:

- ein Zahlungsmittel,
- eine Recheneinheit (Vergleichsmassstab), und
- ein Wertaufbewahrungsmittel (Sparen).[9]

«Geld» in seiner konkreten Funktion als Zahlungsmittel wird in Art. 2 des Bundesgesetzes über die Währung und die Zahlungsmittel[10] definiert als die vom Bund ausgegebenen Münzen, die von der Schweizerischen Nationalbank (SNB) ausgegebenen Banknoten und die auf Franken lautenden Sichtguthaben bei der SNB.

Eine weitere Art von «Geld» ist das Buchgeld der Geschäftsbanken. Die Geschäftsbanken halten Geld auf Bankkonten (sog. Buchgeld). Buchgeld entsteht durch Einzahlung von Bargeld auf Bankkonti oder mittels Kreditvergabe, indem die Banken den Kunden die als Kredit gewährten Beträge auf deren Konto gutschreiben. Buchgeld ist immer eine Forderung gegen-

---

7 Neue Zürcher Zeitung (NZZ) vom 15. Februar 2018, «Kryptowährungen: ‹Nicht auf jede Neuerung muss ein Verbot folgen›», <https://www.nzz.ch/wirtschaft/nicht-auf-jede-neuerung-muss-ein-verbot-folgen-ld.1357501>.

8 Art. 99 Abs. 1 BV (SR 101).

9 Bericht des Bundesrates zu virtuellen Währungen vom 25. Juni 2014, S. 7; CARSTENS, Money, S. 2 ff.

10 WZG (SR 941.10).

über dem kontoführenden Finanzinstitut und damit von dessen Bonität abhängig.[11]

Währung bezeichnet das hoheitlich geordnete Geldwesen eines Staates einschliesslich aller Regelungen zur Sicherung der Geldwertstabilität (Währungsverfassung), die Denominierung, die befreiende Wirkung bei Verwendung als Zahlungsmittel und die allfällige Annahmepflicht (Zwangskurs).[12]

Eine Währung setzt sich nur durch, wenn sie Vertrauen geniesst:

> *«History shows that money as a convention needs to have a basis of trust, supported by some form of institutional arrangement.»*[13]

2. Merkmale von virtuellen Währungen

a) Rechtliche Einordnung

Virtuelle Währungen sind digitale Darstellungen von im Internet handelbaren Werten, die die Funktion von Geld übernehmen, aber nicht als gesetzliche Zahlungsmittel akzeptiert sind.[14]

Virtuelle Währungen vermitteln keinen Anspruch gegen einen Herausgeber.[15]

Die Volatilität[16] der virtuellen Währungen verunmöglicht den Gebrauch als Wertmassstab. Der Wert von Bitcoin und Ether wird nach wie vor in gesetzlichen Zahlungsmitteln angegeben. Die Volatilität gefährdet auch die Verwendung als Wertaufbewahrungsmittel.[17]

Virtuelle Währungen sind nicht gesetzliche Zahlungsmittel i.S. von Verfassung und Gesetz (Art. 99 BV, Art. 1 und 2 WZG und Art. 84 OR).[18]

Das Entwickeln und Anbieten privater (d.h. nicht gesetzlicher) Zahlungsmittel verstösst nicht gegen das Schweizer Währungsrecht.[19] Zivilrecht-

---

11 GIOVANOLI, FS KLEINER, S. 87 ff.

12 ZELLWEGER-GUTKNECHT, Digitale Landeswährung, S. 5.

13 CARSTENS, Money, S. 3.

14 HESS/SPIELMANN, Cryptocurrencies, S. 175 m.w.H.

15 FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs) vom 16. Februar 2018, S. 2.

16 HESS/SPIELMANN, Cryptocurrencies, S. 174 f.

17 CARSTENS, Money, S. 9 f.

18 GRÜNEWALD, Virtuelle Währungen, S. 93 ff. Siehe dazu auch den Bericht des Bundesrates zu virtuellen Währungen vom 25. Juni 2014, S. 5 ff.

19 GRÜNEWALD, Virtuelle Währungen, S. 98 Fn. 21.

lich sind private Zahlungsmittel – u.a. Buchgeld, WIR-Geld, virtuelle Währungen – daher nicht verboten, sofern die Beteiligten in deren Verwendung als Zahlungsmittel einwilligen. Anwendbar auf diese Fälle sind die Bestimmungen des Vertragsrechts, insbesondere des Obligationenrechts.[20]

Virtuelle Währungen sind daher Vermögenswerte und Zahlungsmittel, sofern Letzteres zwischen den Parteien vereinbart worden ist.[21]

b) Die verschiedenen Arten des Vertrauens in Währungen und Zahlungsmittel[22]

Ein horizontales Vertrauensverhältnis kann zwischen Individuen bestehen, beispielsweise bei einem Tauschgeschäft oder beim Wechsel, der letztlich den persönlichen Kredit des Ausstellers verbrieft.

Ein vertikales Vertrauensverhältnis besteht zwischen Finanzinstituten und deren Kunden. Das Vertrauen in die Finanzinstitute wird durch die Rechtsordnung gestärkt.

In der digitalen Ökonomie gilt das verteilte Vertrauen (*distributed trust/distributed consensus*).[23] Dieses stützt sich auf Algorithmen, digitale Protokolle sowie Netzwerke voller Daten.

III. Technische Grundlagen

1. Blockchain Technologie als Basis virtueller Währungen

Die meisten virtuellen Währungen basieren grundsätzlich auf der sog. Blockchain Technologie.[24] Dabei handelt es sich um ein dezentrales Netz-

---

20 Bericht des Bundesrates zu virtuellen Währungen vom 25. Juni 2014, S. 7, 10; HESS/KALBERMATTER/WEISS, SK FinfraG, Art. 81 N 22 Fn. 46.

21 HESS/SPIELMANN, Cryptocurrencies, S. 175 f.

22 Neue Zürcher Zeitung (NZZ) vom 3. Februar 2018, S. 29, «Wie vertraut man einem Algorithmus?».

23 SZABO, Trusted Third Parties, Abschnitte «TTP Minimizing Protocols» und «Conclusion». Zum Distributed Consensus siehe unten Abschnitt III. 1.

