Zeitschrift für Datenrecht und Informationssicherheit

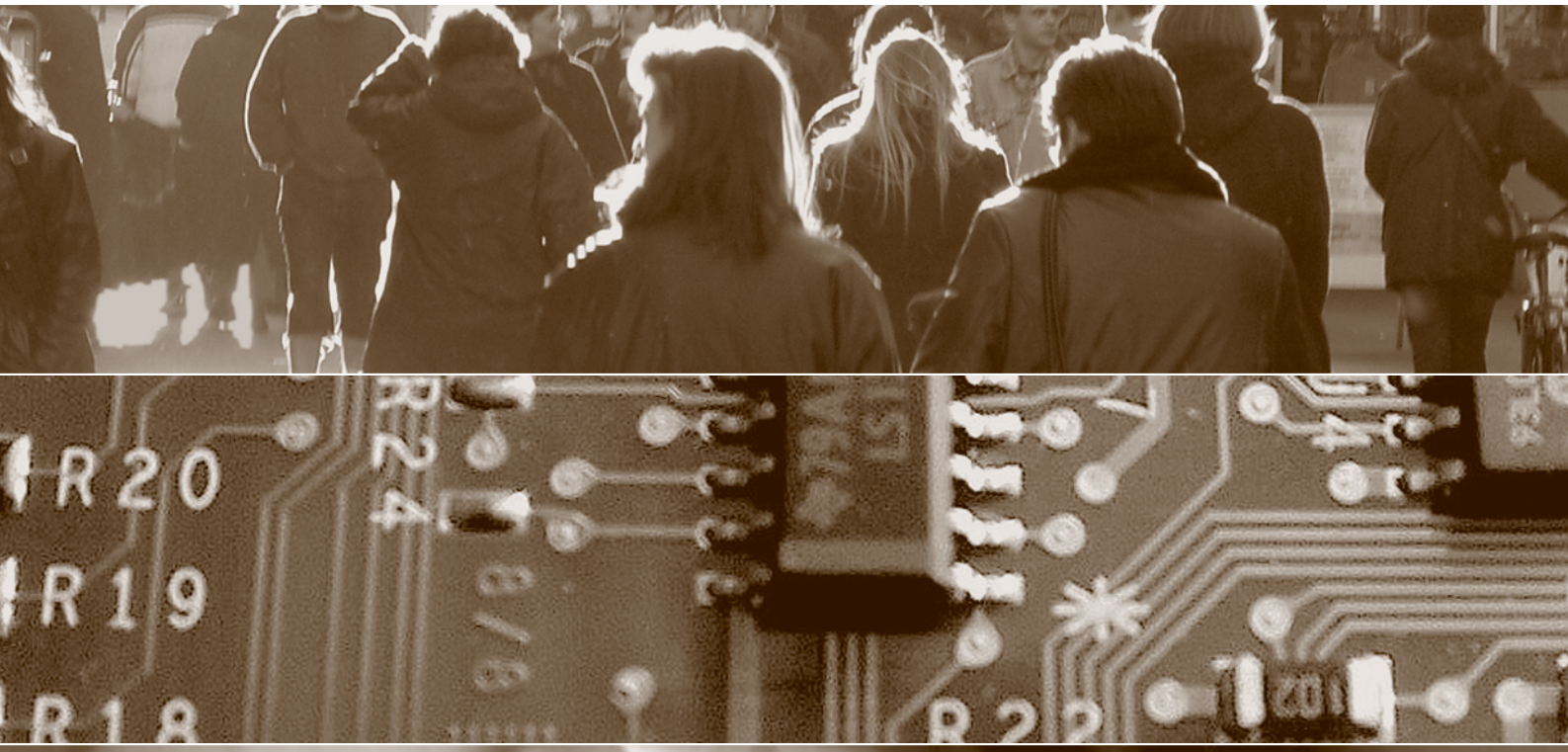
digma

www.digma.info 18. Jahrgang, Heft 1, März 2018

Schwerpunkt:

Anonymes Bezahlen

fokus: Eigenschaften der Kryptowährung Bitcoin
fokus: Nutzerverfolgung via Blockchain
report: Datenschutzreform: Nun braucht es den zweiten Schritt



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

Eigenschaften der Kryptowährung Bitcoin

Geld, aber ohne Sachqualität – wem «gehört» ein Bitcoin bei geteilter Verfügungsmacht?

Gabriela Hauser-Spühler, Rechtsanwältin und Urkundsperson des Kantons Zug, Lachen SZ ghauser@hauser-law.ch

Luzius Meisser, Informatik-Ingenieur und Mitgründer der Bitcoin Association Switzerland, Erlenbach ZH luzius@meisser economics.com

Nach einer allgemeinen Betrachtung der Internetwährung wird erstmals zur Möglichkeit des Mitgewahrsams am Vermögenswert Stellung genommen.

Der Wechselkurs des Bitcoins brach in den Wochen vor dem Jahreswechsel einen Rekord nach dem anderen. Anfang 2017 kostete ein Bitcoin noch USD 1000. Ende Jahr waren es bereits USD 14000. Der Gesamtwert aller Bitcoins erreichte über 200 Milliarden. Bitcoin gehört damit – an der Geldmenge gemessen – zu den grössten 20 Währungen der Welt, noch vor der norwegischen Krone, aber ein Stück hinter dem Schweizer Franken, bei dem die Geldmenge dreimal so gross ist[1,2].

