

Christian Meisser / Luzius Meisser / Ronald Kogens

Verfügunngsmacht und Verfügungsrecht an Bitcoins im Konkurs

Eine auf den Eigenschaften der neuartigen Technologie aufgebaute rechtliche Einordnung unter geltendem Schweizer Recht

We propose to use the terms Verfügungsmacht (power to dispose, analogous to possession) and Verfügungsrecht (right to dispose, analogous to ownership) to discern whom a Bitcoin belongs to in case of a bankruptcy. Using the example of Tezos, we demonstrate that the storage location of private keys alone does not suffice to meaningfully answer the question to whom the foundation's assets belong. Instead, the context and the contractual arrangement, from which the right to these assets can be derived, also need to be taken into account. This view provides a legal basis for the storage of Bitcoins on behalf of a client without taking them onto one's balance sheet, ensuring that the client's assets are not included in the bankruptcy estate. Furthermore, we classify the Internet currency Bitcoin as a rival, fictive, intangible asset sui generis and opine that there is a gap in the law regarding Aussonderung (removing an asset from the bankruptcy estate and returning it to the rightful owner) and Admassierung (adding an asset to the bankruptcy estate from a third party) of Bitcoins. Courts and bankruptcy administrators are encouraged to fill this gap in accordance with article 1 of the Swiss Civil Code when faced with Bitcoins in a bankruptcy case.

Category: Articles

Region: Switzerland

Field of law: FinTech and RegTech

Citation: Christian Meisser / Luzius Meisser / Ronald Kogens, Verfügungsmacht und Verfügungsrecht an Bitcoins im Konkurs, in: Jusletter IT 24-Mai-2018

Inhaltsübersicht

1. Einleitung
2. Praxisbeispiel
3. Rechtliche Grundlagen
 - 3.1. Was sind Bitcoins und wie werden sie gehalten?
 - 3.2. Rechtsnatur von Bitcoin de lege lata: Vermögenswert sui generis
 - 3.3. Rechtsnatur des Private-Keys und der Adresse
 - 3.4. Analoge Anwendung von Prinzipien des Sachenrechts
 - 3.5. Verfügungsmacht und Verfügungsrecht
4. Konkurs des Aufbewahrers und Konsequenzen für den Berechtigten
 - 4.1. Einleitung
 - 4.2. Vorliegen einer Gesetzeslücke
 - 4.2.1. Grundsatz
 - 4.2.2. Immanenter Zweck des Konkursrechts
 - 4.2.3. Regelungen im Konkursrecht
 - 4.3. Lückenfüllung
 - 4.3.1. Unbefriedigende Lösung bei Sachdaten
 - 4.3.2. Aufbewahrung vs. Forderung
 - 4.3.3. Lückenfüllung bei Aufbewahrung von Bitcoins
 - 4.3.4. Was heisst «gehören»?
 - 4.3.5. Sachen
 - 4.3.6. Daten
 - 4.3.7. Bitcoins
 - 4.4. Was fällt in die Konkursmasse?
 - 4.5. Analoge Anwendung auf Bitcoin
5. Mithilfe der Konkursverwaltung bei der Herausgabe
6. Beurteilung des Beispielfalls
 - 6.1. Tezos
 - 6.2. Zusatzbeispiel
7. Best Practices für die Aufbewahrung

1. Einleitung

[Rz 1] Kryptowährungen und der zugrundeliegenden Technologie der Blockchain wird ein enormes Potenzial zugeschrieben.¹ Johann Schneider-Ammann spricht in diesem Zusammenhang von der «Crypto Nation Switzerland».² Diese Technologie stellt eine Chance zur Erneuerung unseres Finanzplatzes dar, die aber nur dann voll ausgeschöpft werden kann, wenn die rechtlichen Rahmenbedingungen stimmen. Eine der offenen Rechtsfragen ist die insolvenzrechtliche Behandlung von Kryptowährungen. Die Antwort darauf hat einschneidende Konsequenzen für viele im Sektor tätige Akteure, denn sie entscheidet letztendlich darüber, ob ein aufbewahrter Bitcoin als Verpflichtung in die Bilanz aufgenommen werden muss und damit allenfalls eine Einlage darstellt. Falls dem so wäre, bräuchten Unternehmen, die Bitcoins für Kunden aufbewahren, in den meisten Fällen eine Banklizenz, und Banken, die dies tun, müssten unter anderem die Bitcoins mit entsprechendem Eigenkapital hinterlegen. Solange die Bitcoins nur aufbewahrt und nicht weiter ausgeliehen oder sonstwie verwendet werden, ist das weder wirtschaftlich sinnvoll, noch