24 Ein gegenteiliges Beispiel ist IOTA: <https://iotasupport.com/whatisiota.shtml>. Das zugrundeliegende Protokoll orientiert sich zwar ebenfalls an der Distributed Ledger Technologie, die Transaktionen werden jedoch parallel über einen sog. Tangle – ein directed acyclic graph (DAG) – bearbeitet und der Sender einer Transaktion ist gleichzeitig für die Verifizierung von zwei vorhergehenden Transaktionen zuständig, was das

werk, welches in der einen oder anderen Form Transaktionen verifiziert, in Blöcken zusammenfasst und in der Folge im jeweiligen Block registriert. Bei der Bitcoin Blockchain verifizieren sog. Full Blockchain Nodes[25] unabhängig voneinander und anhand einer langen Liste von Kriterien die einzelnen Transaktionen, bevor sie diese ans Netzwerk weiterleiten.[26] In der Folge werden diese verifizierten Transaktionen durch sog. Miner in einen neuen Block zusammengefasst, welcher erst nach erfolgreicher Berechnung eines komplizierten Algorithmus den sog. Proof of Work und damit Gültigkeit erlangt.[27] Schliesslich verifizieren die Nodes den neuen Block erneut unabhängig voneinander und anhand einer langen Liste von Kriterien, bevor sie ihn im Netzwerk verteilen und in ihre eigene Blockchain-Kopie aufnehmen.[28]

Der Prozess, durch welchen sich das dezentrale Netzwerk von Teilnehmern auf einen einzigen gültigen Status der Blockchain einigt, unterscheidet sich teilweise zwischen den verschiedenen virtuellen Währungen. Die auf Bitcoin basierenden Währungen wie beispielsweise Litecoin[29] oder das Monero zugrunde liegende CryptoNote-Protokoll[30] sowie zurzeit auch noch Ethereum stützen sich auf den vorgängig umschriebenen Proof of Work. Daneben gibt es zahlreiche Varianten von Konsens-Algorithmen, welche auf unterschiedlich ausgestalteten Proposal- und Voting-Funktionen der Nodes basieren. Wenn das Gewicht eines Proposals oder eines Votes davon abhängig ist, wie viele Einheiten der jeweilige Node von der blockchain-eigenen virtuellen Währung besitzt bzw. als Depot hinterlegt, spricht man vom sog. Proof of Stake.[31] Des Weiteren gibt es auch einen sog. Proof of Importance,

---

Senden erst ermöglicht. Für das technische Whitepaper siehe: <http://iotatoken.com/IOTA_Whitepaper.pdf>.

25 Diese Nodes speichern jeweils die gesamte Blockchain seit der ersten Transaktion im ersten Block; vgl. hierzu ANTONOPOULOS, Mastering Bitcoin, S. 145 f.

26 ANTONOPOULOS, Mastering Bitcoin, S. 177 f.

27 ANTONOPOULOS, Mastering Bitcoin, S. 179 f., 188 f.

28 ANTONOPOULOS, Mastering Bitcoin, S. 197 ff.

29 <https://litecoin.org>.

30 Siehe dazu <https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf>.

31 Für einen anschaulichen Vergleich zwischen Proof of Work und Proof of Stake siehe: ROSIC, Proof of Work vs Proof of Stake; für die bei Ethereum geplante Implementierung des Proof of Stake basierten Casper Systems: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ> sowie <https://github.com/ethereum/research/blob/master/p

bei welchem die Transaktionshäufigkeit sowie das Transaktionsvolumen für die Schaffung eines Blocks massgebend ist.[32]

Was aber wohl die meisten virtuellen Währungen grundsätzlich gemeinsam haben, ist die Datenstruktur eines Blocks. So besteht ein Block u.a. aus der Liste aller in ihm zusammengefassten Transaktionen[33] sowie dem Hash[34] des vorhergehenden Blockes. Dieser Hash wiederum beinhaltet die Datenstruktur des gesamten letzten Blockes und jeder neue Block wird dadurch mit dem vorherigen insoweit verbunden, als der neue Datensatz immer auch den Hash und damit die Transaktionsdaten des vorhergehenden beinhaltet. Eine Änderung in Block x würde also auch alle darauffolgenden Blöcke verändern.[35]

2. Kryptographisch ausgestaltete Transaktionen

Grundlage für alle Transaktionen über ein Blockchain Netzwerk sind kryptographische Schlüssel und die entsprechenden Funktionen, wobei die Ausgestaltung im Detail variieren kann. Basis bildet in der Regel ein Schlüsselpaar, bestehend aus einem Private und einem Public Key. Der Private Key besteht aus einer beliebig festgelegten Zahlenreihenfolge. Der Public Key errechnet sich mittels einer mathematischen Formel – genauer gesagt einer elliptischen Kurve – aus dem Private Key. Ähnliches geschieht mit der Bit-

apers/casper-basics/casper_basics.pdf>; für ein weiteres Beispiel: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#consensus-algorithm-bft-dpos>, <https://cardanodocs.com/cardano/proof-of-stake>.

32 <https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf>.

33 Diese werden oftmals mittels eines sog. Merkle Trees in einem kleineren Datenformat zusammengefasst; für Bitcoin siehe ANTONOPOULOS, Mastering Bitcoin, S. 160 f., 164 ff.; DECKER/WATTENHOFER, Information Propagation, S. 2 f.

34 Ein Hash Algorithmus ist eine Einwegfunktion, die eine beliebig grosse Eingabemenge bzw. Zeichenfolge in einem digitalen Fingerabdruck in Form einer kleineren, fixen Zielmenge bzw. Zeichenfolge abbildet; ANTONOPOULOS, Mastering Bitcoin, S. 71, 188. Siehe auch die Einträge bei WIKIPEDIA: <https://de.wikipedia.org/wiki/Hashfunktion>; <https://de.wikipedia.org/wiki/Kryptologische_Hashfunktion>.