Der Vizepräsident der Europäischen Zentralbank, Vítor Constâncio, verglich Bitcoin in Anspielung auf die Spekulationsblase des 17. Jahrhunderts in den Niederlanden mit einer «Tulpe»[3]. Doch darf Bitcoin nicht einzig als spekulative Gier abgetan werden. Die dem Bitcoin zugrunde liegende Technologie, die Blockchain, ist mehr als eine Tulpe. Sie könnte das Fundament sein für ein «Internet of Finance», einem weltweiten, freien und digitalen Finanzsystem.

Die Schweiz ist ein Kristallisationskeim dieser Entwicklung, die eine enorme Chance für den Finanzplatz darstellt. Bundesrat Johann Schneider Ammann hat unlängst die Vision einer «Crypto Nation Switzerland» geäussert und das Staatssekretariat für Internationale Finanzfragen eine Arbeitsgruppe zur Klärung des rechtlichen Handlungsbedarfs ins Leben gerufen[4,5].

Im vorliegenden Beitrag werden Bitcoin und einzelne aktuelle Fragen im Zusammenhang mit der Internetwährung möglichst vereinfacht und ohne Anspruch auf Vollständigkeit dargestellt. Der Leser möge eine Vorstellung davon erhalten, wie Innovation im Kontext der Digitalisierung aktuell die rechtliche Realität herausfordert.

Ist Bitcoin Geld?

Funktionale Betrachtung

Bitcoin ist eine dezentral organisierte Internetwährung mit einem zugehörigen Zahlungssystem, das auf der Innovation der Blockchain beruht. Der Wechselkurs entsteht wie bei anderen Währungen durch Angebot und Nachfrage auf dem freien Markt. Der Wert eines Bitcoins wird von niemandem garantiert. Seit der Aufhebung des Goldstandards in der Schweiz gilt dies übrigens auch für den Schweizer Franken[6]. Die Menge an Bitcoins ist vordefiniert und auf 21 Millionen Bitcoins begrenzt. Aufgrund dieser Verknappung des Angebots wird Bitcoin oft auch als «digitales Gold» bezeichnet. Anders als in allen zuvor geschaffenen elektronischen Zahlungssystemen finden Transaktionen im Bitcoin-System direkt von Person zu Person statt. Der Finanzintermediär – wie beispielsweise ein zwischengeschalteter Zahlungsdienstleister – entfällt.

Bitcoins oder Bruchteile davon können als unkörperliche und vertretbare Werteinheiten, die stets genau einer Adresse im Bitcoin-System zugeordnet sind, betrachtet werden. Über die Adresse ist definiert, wie die zugehörigen Bitcoins auf eine neue Adresse übertragen werden können. Bei den meisten Adressen wird mittels eines geheimen kryptografischen Schlüssels – eines langen Codes bestehend aus einer Abfolge von Zahlen und Zeichen – über die Werteinheiten verfügt, analog einer Einzelunterschrift. Es können aber auch andere Berechtigungsmechanismen im Zusammenhang mit einer bestimmten Adresse konfiguriert werden, zum Beispiel «Unterschrift zu zweien»[7]. Adressen werden oft auch als Konten bezeichnet, was aber insofern irreführend ist, als sie nicht auf einen Namen lauten und auch keine Guthaben darstellen. Vgl. S. 8 betreffend die Übertragung und Aufbewahrung von Kryptowährungen[8].

Rechtliche Betrachtung

Der Begriff «Geld» oder «Geldschuld» ist im schweizerischen Recht weder definiert noch

Vergleich mit Bargeld

- Wie Bargeld können Bitcoins als Zahlungsmittel dienen. Sie sind als Tauschmittel, Rechnungseinheit und Wertspeicher einsetzbar, und übernehmen entsprechend die typischen Funktionen von Geld[39].
- Wie Bargeld gelten Bitcoins aufgrund deren Handelbarkeit als Vermögenswert[40].
- Wie Bargeld sind Bitcoins keine Forderung, kein Wertrecht im Sinne von Art. 973c OR und auch kein Guthaben.
- Wie Bargeld können Bitcoins ohne Mitwirken eines Intermediärs direkt von Person zu Person übertragen werden.
- Im Gegensatz zu physischem Bargeld, welches an Papier oder Metall gebunden ist, fehlt es dem Bitcoin an Körperlichkeit. Die Körperlichkeit des Bargelds dient dazu, feststellen zu können, wo es sich gerade befindet. Bei Bitcoin übernimmt die Blockchain diese Funktion, mittels derer jeder Bitcoin jederzeit eindeutig einer Adresse zugeordnet werden kann.

systematisch geregelt. Gemäss Art. 84 Abs. 1 OR[9] sind Geldschulden in gesetzlichen Zahlungsmitteln der geschuldeten Währung zu zahlen. Das Obligationenrecht enthält nach wie vor den Grundsatz, dass der Schuldner seine Schuld mittels Barzahlung zu bezahlen hat[10]. Der Gläubiger kann aber ausdrücklich oder konkludent sein Einverständnis zu einer bargeldlosen Zahlung – also einem anderen Zahlungsmittel – erteilen. Mit der Zustimmung des Gläubigers kann entsprechend auch Bitcoin als Zahlungsmittel verwendet werden.