¹ Zum Beispiel: KONRAD HUMMLER, Blockchain – der nächste Wohlstandsschock, NZZ, 3. Mai 2016, S. 27; LUZIUS MEISSER, Eine Chance für den Finanzplatz, NZZ, 27. September 2016, S. 10; LUZIUS MEISSER, Die Blockchain als Standortvorteil, Finanz & Wirtschaft, 13. August 2016, S. 2.

² FADRINA HOFMANN, Schneider-Ammann will eine Crypto Nation Switzerland, Südostschweiz, 19. Januar 2018.

wird dadurch die Sicherheit für den Kunden erhöht. Für den Kunden hätte dies sogar die unerwünschte Konsequenz, dass er im Falle der Zahlungsunfähigkeit des Aufbewahrers schlechter gestellt ist, wie wenn ihm an den aufbewahrten Bitcoins eine eigentümerähnliche Position eingeräumt würde. Aufgrund der rivalisierenden Natur von Bitcoins wird in diesem Beitrag die Ansicht vertreten, dass sich, analog zu Besitz und Eigentum bei Sachen, eine getrennte Betrachtung von Verfügungsmacht und Verfügungsrecht aufdrängt. Diese beiden Begriffe sind dazu geeignet, zu klären, wem ein Bitcoin gehört und wie dieser im Konkursfall zu behandeln ist.

2. Praxisbeispiel

[Rz 2] Die Tezos Foundation ist eine Stiftung, die mittels eines Initial Coin Offerings (ICO) Bitcoins und Ether im Wert von USD 232 Millionen erhalten hat. Dank stark gestiegener Kurse dieser Kryptowährungen überstieg das Stiftungsvermögen im Dezember 2017 temporär sogar die Milliardengrenze. Die Verfügungsmacht über das Stiftungsvermögen ist auf zwei kryptographische Schlüssel aufgeteilt, von denen beide nötig sind, um eine Transaktion auszulösen. Den ersten Schlüssel hat die Stiftung selbst, der zweite Schlüssel liegt bei der Bitcoin Suisse AG.³ Zwischen beiden Parteien besteht ein «*Signature Service Agreement*», das die Bitcoin Suisse AG verpflichtet, ihre Signatur zur Freigabe von Transaktionen zu leisten; die Bitcoin Suisse AG überprüft diese davor aber zuerst auf ihre Plausibilität. Diese Form der Aufbewahrung erhöht die Sicherheit deutlich. Beispielsweise kann ein Hacker, der sich Zugang zu nur einem der beiden Schlüssel verschafft, damit nicht viel anfangen. Es fragt sich nun, ob und wie im Konkursfall einer der beiden Parteien vorgegangen werden soll und in wessen Konkursmasse das Stiftungsvermögen dann fallen würde.

3. Rechtliche Grundlagen

3.1. Was sind Bitcoins und wie werden sie gehalten?

[Rz 3] Bitcoin ist eine dezentral organisierte Internetwährung. Mittels der zugrundeliegenden Technologie der Blockchain wird jeder Bitcoin oder Bruchteile davon einer Adresse zugeordnet. Die Verfügungsmacht über die einer Adresse zugeordneten Bitcoins wird mittels einem oder mehreren kryptographischer Schlüssel (Private-Key) ausgeübt. Bitcoin wird vom Erfinder als «*digitales Bargeld*» bezeichnet, da Bitcoins wie Bargeld ohne Intermediär direkt von Person zu Person übertragen werden können.⁴ Der Preis entsteht auf dem freien Markt durch Angebot und Nachfrage. Während es sich bei Adressen und Private-Keys um Daten handelt, sind Bitcoins selbst nach informationstheoretischen Gesichtspunkten keine Daten.⁵ Die Blockchain besteht zwar aus Datenblöcken, doch sie dient lediglich als Transaktionsregister, ohne die Bitcoins selbst zu be-

³ BITCOIN SUISSE AG, Statement concerning the Tezos Crowd Contribution and the Tezos Foundation, 13. November 2017, <https://bitcoinsuisse.ch/tezos-statement> (alle Websites zuletzt besucht am 13. Mai 2018); FINNEWS, Tezos-ICO: Bitcoin Suisse weiss, wo das Geld ist, <https://finnews.ch/news/finanzplatz/29590>.