35 ANTONOPOULOS, Mastering Bitcoin, S. 159 ff.; <https://bitcoin.org/en/developer-guide#block-chain>.

coin-Adresse, welche – durch eine Hash[36] Funktion – grundsätzlich aus dem Public Key generiert wird.[37]

Die Bitcoin-Adresse ist derjenige Datensatz, welcher als Empfänger für eine Transaktion kommuniziert werden kann, während mit dem Private Key eingehende oder ausgehende Transaktionen verifiziert werden.[38] Die mathematischen Formeln bewirken, dass anhand des Private Keys der Public Key generiert werden kann und darauf basierend die Bitcoin-Adresse; umgekehrt ist dies allerdings nicht möglich. Dasselbe geschieht mit sog. Signaturen, welche vom Private Key abgeleitet werden.[39]

Die vom Private Key abgeleitete Signatur wird für jede Transaktion wieder neu generiert, kann aufgrund der mathematischen Abhängigkeit zwischen Private und Public Key immer mit dem korrespondierenden Public Key in Verbindung gebracht werden und lässt gleichzeitig aber keinen Rückschluss auf den Private Key zu. Die Signatur ermöglicht somit, die Verfügungsgewalt an einzelnen Werten aufzuzeigen, ohne den Private Key preiszugeben.[40]

IV. Unautorisierte Zahlungen

1. Zentralisiert

a) Autorisierung, Authentisierung und Authentifizierung

Finanzinstitute halten die Vermögenswerte der Kunden auf Konti oder in Depots. Der Kunde kann darüber verfügen, wenn er sich als Berechtigter ausweist und eine entsprechende Weisung erteilt. Dieser Prozess setzt sich zusammen aus «Autorisierung», «Authentisierung» und «Authentifizierung».[41]

Die Authentisierung stellt den Nachweis einer Person dar, dass sie tatsächlich diejenige Person ist, die sie vorgibt zu sein.

---

36 Vgl. Fn. 34.

37 Vorliegend dient Bitcoin als Anschauungsbeispiel. Zum Ganzen daher: ANTONOPOULOS, Mastering Bitcoin, S. 61 ff., 65, 70 f.

38 ANTONOPOULOS, Mastering Bitcoin, S. 61, 63, 70.

39 ANTONOPOULOS, Mastering Bitcoin, S. 63 f., 65 ff., 70 ff.

40 ANTONOPOULOS, Mastering Bitcoin, S. 62.

41 AGNIESZKA CZERNIK, Authentisierung, Authentifizierung und Autorisierung.

Die Authentifizierung stellt eine Prüfung der behaupteten Authentisierung dar. In den Worten der PSD 2 ist es «*das Verfahren, mit dessen Hilfe ein Finanzinstitut die Identität eines Zahlungsdienstnutzers oder die Verwendung eines Zahlungsinstruments überprüfen kann*».[42]

Die Autorisierung ist die Einräumung von speziellen Rechten. War die Identifizierung einer Person erfolgreich, heisst es noch nicht automatisch, dass diese Person bereitgestellte Dienste und Leistungen nutzen darf. Darüber entscheidet die Autorisierung. Beispielsweise gilt ein Zahlungsvorgang als autorisiert, wenn der Zahler diesem zugestimmt hat (Art. 64 PSD 2).

In der zentralisierten Struktur mit einzeln kontoführenden Finanzinstituten erfolgen Autorisierung, Authentisierung und Authentifizierung jeweils im bilateralen Verhältnis zwischen Finanzinstitut und Kunde. Die entsprechenden Regeln sind in Verträgen und allgemeinen Geschäftsbedingungen festgehalten. Bei fehlerhaften Vorgängen betreffend Autorisierung, Authentisierung und Authentifizierung regeln Gesetz[43] oder Gerichtspraxis[44] die Rechtsfolgen, insbesondere die Haftung.

b) Widerruf

Im geltenden Schweizer Recht ist der Widerruf geregelt in Art. 470 Abs. 2bis OR für die bargeldlose Überweisung[45] und in Art. 15 Abs. 3 BEG für Transaktionen in Bucheffekten[46]:

- Nach Art. 470 Abs. 1 OR kann eine Anweisung grundsätzlich jederzeit widerrufen werden, es sei denn, der Angewiesene habe dem Anweisungsempfänger Annahme erklärt (Art. 470 Abs. 2 OR). Art. 470 Abs. 2bis OR lässt für Anweisungen im bargeldlosen Zahlungsverkehr Unwiderruflichkeit mit der Belastung des Kontos des Zahlers durch den angewiesenen Finanzintermediär eintreten. Vorbehalten bleiben abweichende Regeln von Zahlungssystemen.

---

42 Art. 4 Ziff. 29 PSD 2.

43 Zu den Art. 73 und 74 PSD 2 siehe EMMENEGGER, Eckpunkte, S. 47 ff.; zu den entsprechenden Bestimmungen in der PSD 1 siehe HESS, Euro-Zahlungen, S. 88 ff.

44 HESS, Euro-Zahlungen, S. 90 ff.

45 HESS, Euro-Zahlungen, S. 76 ff.; HESS/STÖCKLI, Bucheffektengesetz, S. 109 f.

46 HESS/ZBINDEN, BEG-Kommentar, N 31 ff. zu Art. 15 BEG; HESS/STÖCKLI, Bucheffektengesetz, S. 109.

- Nach dem Wortlaut von Art. 15 Abs. 3 BEG ist ein Widerruf immer dann nicht mehr möglich, sobald das Effektenkonto des Kontoinhabers belastet wurde.

Sowohl im bargeldlosen Zahlungsverkehr wie bei der Effektenabwicklung erfolgt der Widerruf gegenüber dem kontoführenden Finanzinstitut. Die Regeln betreffend Widerruf sind auf die heutige zentralisierte Finanzmarktinfrastruktur zugeschnitten, welche auf vertikalem Vertrauen basiert. Die Finanzinstitute führen zentral Konti und sind somit Ansprech- und Vertragspartner des Kunden.

Es besteht vertikales Vertrauen. Mit Blick auf das verteilte Vertrauen bei virtuellen Währungen stellt sich die Frage: An wen soll man sich bei einem Widerruf halten?

c) Stornierung

In der zentralisierten Struktur der Finanzwelt ist die Stornierung einer infolge fehlender oder unwirksamer Weisung/Anweisung zu Unrecht erfolgten Transaktion durch das kontoführende Finanzinstitut möglich. Im Effektenbereich bilden Art. 27/28 BEG[47] die Rechtsgrundlage, im Zahlungsverkehr ist die Stornierungsmöglichkeit zumeist stillschweigender Vertragsinhalt.[48]

Auch bezüglich der Stornierung stellt sich für ein dezentrales Netzwerk unweigerlich die Frage nach deren Praktikabilität: Wer ist autorisiert und in der Lage, eine Transaktion rückgängig zu machen, insbesondere angesichts der erschwerten Abänderlichkeit der auf der Blockchain registrierten Daten?[49]

2. Dezentral

a) Verifizierung

Wie ausgeführt wurde, werden Transaktionen in virtuellen Währungen regelmässig mittels einer vom Private Key abgeleiteten Signatur verifiziert. Der Inhaber des Private Keys kann somit eine Transaktion auslösen. Erfolgt diese Verifizierung, wird die Anzahl der von der Transaktion betroffenen

47 HESS/STÖCKLI, Bucheffektengesetz, S. 110 ff.; WEBER, BEG Kommentar zur Art. 27 und 28 BEG, passim.

48 BUIS, Stornorecht, S. 126, 128.

49 Abschnitt IV.2.c nachstehend.

virtuellen Währungen der mit dem Private Key verbundenen Bitcoin-Adresse zugewiesen. Die Transaktion ist im Grundsatz abgeschlossen, sobald die Mehrheit der am Netzwerk Beteiligten diese Zuweisung akzeptiert und in die aktuelle Version der Blockchain aufnimmt.