Im Bundesgesetz über Währung und die Zahlungsmittel (WZG)[11] sowie im Nationalbankengesetz (NBG)[12] sind sodann die *gesetzlichen* Zahlungsmittel in der Schweiz definiert. Es handelt sich um die vom Bund ausgegebenen Münzen, die von der Schweizerischen Nationalbank (SNB) ausgegebenen Banknoten und die auf Franken lautenden Sichtguthaben bei der SNB (Art. 2 WZG). Für diese gesetzlichen Zahlungsmittel besteht für den Gläubiger eine grundsätzliche Annahmepflicht als Zahlungsmittel (vgl. Art. 3 WZG)[13]. Die gesetzlichen Zahlungsmittel werden als «Geld im engeren Sinn» bezeichnet[14].

Neben den gesetzlichen Zahlungsmitteln existieren aber andere, weit wichtigere und verbreitetere Formen von Zahlungsmitteln, bspw. *Buchgeld* in der Form von Guthaben bei einer Bank oder *elektronisches Geld* (auch «E-Money» genannt)[15], bei welchen vor allem auf die Funktion als Tausch- und Zahlungsmittel abgestellt wird[16]. Da Bitcoin und andere Kryptowährungen inzwischen in der Öffentlichkeit verbreitet und akzeptiert sind und insbesondere die typischen Funktionen von Geld übernommen haben, können diese rechtlich betrachtet als «*Geld im weiteren Sinn*» qualifiziert werden[17].

Ist Bitcoin eine Währung?

Obwohl unter dem Begriff «Währung» allgemein die übliche Bezeichnung für das jeweils gültige gesetzliche Zahlungsmittel innerhalb eines Währungsraums verstanden wird, haben sich bezogen auf Bitcoins umgangssprachlich die Begriffe «Internetwährung» oder «virtuelle Währung» bereits etabliert[18]. Das Wort «virtuell» ist allerdings insofern irreführend, als Bitcoins und andere Kryptowährungen einen sehr realen und nicht nur virtuellen Wert aufweisen.

Die oft als Synonyme für Bitcoins verwendeten Bezeichnungen «Digitalwährung» oder «digitale Währung» sind nur beschränkt aussagekräftig.

Die ebenfalls oft als Synonyme für Bitcoins verwendeten Bezeichnungen «Digitalwährung» oder «digitale Währung» sind ebenfalls nur beschränkt aussagekräftig. «Digital» bedeutet lediglich, dass Beträge mittels Ziffern dargestellt werden und sich nicht etwa nach dem Gewicht einer Münze[19] richten. Das bereits erwähnte elektronische Geld wird – wie Bitcoins auch – digital dargestellt. Bitcoins sind aber im Gegensatz zu elektronischem Geld nicht mit

Kurz&bündig

Bitcoin und die zugrunde liegende Technologie der Blockchain sind längst keine Randphänomene mehr. Zwar ist Bitcoin in vielerlei Hinsicht neuartig. Das steht aber einer Einordnung als «Geld im weiteren Sinn» bzw. als «Kryptowährung» nicht im Weg. Bitcoin dient zurzeit primär als Spekulationsobjekt, aber auch zur Wertaufbewahrung und als Zahlungsmittel. Während das Bitcoin-System nur die Übertragung von Bitcoins erlaubt, ist die Blockchain von Ethereum, der zweitgrössten Kryptowährung, frei programmierbar und erlaubt die Emission beliebiger «Tokens». Diese können Währungen, Anleihen, Aktien oder beliebige andere Vermögenswerte mit oder ohne vom Emittenten garantierten Wert darstellen. Kryptowährungen haben das Potenzial, einen Digitalisierungsschub im Finanzbereich auszulösen. Um dieses Potenzial zu realisieren, bedarf es aber noch der Klärung verschiedener Rechtsfragen und der Beseitigung rechtlicher Hürden.

einem gesetzlich zugelassenen Zahlungsmittel unterlegt und weisen eine eigene Denomination auf.

Nach der hier vertretenen Ansicht bringt schliesslich der Überbegriff «Kryptowährung», der auch für Bitcoins zu bevorzugen ist, korrekt zum Ausdruck, dass die dem Bitcoin zugrunde liegende Technologie auf kryptografischen Methoden beruht. Kryptografie umfasst Verschlüsselungstechnik, aber auch elektronische Fingerabdrücke und Signaturen. Das Präfix «Krypto» trifft auch auf andere Anwendungsformen zu, je nachdem, was mittels Blockchain verwaltet werden soll. Die Anwendungsmöglichkeiten der Blockchain-Technologie umfassen faktisch nämlich viel mehr als blosse Bitcoin-Transaktionen, wie etwa die Kryptoaktie oder Kryptoanleihe, je nach Art des zugrunde liegenden Werts. Allerdings besteht keine allgemein anerkannte und international etablierte Klassifizierung für Werte, die mittels Blockchain verwaltet werden können. Immerhin hat die schweizerische Finanzmarktaufsicht (FINMA) kürzlich in der Wegleitung zu sogenannten Initial Coin Offerings erstmals eine Klassifizierung vorgenommen[20].

Die Liste an ungeklärten Fragen im Zusammenhang mit Kryptowährungen und insbesondere Kryptoassets und weiteren Ausprägungen der Blockchain-Technologie ist lang.