⁴ SATOSHI NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, bitcoin.org/bitcoin.pdf.

⁵ Vgl. GABRIELA HAUSER-SPÜHLER/LUZIUS MEISSER, Eigenschaften der Kryptowährung Bitcoin, in: Digma, 2018, Heft 1, S. 6.

inhalten. Letztere sind rein fiktiv.⁶ Die Blockchain des Bitcoin-Systems bezweckt einen globalen Konsens unter allen Systemteilnehmern herzustellen, welche Bitcoins aktuell welcher Adresse zugeordnet sind.⁷ Die Adresse selbst ist ein kryptographischer Fingerabdruck (Hash) der Regeln, wie man über die zugeordneten Bitcoins verfügen kann. Im einfachsten Fall genügt dafür ein einziger Private-Key und die Adresse wird aus dem zugehörigen Public-Key abgeleitet, mit welchem die Gültigkeit der Transaktion überprüft werden kann.⁸

3.2. Rechtsnatur von Bitcoin de lege lata: Vermögenswert sui generis

[Rz 4] Bitcoin ist eine alternative Währung. Die einzelnen Werteinheiten kommen aber in keiner der beiden von Währungen bekannten Formen daher. Bitcoins sind nicht Buchgeld, da sie keine Forderung darstellen.⁹ Bitcoins sind aber mangels Körperlichkeit auch nicht Bargeld. Auch stellen sie kein Mitgliedschaftsrecht oder eine sonstige geläufige Form von Vermögenswerten dar. Bitcoins sind zudem im Gegensatz zu Bitcoin-Adressen und Private-Keys auch keine Daten.¹⁰ In der Bitcoin-Blockchain werden lediglich die Transaktionsdaten (vergleichbar mit Zessionsketten bei Forderungen, aber ohne Personendaten) festgehalten, nicht aber die Bitcoins selbst abgelegt. Durch den Zugang zum Private-Key können Bitcoins tatsächlich,¹¹ sowie auch rechtlich¹² beherrscht werden. Sie sind im Gegensatz zu Daten rivalisierend, weil alternative Verwen-

⁶ SHAWN BAYERN, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE L. REV. ONLINE 22, 31 (2014).

⁷ In der Informatik ist das Finden eines Konsenses in einem Netzwerk von beschränkt zuverlässigen und beschränkt vertrauenswürdigen Teilnehmern im Allgemeinen als «Distributed Consensus» Problem bekannt. Die Blockchain ist nicht der erste, aber ein neuartiger Lösungsansatz zu diesem Problem. Vgl. ROGER WATTENHOFER, *The Science of the Blockchain*, 2016.

⁸ Dieser Sachverhalt wird oft vereinfacht dargestellt und behauptet, der Public-Key sei die Adresse. Für eine präzise Auseinandersetzung greift diese Betrachtung aber zu kurz. Da es sich bei der Adresse nur um einen Fingerabdruck handelt, sieht man ihr nicht an, welche und wie viele Schlüssel zur Ausübung der Verfügungsmacht über die zugeordneten Bitcoins nötig sind. Das heisst, man kann zwar aus dem Public-Key oder komplexeren Zugriffsregeln die Adresse herleiten, aber nicht umgekehrt. Um von einer Adresse auf die Inhaber der Verfügungsmacht über die zugeordneten Bitcoins schliessen zu können, benötigt man zusätzliche Angaben, welche nicht auf der Blockchain vorzufinden sind. Die oft verwendete Bezeichnung der Blockchain als «Eigentumsregister» ist also insofern irreführend, als es nicht möglich ist, allein aufgrund der in der Blockchain vorhandenen Daten auf den Eigentümer zu schliessen. Umgekehrt können sich aber die «Besitzer» eines Bitcoins durch Offenlegen der fehlenden Informationen zweifelsfrei als solche identifizieren.