Wird die Transaktion von den Netzwerkteilnehmern nicht akzeptiert, gelangt sie nicht in einen Block und/oder wird sie nicht von der Mehrheit der Nodes in die Blockchain aufgenommen, gilt die entsprechende Transaktion als nicht vorhanden. Damit würde zwar eine verifizierte Zahlung vorliegen, sie hätte für das Netzwerk aber keinerlei Relevanz.

Wenn eine Transaktion mittels eines fremden, allenfalls gestohlenen Private Keys signiert wird, ist die Ausgangslage vorderhand ähnlich wie bei einer traditionellen Bankzahlung: Der die Transaktion Auslösende gibt sich mittels des von der Bank bzw. dem Netzwerk anerkannten Verifizierungsverfahrens als Berechtigter aus und wird auch als solcher anerkannt. Denn das Netzwerk verifiziert eine Transaktion nur anhand der vom Private Key abgeleiteten, korrekten Signatur. Wird eine Transaktion auf Basis eines kryptographisch richtigen Private Keys signiert, werden die Mehrzahl der Nodes die Transaktion verifizieren und im Netzwerk verteilen. Somit kann ein Verlust des Verifizierungsmerkmals, also des Private Keys, bei genauer Betrachtung auch bei Transaktionen in virtuellen Währungen zu einer unautorisierten Zahlung führen. Wie zu zeigen sein wird, unterscheiden sich allerdings die Folgen einer unautorisierten Zahlung in diesem Bereich diametral vom Konzept, welches dem traditionellen Zahlungsverkehr zugrunde liegt.[50]

b) Cold Storage und Co.

Damit sich niemand eines fremden Private Keys bedient, gibt es mittlerweile zahlreiche Varianten, einen Verlust mit grösstmöglicher Sicherheit zu verhindern.

Wie bereits ausgeführt, können virtuelle Währungen an sich nicht gehalten oder verwahrt werden, da es sich hierbei um öffentlich zugängliche Datenstränge handelt. Will man seinen Bestand an virtuellen Währungen sicher verwahren, so ist hierfür der Private Key entsprechend sicher aufzubewahren.

Während eine starke Verschlüsselung und ein Backup der Wallet bzw. der darin abgespeicherten Private Keys stark an andere passwortgeschützte

[50] Abschnitt IV.2.c/d nachstehend.

Konten erinnert, scheint das sog. Cold Storage trotz Digitalisierung das Rad der Zeit wieder um Jahrzehnte zurückzudrehen. Bei der Cold Storage werden die Private Keys offline, also ohne Zugang zum Internet verwahrt. Dies soll insbesondere Hackerangriffen vorbeugen. Noch mehr Sicherheit wird erreicht, wenn man bereits bei der Schaffung des Private Keys auf eine Verbindung zum Internet verzichtet. [51]

Für den täglichen Gebrauch ist diese Art der Verwahrung jedoch mühsam, da Transaktionen nur über eine Internetverbindung möglich sind. Dies führt dazu, dass die Guthaben in virtuellen Währungen oft aufgeteilt werden in einen grossen Betrag, welcher offline als eine Art Sparguthaben lagert und in einen kleineren Betrag für den täglichen Gebrauch mittels einer sog. Hot Wallet, welche mit dem Internet verbunden ist.[52]

Zahlreiche Handelsplattformen (sog. Cryptocurrency Exchanges) geben an, dass sie die Mehrheit der Kundenvermögen offline verwahren.[53] Allerdings gibt es immer wieder Berichte von erfolgreichen Hackerangriffen auf Hot Wallets und die Verwahrung von Kundenvermögen in Cold Wallets scheint sich noch nicht überall durchgesetzt zu haben.[54]

Cold Storage kann beinahe klassisch über ein sog. Paper Wallet erfolgen. Dabei sind der Private und Public Key auf einem Stück Papier aufgedruckt und oftmals noch mit einem QR-Code versehen, damit ein Einlesen mittels eines digitalen Gerätes möglich wäre.[55] Da auf dem Papier aber sämtliche relevanten Daten ersichtlich sind, muss das Papier entsprechend sicher auf-

---

51 <https://en.bitcoin.it/wiki/Cold_storage>; BAJPAJ, What Is Cold Storage For Bitcoin; <https://www.bitcoin.com/guides/setting-up-your-own-cold-storage-bitcoin-wallet>; ANTONOPOULOS, Mastering Bitcoin, S. 104 f.

52 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin.

53 So z.B. Kraken <https://www.kraken.com/en-us/security/practices>; Bitfinex <https://www.bitfinex.com/legal/security_policy>; Coinbase <https://www.coinbase.com/security>; Bittrex: <https://support.bittrex.com/hc/en-us/articles/115003684411>.

54 Für den Hack der japanischen Cryptocurrency Exchange Coincheck siehe ALPEYEV/NAKAMURA, How to Launder $500 Million in Digital Currency; WELTER, Hackerangriff trifft japanische Krypto-Börse; im Fall BitGrail besteht zumindest das Risiko, dass die Verwahrung in einer Hot Wallet den Hack ermöglicht hatte: YOUNG, BitGrail Vs. Nano.