Übertragung und Aufbewahrung von Kryptowährungen

Die Übertragung von Kryptowährungen geschieht mittels kryptografisch signierten und damit fälschungssicheren Transaktionen im Bitcoin-System, welches über das Internet zugänglich ist. Alle Transaktionen werden analog einer Buchhaltung in der Blockchain gespeichert und auf diese Weise allen Systemteilnehmern bekannt gemacht, so dass diese von jedem nachvollzogen und überprüft werden können. Aufgrund der unabänderlichen Transaktionshistorie ist jede Währungseinheit jederzeit einer Adresse zuordenbar. Oft genügt ein einziger Zugangsschlüssel, um über die einer Adresse zugeordneten Werte verfügen zu können (Einzelunterschrift). Es gibt aber auch andere Varianten. Dies wird im Folgenden anhand des Beispiels von Bitcoin genauer erläutert.

Bitcoins können als unkörperliche, vertretbare Werteinheiten, die stets genau einer Adresse im Bitcoin-System zugeordnet sind, betrachtet werden. Die Verfügungsmacht über alle einer Adresse zugeordneten Bitcoins (oder Bruchteilen davon) wird mittels zugehöriger kryptografischer Schlüssel ausgeübt. Damit ergeben sich im Standardfall einer Adresse mit Einzelunterschrift zwei Möglichkeiten, wie der Besitz an einem Bitcoin übertragen werden kann:

- durch das Übergeben des geheimen Signierschlüssels an den neuen Besitzer[21];
- durch das Übertragen des Bitcoins auf eine Adresse, die unter der Verfügungsmacht des neuen Besitzers steht. Dazu wird unter Verwendung des geheimen Schlüssels eine entsprechende Transaktion kryptografisch signiert und im Bitcoin-System bekannt gemacht.

Die genauen Bedingungen, wie und unter welchen Umständen die Bitcoins von einer Adresse auf eine neue Adresse übertragen werden können, sind konfigurierbar. Verbreitet sind etwa «multi-signature» Adressen, mittels derer die Verfügungsmacht auf mehrere Schlüssel aufgeteilt werden kann. So kann zum Beispiel eine «Unterschrift zu zweien» direkt im System abgebildet werden. In diesem Fall werden zwei von mehreren geheimen Schlüsseln benötigt, um eine Transaktion auszulösen. Damit verfügen mehrere Parteien über die Vermögenwerte bzw. es kann Mitgewahrsam mehrerer Parteien bestehen. Zudem ist es beispielsweise auch möglich, Adressen zu erstellen, die nur eingehende, aber keine ausgehenden Transaktionen zulassen («black hole address»), oder solche, auf der die zugeordneten Bitcoins bis zu einem bestimmten Zeitpunkt in der Zukunft unwiderruflich blockiert sind. In Systemen der zweiten Generation, zum Beispiel Ethereum, sind die Adressen mit beliebigem Inhalt programmierbar und werden damit zu «Smart Contracts».

Viele ungelöste Fragen

Die Liste an ungeklärten Fragen im Zusammenhang mit Kryptowährungen und insbesondere Kryptoassets und weiteren Ausprägungen der Blockchain-Technologie ist lang. Die technischen Möglichkeiten übersteigen derzeit die gegenwärtige rechtliche Realität. Die Technologie hinter Bitcoin und Kryptowährungen lässt sich dadurch allerdings nicht bremsen.

Die Blockchain kann bspw. auch als Eigentumsregister für Forderungen und Wertrechte verwendet werden. In diesem Fall besteht das Problem, dass das Schweizer Gesetz in beiden Fällen die Schriftform für eine rechtsgültige Übertragung verlangt (Art. 165 Abs. 1 OR, Art. 973c OR). Dies hemmt die Realisierung des enormen Potenzials von Kryptoaktien und

Kryptoanleihen in der Schweiz. Es wäre wünschenswert, auf das Erfordernis der Schriftform zu verzichten oder zumindest die Beweiskraft eines Eintrags in einer Blockchain gesetzlich anzuerkennen[22].

Obwohl seit der ersten Beschreibung des Erfinders von Bitcoin bereits fast zehn Jahre vergangen sind, ist Bitcoin in der Rechtslandschaft immer noch ein neues Phänomen. Viele zivil- und vollstreckungsrechtliche, aber auch regulatorische[23] und datenschutzrechtliche[24] Fragen sind ungelöst. Der Gesetzgeber, aber auch Behörden, sind daher aufgefordert, neuen Entwicklungen im Hinblick auf die Entfaltung des inhärenten Potenzials Rechnung zu tragen, indem sie bestehende Gesetze technologieneutral anwenden und nötigenfalls anpassen[25].

Doch bereits die Klärung der Rechtsnatur von Bitcoins und anderen Kryptowährungen bereitet sowohl in der Schweiz als auch im Ausland Kopfzerbrechen. Es wird derzeit beispielsweise in Bezug auf Bitcoins diskutiert, ob Bitcoins als Sachen zu qualifizieren sind, wem diese im Konkursfall eines Schuldners gehören und ggf. ausgesondert werden können. Im Folgenden wird auf diese zwei wichtigen Aspekte eingegangen, da sie besonders geeignet sind, die Problematik der technologieneutralen Auslegung und Anwendung bestehender Gesetze zu beleuchten.

Sind Bitcoins Sachen?

In mancherlei Hinsicht verhalten sich Bitcoins und andere Kryptowährungen wie Sachen. Es wäre hilfreich, das Sachenrecht darauf anwenden zu können. Der Kanton Zug anerkennt zum Beispiel Bitcoins als Sacheinlage bei Firmengründungen[26]. Auch kann die Unterscheidung zwischen Eigentum und Besitz bei Kryptowährungen sinnvoll sein. Damit liesse sich die getrennte und individualisierte Aufbewahrung von Bitcoins durch Dritte besser von Bitcoin-Guthaben differenzieren, die bloss Forderungen darstellen. Doch könnte eine Einordnung als Sache auch Probleme mit sich bringen, etwa zollrechtlich bei der Einfuhr oder mehrwertsteuerrechtlich beim Verkauf.

In der Praxis ist diese Frage insbesondere dann relevant, wenn beurteilt werden muss, ob die Entgegennahme von Kryptowährungen durch Dienstleister wie bspw. Wallet-Provider zwecks Aufbewahrung eine Kundeneinlage im Sinn des Bankengesetzes (BankG)[27] darstellt.

Gemäss Art. 1 Abs. 2 BankG dürfen natürliche und juristische Personen, die dem Bankengesetz nicht unterstehen, keine Publikumseinlagen gewerbsmässig entgegennehmen. Dieses Verbot bezweckt, Sparer vor der Gefahr eines Verlustes als Folge der Insolvenz ihres Vertragspartners zu schützen[28]. Diese Gefahr besteht nicht, wenn Bitcoins beim Konkurs des Dienstleisters nicht in dessen Konkursmasse fallen würden, oder vom Kunden aufgrund seines Eigentumsrechts an der *Sache* ausgesondert werden könnten. Zur Aussonderung vgl. sogleich nach dem nächsten Zwischentitel.

Das grösste Hindernis zur Einordnung von Bitcoin als Sache ist Art. 713 ZGB, der für die Qualifikation als bewegliche Sache Körperlichkeit verlangt[29]. Auf den ersten Blick scheint es, dass man dieses Problem lösen könnte, indem man auch *Daten* als Sachen qualifiziert, wie dies zum Beispiel Eckert nahelegt[30].

Aus informationstheoretischer Sicht handelt es sich bei Bitcoins allerdings weder um «Daten» noch um «Informationen»[31]. Zudem existiert keine allgemeingültige rechtliche Definition, was «Daten» sind. Der Begriff wird in der Gesetzgebung uneinheitlich verwendet[32].

Hingegen handelt es sich immerhin bei den Adressen und den Zugangsschlüsseln im Bitcoin-System um informationstheoretische Daten. Beide sind eine Zeichenfolge und können auch, wie bei Daten üblich, beliebig kopiert werden. Im Gegensatz dazu sind Kryptowährungen aber nicht an bestimmte Daten gebunden und können auch nicht kopiert werden. Die Datenübertragung beim Übertragen von Bitcoins dient lediglich dazu, alle Systemteilnehmer über die Transaktion zu benachrichtigen und passiert völlig unabhängig davon, wer Bitcoins an wen überträgt. Vor diesem Hintergrund erscheint zweifelhaft und wäre näher zu untersuchen, ob Bitcoins rechtlich überhaupt als Daten qualifiziert werden können. Dies wäre aber die Grundvoraussetzung für die Idee, Bitcoins als digitale Daten (Res digitalis) unter den Sachbegriff des ZGB zu subsumieren.

Es wird in Bezug auf Bitcoins diskutiert, ob Bitcoins als Sachen zu qualifizieren sind, wem diese im Konkursfall gehören und ob sie ausgesondert werden können.

Aussonderung im Konkurs

Gemäss Art. 197 Abs. 1 SchKG bildet sämtliches Vermögen, das zur Zeit der Konkurseröffnung dem Schuldner *gehört,* eine einzige Masse (Konkursmasse), die zur gemeinsamen Befriedigung der Gläubiger dient. Da grundsätzlich alle verwertbaren *Vermögenswerte* des Schuldners pfändbar sind, sind auch Bitcoins

im Sinne von Art. 89 ff. SchKG pfändbar und können in die Konkursmasse fallen[33].

Wie bereits erwähnt sind *Sachen,* die nach Art. 242 Abs. 1 SchKG erfolgreich ausgesondert werden konnten, nicht mehr Teil der Konkursmasse. Gemäss Maurenbrecher/Meier (und auch den von den Autoren zitierten Quellen) könnten Kryptowährungen aber nicht qua Eigentum aus der Konkursmasse eines Schuldners ausgesondert werden, da diese keine Sachen seien[34]. Gleich verhält es sich bei der Admassierung: Sollen *bewegliche oder unbewegliche Sachen* im Gewahrsam oder Mitgewahrsam eines Dritten in die Konkursmasse gezogen werden, muss die Admassierungsklage erhoben werden (Art. 242 Abs. 3 SchKG). Da Bitcoins den Sachbegriff nicht erfüllen, können Bitcoins im Gewahrsam oder Mitgewahrsam eines Dritten folglich nicht mittels der Admassierungsklage – einer ordentlichen Eigentumsklage – zur Konkursmasse gezogen werden[35].

Da grundsätzlich alle verwertbaren Vermögenswerte des Schuldners pfändbar sind, sind auch Bitcoin pfändbar und können in die Konkursmasse fallen.