55 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin; ANTONOPOULOS, Mastering Bitcoin, S. 104 ff. Für mögliche Tools zur Generierung der Keys siehe <https://tools.bitcoin.com/paper-wallet>; <https://walletgenerator.net>.

bewahrt und vor Blicken und Zugang Dritter geschützt werden.[56] Um die Sicherheit zu erhöhen, ist es allerdings auch möglich, dass auf dem Paper Wallet ein verschlüsselter Private Key angezeigt wird, welcher nur in Kombination mit einem zusätzlichen Passwort gültig ist.[57]

Des Weiteren kann der Private Key auch auf einem USB Stick gespeichert werden und dieser Stick dann sicher verwahrt werden, z.B. in einem Tresor. Ähnlich funktionieren sog. Hardware Wallets, welche meist als UBS Stick mit mehr oder weniger Zusatzfunktionen ausgestaltet sind und – sobald mit dem Internet verbunden – auch Transaktionen ermöglichen.[58]

Eine weitere Variante ist schliesslich ein sog. Sound Wallet. Der Private Key wird hier in verschlüsselter Form von einer Bild- in eine Audio-Datei umgewandelt und auf einer CD oder sogar Vinyl Platte verewigt. Der Private Key kann sodann nur mittels eines Spektrometers gelesen werden, wobei die Audio-Datei hierfür wieder in eine Bilddatei umgewandelt wird.[59]

All diese Möglichkeiten von Cold Storage haben gemeinsam, dass sie in traditioneller Weise sicher verwahrt werden müssen (z.B. Tresor, Schliessfach). Dies gipfelt sogar in Angeboten für Verwahrung im Untergrund über mehrere Kontinente verteilt.[60]

c) Stark erschwerte Abänderlichkeit

Wie bereits angetönt, liegt das eigentliche Problem einer unautorisierten Zahlung im Bereich der virtuellen Währungen an faktischen Gegebenheiten. Es wurde dargelegt, dass die Verifizierung von Transaktionen zum einen dezentral erfolgt und zum anderen die einzelnen Transaktionen in Blöcken, welche miteinander verbunden sind, zusammengefasst werden.

Tritt nun der Fall ein, dass jemand mit einem fremden Private Key eine unautorisierte Transaktion ins Netzwerk schickt, wird diese mutmasslich von allen oder zumindest der Mehrheit der Nodes als korrekt verifiziert und im Netzwerk verteilt werden. In der Folge wird die Transaktion im Rahmen des anwendbaren Konsens-Algorithmus in einen Block integriert und dieser nach Verifikation wieder im Netzwerk verteilt. Die unautorisierte Zahlung

---

56 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin; ANTONOPOULOS, Mastering Bitcoin, S. 104 ff.; <https://walletgenerator.net>.

57 ANTONOPOULOS, Mastering Bitcoin, S. 105 f.

58 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin.

59 ULM, Listen to your Bitcoins with Sound Wallet; THOMA, Sound Wallet.

60 Vgl. hierzu <https://xapo.com/vault>.

wird also mehrfach von einer unzählbar grossen Teilnehmerzahl bearbeitet, ohne dass es eine zentrale Anlaufstelle geben würde, bei welcher eine Rückabwicklung begehrt werden könnte.

Als wäre dies nicht bereits genug, wird das Ganze durch die Aneinanderreihung der einzelnen Blöcke noch zusätzlich erschwert. Der Block x, in welchen die unautorisierte Transaktion aufgenommen wurde, wird sowohl durch die Daten der Transaktion wie auch durch die Daten bzw. den Hash des vorherigen Blockes x-1 bestimmt. Zusätzlich wird jeder darauffolgende Block x+n auch die Daten des Blockes x und damit der unautorisierten Transaktion enthalten. Damit wäre eine Rückabwicklung mit einem so grossen technischen, aber auch energetischen und damit finanziellen Aufwand verbunden, dass dies für einen normalen Teilnehmer schlicht nicht möglich ist. Sollte also der Widerruf oder die Stornierung bzw. allgemein die Rückabwicklung einer Transaktion nicht bereits aufgrund der dezentralen Struktur der Blockchain ausgeschlossen sein, so würde sie spätestens aufgrund des zu grossen Aufwandes unrealistisch.

d) Fork als Spezialfall

Der Grundsatz, dass Transaktionen aufgrund der vorgängig umschriebenen Funktionsweise nachträglich nicht mehr geändert werden können, erfährt im Zusammenhang mit sog. Forks einen Vorbehalt.

Grundsätzlich sind gewisse Gabelungen oder Neudeutsch Forks der Blockchain Technologie immanent. Sie erfolgen regelmässig dann, wenn zwei gültige Blöcke gleichzeitig innert eines kurzen Zeitabstandes geschaffen werden und zu einer Abweichung der Ansichten der verschiedenen Netzwerkteilnehmer betreffend die korrekte Transaktionshistorie führen.[61] Normalerweise ist dies ein vorübergehender Zustand, da sich bald die längste Kette durchsetzt und sich dann wieder alle Nodes auf eine richtige Kette einigen.[62]

---

61 ANTONOPOULOS, Mastering Bitcoin, S. 200 f.; <https://bitcoin.org/en/developer-guide#block-chain>; DECKER/WATTENHOFER, Information Propagation, S. 3 und 6; CASTOR, A Short Guide to Bitcoin Forks.

62 ANTONOPOULOS, Forkology: A Study of Forks for Newbies, ab 04:30; ANTONOPOULOS, Mastering Bitcoin, S. 200; DECKER/WATTENHOFER, Information Propagation, S. 3; CASTOR, A Short Guide to Bitcoin Forks.

Ein Fork kann jedoch auch bei der Weiterentwicklung der den jeweiligen virtuellen Währungen zugrundeliegenden Open Source Software erfolgen.[63] Wird eine neue Regel in den Code integriert, welche es auch denjenigen Nodes, welche das Update (noch) nicht implementiert haben, ermöglicht, Transaktionen zu verifizieren und zu akzeptieren, spricht man von einem sog. *Soft Fork*. Die Regeln für die Gültigkeit von Transaktionen werden mit der neuen Software Version strenger und diese ist abwärtskompatibel. Die Nodes mit der aktualisierten oder neuen Software lehnen Transaktionen, welche nach der alten Softwareversion gültig gewesen wären, ab. Dagegen können diejenigen Nodes, welche noch die alte Version nutzen, auch Transaktionen basierend auf dem neuen Standard bearbeiten und akzeptieren. Damit ist weiterhin eine Teilnahme der Nodes möglich, welche die neue Regel noch nicht implementiert haben. Zur Veranschaulichung diene hier die Verkleinerung der Blockgrösse von 1MB auf 500kB: Ein Node mit neuer Software weist jeden Block ab, der die Grösse von 500kB überschreitet, während der Node mit der ursprünglichen Software generell Blöcke bis 1MB und damit auch 500kB akzeptieren kann.[64]

Die vorgängig umschriebene Art eines Forks unterscheidet sich vom sog. *Hard Fork*. Hierbei erfolgt eine Code-Änderung, die dazu führt, dass Transaktionen, welche nach den neuen Regeln gültig sind, von den Nodes, welche das Update nicht implementieren, zurückgewiesen werden. Die Regeln für die Gültigkeit von Transaktionen werden lascher und es mangelt hier an der Kompatibilität der neuen Software mit der alten. Wird das Update folglich nicht von allen Nodes übernommen, kommt es zu einer Spaltung der Blockchain, in eine mit und in eine ohne das entsprechende Update.[65] Ein Beispiel für einen Hard Fork ist die Abspaltung der Bitcoin Cash Blockchain am 1.