Die erwähnten Klagen gemäss Art. 242 SchKG sollten eigentlich dazu dienen, die Konkursmasse auf die wesentlichen *Vermögenswerte* des Schuldners einzuschränken oder auszudehnen. Sie sind allerdings auf *Sachen* bzw. in Bezug auf die Aussonderung nach konstanter Rechtsprechung auf *körperliche Gegenstände* beschränkt[36]. Diese Inkongruenz der Begrifflichkeiten in den Art. 197 Abs. 1 und 242 SchKG führt zu unsachgerechten Lösungen.

Fussnoten

1 Die aktuelle Geldmenge bzw. Marktkapitalisierung vieler Kryptowährungen ist auf <https://coinmarketcap.com> (besucht am 10.1.2018) zu finden.

2 Die Geldmenge M1 des Schweizer Frankens lag im November 2017 bei 639 Milliarden. Quelle: SNB, abrufbar unter: <https://data.snb.ch/de/topics/snb#!/cube/snbmonagg> (besucht am 10.11.2018).

3 NZZ-Online vom 28. November 2017, Was die Zentralbanken zu Kryptowährungen wie Bitcoin sagen, abrufbar unter: <https://www.nzz.ch/finanzen/was-die-zentralbanken-zu-kryptowaehrungen-wie-bitcoin-sagen-ld.1333372> (besucht am 28.12.2017). In den Niederlanden wurden damals für einzelne Tulpensorten (bspw. für die teuerste Tulpe aller Zeiten namens *Semper Augustus*) ein Mehrfaches eines durchschnittlichen Jahreseinkommens bezahlt.

4 Financial Times vom 16.2.2018, «Crypto nation Switzerland issues guidelines to support market», abrufbar unter: <https://www.ft.com/content/737b9634-1303-11e8-8cb6-b9ccc4c4dbbb> (besucht am 16.2.2018).

5 Medienmitteilung des Bundesrats vom 18.1.2018, Arbeitsgruppe Blockchain/ICO wird ins Leben gerufen, abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-69539.html (besucht am 18.1.2018).

6 Die Schweizerische Nationalbank (SNB) führt als unabhängige Zentralbank die Geld- und Währungspolitik des Landes (Art. 99 der Schweizerischen Bundesverfassung vom 18. April 1999 [BV], SR 101). Sie muss die Preisstabilität gewährleisten. Sie ist daher durch Ausschöpfen ihrer Mittel zur Beeinflussung der Geldmenge um einen stabilen Frankenkurs bemüht, kann allerdings keinen bestimmten Wert garantieren. Vgl. im Detail zur Aufhebung des Goldstandards und zur Geld- und Währungspolitik der SNB Hettich Peter, Art. 99 N 2 und 10 ff., in: Ehrenzeller Bernhard/ Schindler Benjamin/Schweizer Rainer, J./Vallender Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., 2014.

7 Die bei Kryptowährungen üblichen elektronischen Signaturen identifizieren den unterzeichnenden zweifelsfrei als den bisherigen Inhaber der mittels der signierten Transaktion versendeten Werteinheiten. Im Kontext des neuen Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03) erfüllt eine solche Signatur nach der hier vertretenen Ansicht die Kriterien der sogenannten fortgeschrittenen elektronischen Signatur gemäss Art. 2 Abs. 1 lit. b, da sie (1) dem Inhaber zugeordnet ist, (2) der Signierende zwar nicht mit Namen, aber zweifelsfrei als Inhaber identifiziert wird, (3) sie mit einem geheimen Schlüssel erzeugt wird, der der Inhaber unter seiner alleinigen Kontrolle halten kann, und (4) sie mit den Transaktionsdaten so verknüpft ist, dass die zugehörige Transaktion nicht mehr unerkannt verändert werden kann. Der Fall einer Adresse mit mehreren Mitinhabern funktioniert analog. Die Signatur eines einzelnen Mitinhabers identifiziert diesen als solchen, aber die Transaktion erlangt erst Gültigkeit, wenn genügend viele Mitinhaber sie signiert haben.

8 Für eine detaillierte Erklärung der technischen Funktionsweise von Kryptowährungen verweisen wir auf: Meisser Luzius, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 144 ff.

9 Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht, OR), SR 220.

10 BSK OR I-Leu, Art. 84 N 4, in: Honsell Heinrich/Vogt Nedim Peter/Wiegand Wolfgang (Hrsg.), Basler Kommentar Obligationenrecht I, 6. Aufl., Basel 2015 (zit. BSK OR I-Verfasser).

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

12 Bundesgesetz vom 3. Oktober 2003 über die Schweizerische Nationalbank (Nationalbankgesetz, NBG), SR 951.11.

13 Der Schweizer Franken ist inzwischen nicht mehr an Gold gebunden. Die Goldbindung umfasste früher die Goldeinlösungspflicht, die Golddeckungspflicht und die Goldparität. Bis zur Aufhebung der Goldeinlösungspflicht der SNB durch Inkraftsetzung des alten NBG im Jahr 1954 galt Gold als gesetzliches Zahlungsmittel; Peter Nobel, Schweizerisches Finanzmarktrecht und internationale Standards, 3. Aufl., Bern 2010, § 6 N 17.

14 BSK OR I-Leu, Art. 84 N 2.

In Analogie zu individualisierbaren Sachen wie bspw. ausgeschiedenen Münzen (Geld in einem Umschlag) oder markierten Banknoten sollte das Eigentum an der Kryptowährung immerhin dann beim Hinterleger verbleiben, wenn das hinterlegte Vermögen weiterhin zuordenbar bleibt[37].

Dies muss umso mehr für Fälle gelten, in welchen für den Gläubiger faktisch kein Ausfallrisiko besteht und er deshalb nicht schutzbedürftig ist.

Die Frage kann anhand des Falles veranschaulicht werden, in dem eine Bitcoin-Adresse mit mehreren Schlüsseln gesichert ist und wovon der Schuldner nur einen hat. Diese Möglichkeit wurde bisher von den jeweiligen Autoren bei ihrer Beurteilung nicht berücksichtigt[38]. Werden Bitcoins zum Beispiel mit einer «2 out of 3 multi-signature» aufbewahrt und die drei geheimen Schlüssel auf drei verschiedene Parteien verteilt, kann der Eigentümer der Bitcoins selbst dann noch über seine Bitcoins verfügen, wenn eine der drei Parteien mit Verfügungsmacht über *einen* geheimen Schlüssel sich im Konkurs befindet und nicht mehr handlungsfähig ist.

Es stellt sich daher die Frage, was «gehören» im Sinne von Art. 197 Abs. 1 SchKG bei Kryptowährungen bedeutet: Gehört ein Bitcoin stets demjenigen, der die Verfügungsmacht hat, oder ist es auch möglich, die Bitcoins anderer trotz Verfügungsmacht lediglich zu verwalten, ohne sie in das eigene Vermögen aufzunehmen?

Nach der hier vertretenen Ansicht fallen Kryptowährungen bei geteilter Verfügungsmacht bzw. Mitgewahrsam des Schuldners nicht per se in das Vermögen des Schuldners und somit nicht in die Konkursmasse. In einem Fall, in dem der Gläubiger also ein faktisches Aussonderungsrecht hat und entsprechend kein

Fussnoten (Fortsetzung)

15 Unter elektronischem Geld versteht man zwei technisch unterschiedliche Verfahren, bei welchen Werteinheiten in einer für gesetzliche Zahlungsmittel zugelassenen Währung in digitaler Form direkt auf einem Medium gespeichert werden (bspw. auf Chipkarten, Prepaid-Karten oder auf einem PC). Vgl. auch Definition in der Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten; EZB, Bericht der Europäischen Zentralbank über Elektronisches Geld, August 1998, 8.

16 Weber Rolf H., Berner Kommentar zum schweizerischen Privatrecht, Die Erfüllung der Obligationen, Art. 68–96 OR, 2. Aufl., Bern 2004, Art. 84 OR N 15; BSK OR I-Leu, Art. 84 N 2.

17 Bärtschi Harald/Meisser Christian, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 113 ff., 142 f.; gleicher Meinung Piller François, Virtuelle Währungen – Reale Rechtsprobleme?, in: AJP 2017, 1426 ff., 1429.

18 Verwendung des Begriffs in der Verordnung der Eidgenössischen Finanzmarktaufsicht vom 3. Juni 2015 über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor (GwV-FINMA, SR 955.033.0), Art. 2 lit. c sowie im Bericht des Bundesrats zu virtuellen Währungen; vgl. zudem: Financial Action Task Force (FATF), Guidance for a Risk-Based Approach, Virtual Currencies, Juni 2015; EZB, Bericht der Europäischen Zentralbank über Virtual Currency Schemes, Oktober 2012, Ziff. 2.1, 5 und 13 sowie den ergänzenden Bericht Virtual currency schemes – a further analysis, Februar 2015.

19 Z.B. Kurant- oder Scheidemünze.

20 Vgl. FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs) vom 16. Februar 2018, 2 f.

21 Der geheime Schlüssel (auch «private key» genannt) kann jemandem zur Kenntnis gebracht bzw. digital mitgeteilt oder physisch übergeben werden. Letzteres ist zum Bespiel beim Übergeben einer physischen Casascius-Silbermünze der Fall. Diese werden in den Medien oft zur bildlichen Darstellung von Bitcoins verwendet und haben ein Siegel auf der Rückseite, hinter dem der geheime Schlüssel versteckt aufgedruckt ist.

22 Hess Martin/Lienhard Stephanie, Übertragung von Vermögenswerten auf der Blockchain, in: Jusletter, 4. Dezember 2017; Wagner Alexander/Weber Rolf, Corporate Governance auf der Blockchain, in: Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht, 1/2017, 59 ff.; Girsberger Daniel/Hermann Johannes Lukas, in: Huguenin Claire/Hilty Reto M. (Hrsg.), Schweizer Obligationenrecht 2020 – Entwurf für einen neuen allgemeinen Teil, Art. 165, 497 f.; Meisser Luzius, Die Blockchain als Standortvorteil, in: Finanz & Wirtschaft, 13. August 2016, 2; Meisser Luzius, Eine Chance für den Finanzplatz, NZZ, 27. September 2016, 10.

23 In der Schweiz ist gemäss der Aufsichtsmitteilung der FINMA (04/17) vom 29. September 2017 ein markanter Anstieg von sog. Initial Coin Offerings («ICOs») – eine digitale Form der öffentlichen Kapitalbeschaffung durch die Herausgabe von Kryptowährungen, die ausschliesslich über die Distributed Ledger bzw. Blockchain Technologie erfolgt – feststellbar. Eine allgemeingültige finanzmarktrechtliche Kategorisierung ist gemäss FINMA nicht möglich, da sich die konkrete Ausgestaltung von ICOs im Einzelfall in technischer, funktionaler und ökonomischer Hinsicht sehr stark unterscheiden.