---

63 <https://www.btc-echo.de/tutorial/der-fork-guide-was-ist-eine-fork-und-welche-arten-gibt-es-soft-fork-hard-fork-uasf-masf>; CASTOR, A Short Guide to Bitcoin Forks.

64 Vgl. zum Ganzen: ANTONOPOULOS, Forkology: A Study of Forks for Newbies, ab 09:45; <https://www.btc-echo.de/tutorial/der-fork-guide-was-ist-eine-fork-und-welche-arten-gibt-es-soft-fork-hard-fork-uasf-masf>; <https://bitcoin.org/en/developer-guide#consensus-rule-changes>; CASTOR, A Short Guide to Bitcoin Forks; bitcoin*wiki*, Softforks, <https://en.bitcoin.it/wiki/Softfork>.

65 Vgl. zum Ganzen: ANTONOPOULOS, Forkology: A Study of Forks for Newbies, ab 09:45; <https://www.btc-echo.de/tutorial/der-fork-guide-was-ist-eine-fork-und-welche-arten-gibt-es-soft-fork-hard-fork-uasf-masf>; <https://www.investopedia.com/terms/h/hard-fork.asp>; <https://bitcoin.org/en/developer-guide#consensus-rule-changes>; CASTOR, A Short Guide to Bitcoin Forks.

August 2017: Die neue Blockgrösse von 8MB kann nur von Nodes/Minern akzeptiert werden, die das entsprechende Update durchgeführt haben. Mit einer älteren, auf Blöcke von 1MB ausgerichteten, Version der Software ist die Verarbeitung von 8MB-Blöcken nicht möglich.[66]

Durch Forks werden also Transaktionen neuen Regeln unterstellt, sodass ursprünglich gültige Transaktionen ungültig oder ursprünglich ungültige Transaktionen allenfalls sogar gültig werden.

Für eine Rückabwicklung im Fall einer unautorisierten Zahlung taugen diese Mechanismen allerdings nicht. Vielmehr sind sie mit zusätzlichen Risiken verbunden. Neben der generellen Unsicherheit während der Umstellung auf eine neue Software-Version, besteht im Falle von Hard Forks insbesondere das Problem von sog. Replay Attacks. Da die technologische Basis der gespaltenen Blockchain jeweils dieselbe ist,[67] besteht die Gefahr, dass eine Transaktion zweimal – sowohl in der ursprünglichen als auch in der abgespaltenen, neuen Blockchain – ausgeführt wird.[68]

V. Haftung

1. In der zentralisierten Welt

Das Schweizer Zivilrecht regelt die Haftung zwischen Vertragsparteien und bei unerlaubten Handlungen. Dabei setzt es voraus, dass der Schuldner (Art. 97 ff. OR) respektive der Ersatzpflichtige (Art. 41 OR) bekannt sind. Es gibt Rechtssubjekte, die man ins Recht fassen kann. Den meisten Dienstleistungen im Finanzbereich liegt üblicherweise ein Auftragsverhältnis zwischen dem Anbieter des Dienstes und dem Benutzer zu Grunde. Der Beauftragte bzw. der Anbieter einer Dienstleistung ist zur getreuen Geschäftsführung nach Art. 398 OR verpflichtet und untersteht somit der auftragsrechtlichen Sorgfalts- und Treuepflicht. Vom Beauftragten wird gefordert, alles zu tun, um die richtige Erfüllung der Hauptleistung und die Verwirklichung des Leistungserfolges zu sichern und dabei das Integritätsinteresse des

66 BERGMANN, Was passiert bei einem Hard Fork?; BERGMANN, Das kleine 1x1 zur Bitcoin Cash Fork.

67 So erhält der Nutzer bei einem Hard Fork grundsätzlich gleich viele Einheiten der neuen virtuellen Währung, wie er bereits von der alten besitzt, wobei die neuen Einheiten ursprünglich dem gleichen Schlüsselpaar zugeordnet sind.

68 HERTIG, Rise of Replay Attacks; SONG, Replay Attacks Explained.

Gläubigers zu beachten. Unsachgemässes, unsorgfältiges Verhalten wird deshalb grundsätzlich als Vertragsverletzung aufgefasst.[69]

Das Aufsichtsrecht[70] stipuliert Pflichten für regulierte Finanzinstitute, Banken, Effektenhändler etc., welche sowohl aufsichtsrechtlich relevant sind als auch zur Konkretisierung der zivilrechtlichen Sorgfaltspflicht dienen können. Als Beispiel kann das Rundschreiben der FINMA «Operationelle Risiken Banken» erwähnt werden, insbesondere dessen Anhang 3 «Umgang mit elektronischen Kundendaten».[71] Weitere Regeln inklusive Haftungsbestimmungen finden sich im Datenschutzrecht[72] sowie im Strafrecht.[73]

2. Haftungssubjekt in der dezentralen Welt?

Die dezentrale Welt zeichnet sich aus durch transnationale, mehrschichtige Gemeinschaften von Nutzern und Beitragserbringern (User, Miner etc.). Es gibt weder einen eindeutig bestimmbaren Ort, an dem anzuknüpfen wäre, noch eine eindeutig als Verursacher bestimmbare Person.

Gegen wen geht man vor bei dezentral geschaffenen Applikationen? Wer ist beispielsweise der Emittent von Bitcoin, Ether etc.? Können ein Algorithmus oder ein Code Rechtssubjekte sein? Diese Fragen sind nach wie vor weitgehend ungeklärt.

Bei Softwareprogrammen sind primär die Programmierer haftbar, wenn es möglich ist, ihnen einen Fehler und Verschulden gemäss den zivilrechtlichen Haftungsnormen nachzuweisen.[74] Das Programm selbst kann ja nicht unsorgfältig handeln, da es automatisch abläuft.

Intermediäre wie Cryptocurrency Exchanges, Wallet Provider etc. sind Rechtssubjekte, die man ebenfalls ins Recht fassen kann. Anwendbar sind allgemein gültige Normen wie das Datenschutzgesetz[75] und auf Verträge

---

69 KELLER/HESS, Rechtliche Anforderungen, S. 199.

70 Vgl. zum Folgenden KELLER/HESS, Rechtliche Anforderungen, S. 188 ff., 200.

71 FINMA-RS 2008/21; siehe dazu KELLER/HESS, Rechtliche Anforderungen, S. 189 ff.

72 Bestimmungen über die Datensicherheit: Art. 7 DSG, Art. 8 VDSG; siehe dazu KELLER/HESS, Rechtliche Anforderungen, S. 196 f., 201.

73 Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143 StGB); Verletzung des Fabrikations- oder Geschäftsgeheimnisses (Art. 162 StGB).

74 WEBER, Leistungsstörungen, S. 9 Abschnitt III.2.2.

75 ISLER, Datenschutz, passim.

das Zivilrecht sowie das Strafgesetzbuch.[76] Sehr oft sehen die anwendbaren Vertragsbestimmungen eine weitestgehende Freizeichnung vor:

> «*Participants therefore release and indemnify the provider from all liability for any loss that may occur as a result of their participation in the application and in connection with these risks.*»

Die Geltung solcher Klauseln wird durch die Ungewöhnlichkeitsregel eingeschränkt.[77] Die Ungewöhnlichkeitsregel läuft dort ins Leere, wo der Vertragspartner auf die an sich ungewöhnliche Klausel hingewiesen wurde und folglich von ihrem Inhalt Kenntnis genommen hat.[78]

Zumindest für Konsumenten stellt ein solch genereller Haftungsausschluss wohl einen Verstoss gegen Art. 8 UWG dar.[79] Eine Art. 8 UWG verletzende Klausel ist widerrechtlich (Art. 20 OR). Vertragsrechtlich kann Art. 8 UWG zur Nichtigkeit der betroffenen Klauseln führen.[80]

Sofern ein Haftungssubjekt bekannt ist, sollte die Haftung gemäss dem Prinzip der Risikosphären verteilt werden: Jede Partei übernimmt diejenigen Risiken, die aus ihrem Einflussbereich stammen, den sie am ehesten kontrollieren kann.[81] Das führt zur Haftung der Cryptocurrency Exchanges bei Verlust der Vermögenswerte ihrer Kunden, weil diese in der Hot Wallet verwahrt werden, welche gehackt wurde. Ebenso haften die Wallet-Betreiber, die Erschaffer von Applikationen, Programmen und Smart Contracts für die Mängel der von ihnen erschaffenen oder zur Verfügung gestellten Produkte.

Wie diese theoretische Haftbarkeit in der Praxis durchsetzbar ist, bleibt allerdings abzuwarten. Zu breit sind die Problemfelder[82] und zu unerfahren wohl viele Beteiligte.

---

76 WEBER, Leistungsstörungen, S. 8 f. Abschnitt III.2.1.

77 BGE 135 III 1 E. 2.1 S. 7; 138 III 411 E. 3.1 S. 412.

78 BGE 109 II 452 E. 5b S. 458; KOLLER, Auslegeordnung, S. 17 ff., 32 f.; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 37 ff., 181.

79 Siehe dazu KELLER/HESS, Rechtliche Anforderungen, S. 199; KOLLER, Auslegeordnung, S. 17 ff.; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 83 ff.

80 KOLLER, Auslegeordnung, S. 64 ff.; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 146 ff.

81 WIEGAND/MARTI, E-Banking Vereinbarung, S. 102; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 202 ff.

82 Zur Frage des anwendbaren Rechts siehe HESS/SPIELMANN, Cryptocurrencies, S. 196 f.

VI. Zusammenfassung

Die zentralisierte Welt verfügt über ein differenziertes Regelwerk oder entsprechende Gerichtspraxis, welche bei nicht-autorisierten Transaktionen die Haftung und Schadloshaltung regeln.

In der dezentralen Welt überwiegt als Folge der Gleichung «code is law»[83] die faktische Durchsetzung gemäss der zugrundeliegenden Technologie gegenüber den gesetzlichen Normen oder der Gerichtspraxis. Die Verfügung mittels und über den Private Key ist endgültig, Autorisierung oder Nichtautorisierung hin oder her. Es zählt die Eigenverantwortung der InhaberInnen des Private Key.

Die gesetzlichen Vorschriften und die Gerichtspraxis beruhen seit jeher auf dem Faktischen. Das Recht wird der digitalen Realität Rechnung tragen, aber diese nicht als unabänderliche Wahrheit hinnehmen. Jurisprudenz bedeutet nach wie vor Abwägen von Interessen und Rechtsgütern:

> *«La proportionnalité est inhérente, en effet, à l'idée de justice, principe régulateur de tout droit.»*[84]

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 5. Mai 2018.

ALPEYEV PAVEL/NAKAMURA YUJI, How to Launder $500 Million in Digital Currency vom 29./31. Januar 2018, abrufbar unter: <https://www.bloomberg.com/news/articles/2018-01-29/how-to-launder-500-million-in-digital-currency-quicktake-q-a>.

ANTONOPOULOS ANDREAS M., Forkology: A Study of Forks for Newbies vom 24. Juni 2017, abrufbar unter: <https://www.youtube.com/watch?v=rpeceXY1QBM>.

ANTONOPOULOS ANDREAS M., Mastering Bitcoin:Unlocking Digital Cryptocurrencies, Sebastopol 2015.

BAJPAJ PRABLEEN, What Is Cold Storage For Bitcoin, abrufbar unter: <https://www.investopedia.com/articles/investing/030515/what-cold-storage-bitcoin.asp>.

BERGMANN CHRISTOPH, Das kleine 1x1 zur Bitcoin Cash Fork: Alles, was ihr wissen müsst vom 8. August 2017, abrufbar unter: <https://bitcoinblog.de/2017/08/08/das-kleine-1x1-zur-bitcoin-cash-fork-alles-was-ihr-wissen-muesst>.

83 LESSIG, Code Is Law, passim.

84 HUBER, Considérations, S. 417 ff., 423.

BERGMANN CHRISTOPH, Was passiert bei einem Hard Fork?vom 15. Juni 2015, abrufbar unter: <https://bitcoinblog.de/2015/06/15/was-passiert-bei-einem-hard-fork>.

BUIS ERIC, Das Stornorecht der Bank im Überweisungsverkehr, in: SZW 2002, S. 120–128.

CARSTENS AUGUSTIN, Money in the digital age: what role for central banks? Lecture of 6 February 2018 at the House of Finance, Goethe University, Frankfurt, abrufbar unter : <https://www.bis.org/speeches/sp180206.pdf>.