24 In der Blockchain können beliebige Informationen gespeichert werden. Vor dem Hintergrund des EuGH Urteils C-131/12 (ECLI:EU:C:2014:317, Google-Entscheid) ist aus datenschutzrechtlicher Sicht bspw. problematisch, dass in der Blockchain enthaltene Informationen unwiderruflich gespeichert sind und diese grundsätzlich von jeder Person gelesen werden können. Es ist derzeit nicht geklärt, wie mit dem im EuGH statuierten Recht auf Vergessen in Bezug auf Personendaten, die in der Blockchain gespeichert sind, umzugehen ist. Vgl. auch Isler Michael, Datenschutz auf der Blockchain, in: Jusletter, 4. Dezember 2017.

25 Der Bund hat im Dezember 2017 eine Arbeitsgruppe ins Leben gerufen, die sich mit den Folgen von Kryptowährungen und der Blockchain-Technologie für die Schweiz befasst; Müller Jürg, «Eine Lex Bitcoin braucht es nicht», NZZ, 28. Dezember 2017, 9.

26 Kanton Zug, Behördenmitteilung, HR Zug lässt Kryptowährungen als Sacheinlage zu, 4. September 2017, abrufbar unter: <https://www.zg.ch/behoerden/volkswirtschaftsdirektion/handelsregisteramt/aktuell/bitcoin-als-sacheinlage> (besucht am 11.1.2018).

Ausfallrisiko besteht, ist es mit anderen Worten nicht sachgerecht, Vermögen des Eigentümers ohne Weiteres dem Vermögen des konkursiten Verwahrers und somit der Konkursmasse zuzuordnen bzw. den Gläubiger im Weiteren von einer Klage nach SchKG Art. 242 Abs. 1 SchKG auszuschliessen. Dies gilt grundsätzlich auch für den alleinigen Gewahrsam des Schuldners. Das heisst, dass selbst bei alleiniger Verfügungsmacht des Schuldners über Vermögenswerte des Gläubigers die Antwort, ob die Kryptowährung in die Konkursmasse fällt bzw. ob sie dem Schuldner «gehört», von den konkreten Umständen, etwa den vertraglichen Verhältnissen, der Aufbewahrungsart der Zugangsschlüssel und der Individualisierbarkeit der Vermögenswerte beim Schuldner, abhängt. ■

Fussnoten (Fortsetzung)

27 Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen (Bankengesetz, BankG), SR 952.0.

28 Botschaft des Bundesrates an die Bundesversammlung über die Revision des Bankengesetzes vom 13. Mai 1970, in: BBl 1970 I 1144, 1145; BSK BankG-Bahar/Stupp, Art. 1 N 1.

29 Bärtschi/Meisser (Fn. 15), 141; Maurenbrecher Benedikt/Meier Urs, Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen, in: Jusletter, 4. Dezember 2017, Rz. 20.

30 Eckert Martin, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, in: SJZ 112/2016 265 ff.; Maurenbrecher/Meier (Fn. 26), Rz. 20.

31 Vgl. Shannon Claude, A Mathematical Theory of Information, 1948, ACM SIGMOBILE Mobile Computing and Communications Review 5.1 (2001), 3-55.

32 Vgl. Datenschutzbeauftragter online, abrufbar unter: <https://www.datenschutzbeauftragter-online.de/datenschutz-definition-was-sind-daten/6760/> (besucht am 11.1.2018).

33 Gleicher Meinung Gobat Sébastian, Les monnaies virtuelles à l'épreuve de la LP, in: AJP 2016, 1095 ff., 1101.

34 Maurenbrecher/Meier (Fn. 28), Rz. 25.

35 BSK-SchKG II–Russenberger, Art. 242 N 7 und 10, in: Staehelin Adrian/Bauer Thomas/Staehelin Daniel (Hrsg.), Basler Kommentar Schuldbetreibung und Konkurs II, 2. Aufl., Basel 2010 (zit. BSK SchKG II-Verfasser).

36 BSK-SchKG II–Russenberger, Art. 242 N 10; BGE 128 III 388, 105 III 14, 90 III 92.

37 Geld kann nämlich im Konkurs des Verwahrers in gewissen Konstellationen gestützt auf Art. 242 SchKG ausgesondert werden. Die Vermutung von Art. 481 Abs. 2 OR würde in einem solchen Fall umgestossen. Vgl. zur Aussonderbarkeit von Geld in gewissen Konstellationen: Schönknecht Florian, Der Einlagebegriff nach Bankengesetz, in: GesKR 3/2016 300 ff.

38 Die Möglichkeit des Mitgewahrsams erwähnen bereits Graham-Siegenthaler Barbara/Furrer Andreas, The Position of Blockchain Technology and Bitcoin in Swiss Law, in: Jusletter 8. Mai 2017, Rz. 97.

39 Vgl. die Begriffsdefinition der Financial Action Task Force (FATF), Guidance for a Risk-Based Approach, Virtual Currencies, Juni 2015, 26 f.

40 Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070), 25. Juni 2014, 8. Die Subsumption unter den Begriff Vermögenswert führt letztlich dazu, dass kryptografische Währungen wie «Bitcoin» von der Gesetzgebung, insbesondere dem Strafrecht und dem Schuldbetreibungs- und Konkursrecht, erfasst werden.