CASTOR AMY, A Short Guide to Bitcoin Forks vom 27. März 2017, abrufbar unter: <https://www.coindesk.com/short-guide-bitcoin-forks-explained>.

CZERNIK AGNIESZKA, Authentisierung, Authentifizierung und Autorisierung vom 24. Juni 2016, abrufbar unter: <https://www.datenschutzbeauftragter-info.de/authentisierung-authentifizierung-und-autorisierung>.

DECKER CHRISTIAN/WATTENHOFER ROGER, Information Propagation in the Bitcoin Network, 13-th IEEE International Conference on Peer-to-Peer Computing, 2013, abrufbar unter: <http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf>.

EMMENEGGER SUSAN, PSD2: Eckpunkte und Relevanz für Schweizer Finanzdienstleister, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 17–66.

GIOVANOLI MARIO, Bargeld, Buchgeld, Zentralbankgeld: Einheit oder Vielfalt im Geldbegriff?, in: Festschrift für Beat Kleiner, Banken und Bankrecht im Wandel, Zürich 1993, S. 87–124.

GRÜNEWALD SERAINA, Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme (ZIK): Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 61, Zürich 2015, S. 93–112.

HERTIG ALYSSA, Rise of Replay Attacks Itensifies Ethereum Divide vom29/31. Juli 2016, abrufbar unter: <https://www.coindesk.com/rise-replay-attacks-ethereum-divide>.

HESS MARTIN, Euro-Zahlungen gemäss den SEPA-Rulebooks, insbesondere die Haftung der Banken, in Susan Emmenegger (Hrsg.), Cross-Border Banking, Basel 2009, S. 47–104.

HESS MARTIN/KALBERMATTER ANDRÉ/WEISS VOIGT ALEXANDRA, Kommentierung von Art. 81 FinfraG, in: Rolf Sethe/Olivier Favre/Martin Hess/Stefan Kramer/Ansgar Schott (Hrsg.), Schulthess-Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG, Zürich 2017.

HESS MARTIN/SPIELMANN PATRICK, Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht, in: Kapitalmarkt – Recht und Transaktionen XII, Zürich 2017, S. 145–202.

HESS MARTIN/STÖCKLI KATJA, Das Bucheffektengesetz aus der Optik des Kapitalmarktrechts, in: Kapitalmarktransaktionen V, Zürich 2010, S. 65–120.

HESS MARTIN/ZBINDEN ANDREA, Kommentierung von Art. 15 BEG, in: Dieter Zobl/Martin Hess/Ansgar Schott (Hrsg.), Kommentar zum Bucheffektengesetz (BEG), Zürich 2013.

HUBER MAX, Quelques considérations sur une révision éventuelle des Conventions de la Haye relatives à la guerre, in: Revue Internationale de la Croix Rouge, 37 (439)/ 1955, S. 417–433.

ISLER MICHAEL, Datenschutz auf der Blockchain, in: Jusletter 4. Dezember 2017.

KELLER CLAUDIA/HESS MARTIN, Rechtliche Anforderungen an System- und Datensicherheit und Compliance für webbasierte und mobile Zahlungen, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, (ZIK): Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 61, Zürich 2015, S. 181-205.

KOLLER THOMAS, Art. 8 UWG: Eine Auslegeordnung, in: Susan Emmenegger (Hrsg), Das Bankkonto, Basel 2013, S. 17–81.

LESSIG LAWRENCE, Code Is Law, On Liberty in Cyberspace, in: Harvard Magazine 29 February 2012, abrufbar unter: <https://harvardmagazine.com/2000/01/code-is-law-html>.

NAKAMOTO SATOSHI, Bitcoin: A Peer-to-Peer Electronic Cash System, abrufbar unter: <https://bitcoin.org/bitcoin.pdf>.

ROSIC AMEER, Paper Wallet Guide: How to Protect Your Cryptocurrency, 2017, abrufbar unter: <https://blockgeeks.com/guides/paper-wallet-guide>.

ROSIC AMEER, Proof of Work vs. Proof of Stake: Basic Mining Guide, 2017, abrufbar unter: <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake>.

SONG JIMMY, Replay Attacks Explained vom 21. August 2017, abrufbar unter: <https://bitcointechtalk.com/replay-attacks-explained-e3d6d2ea0ab2>.

SZABO NICK, Trusted Third Parties Are Security Holes, originally published in 2001, abrufbar unter: <http://nakamotoinstitute.org/trusted-third-parties/#selection-7.6-17.34>.

THOMA JÖRG, Sound Wallet. Private Schlüssel, auf Schallplatte gepresst vom 5. September 2014, abrufbar unter: <https://www.golem.de/news/sound-wallet-private-schluessel-auf-schallplatte-gepresst-1409-109073.html>.

ULM BOGDAN, Listen to your Bitcoins with Sound Wallet vom 2. September 2014, abrufbar unter: <https://cointelegraph.com/news/listen-to-your-bitcoins-with-sound-wallet>.

WEBER ROLF H., Kommentierung von Art. 27 und 28 BEG, in: ZOBL DIETER/HESS MARTIN/SCHOTT ANSGAR, Kommentar zum Bucheffektengesetz (BEG), Zürich, 2013.

WEBER ROLF H., Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts, in: Jusletter 4. Dezember 2017.

WELTER PATRICK, Hackerangriff trifft japanische Krypto-Börse vom 29. Januar 2018, abrufbar unter: <https://www.nzz.ch/wirtschaft/hackerangriff-trifft-japanische-krypto-boerse-ld.1352017>.

WIDMER ESTHER, Missbräuchliche Geschäftsbedingungen nach Art. 8 UWG (Diss. Bern), Zürich 2015.

WIEGAND WOLFGANG/MARTI MARIO, Die E-Banking-Vereinbarung – Rechtliche Einordnung und Wirkung, in: E-Banking, Die einzelnen Rechtsgeschäfte, Berner Bankrechtstag BBT, Band 9/2002, Bern 2002, S. 75–108.

YOUNG JOSEPH, BitGrail Vs. Nano: Who Is Responsible For the $150 Million Theft? vom 18. Februar 2018, abrufbar unter: <https://cointelegraph.com/news/bitgrail-vs-nano-who-is-responsible-for-the-150-million-theft>.

ZELLWEGER-GUTKNECHT CORINNE, Digitale Landeswährung – Ein Überblick, in: Jusletter vom 31. Oktober 2016.