⁹ MIRJAM EGGEN, *Chain of Contracts*, AJP 2017, S. 14; FRANÇOIS PILLER, *Virtuelle Währungen – Reale Rechtsprobleme?*, AJP 2017, S. 1428.

¹⁰ Die Verfügungsmacht an Bitcoins wird zwar mittels einer Datenstruktur, nämlich der Blockchain, festgehalten, doch das macht die Bitcoins selbst noch nicht zu Daten. Bei Buchgeld, Wertrechten, und Grundstücken, deren Besitzverhältnisse ebenfalls in geeigneten Datenstrukturen festgehalten werden, handelt es sich deswegen ja auch nicht um Daten. Daten lassen sich üblicherweise im Gegensatz zu Bitcoins frei kopieren und sind auch nicht rivalisierend. Die gegenteilige und unseres Erachtens falsche Auffassung, dass Bitcoins Daten seien, wird regelmässig repetiert ohne eine Begründung oder Quelle anzugeben.

¹¹ Tatsächliche Beherrschbarkeit liegt vor, wenn ein Rechtssubjekt ein Gut nach seinen Möglichkeiten beherrschen bzw. seinem Willen unterwerfen kann. Näheres bei: OLIVER KÄLIN, *Der Sachbegriff im schweizerischen ZGB*, Diss., Zürich 2002, S. 56; WOLFGANG WIEGAND, in: Heinrich Honsell/Nedim Peter Vogt/Thomas Geiser (Hrsg.), *Basler Kommentar, Zivilgesetzbuch Bd. II*, 5. Aufl. 2014, N 12 zu Vor Art. 641 ff. ZGB; HEINZ REY, *Die Grundlagen des Sachenrechts und das Eigentum*, Grundriss des schweizerischen Sachenrechts, Band I, 3. Aufl., Bern 2007, Rz. 77.

¹² Als rechtlich beherrschbar gilt ein Gut, wenn das positive Recht die Herrschaft darüber zulässt bzw. daran Rechte begründet werden können. Näheres bei: KÄLIN (Fn. 11), S. 58; WIEGAND (Fn. 11), N 13 zu Vor Art. 641 ff. ZGB.

dungen um ihren Einsatz konkurrieren.¹³ Aufgrund von den genannten Eigenschaften sind Bitcoins unseres Erachtens «*rivalisierende, fiktive, unkörperliche Vermögenswerte sui generis*».¹⁴

[Rz 5] In der jüngsten Zeit ist vermehrt die Diskussion entfacht, ob Bitcoins als Sachen gelten können. Die Lehre definiert Sachen als unpersönliche, körperliche, und abgrenzbare Gegenstände, welche der rechtlichen Beherrschung zugänglich sind.¹⁵ Der Sachbegriff ist aber funktioneller Natur, weshalb die Qualifikation als Sache nicht alleine von der physikalischen Beschaffenheit, sondern vor allem von der wirtschaftlichen Funktion, der Verkehrsanschauung und von ethischen Überlegungen abhängt.¹⁶ Letztendlich geben teleologische Erwägungen den Ausschlag darüber, ob die Rechtsordnung etwas als Sache anerkennt oder nicht.¹⁷ Ohne auf jedes der einzelnen Sachmerkmale einzugehen, wird hier die Ansicht vertreten, dass die Qualifikation von Bitcoins als Sache am gemäss der zurzeit herrschenden Lehre für die Sachqualität zentralen Kriterium der Körperlichkeit scheitert,¹⁸ auch wenn die weiteren Merkmale vermutlich bejaht werden können. Das Merkmal der Körperlichkeit führt zu einer Beschränkung des Sachbegriffs auf materielle Gegenstände mit räumlicher Ausdehnung bzw. einer Massenbehaftung und deren Abgrenzung zu Rechten und unkörperlichen Gegenständen.¹⁹

[Rz 6] Art. 713 Schweizerisches Zivilgesetzbuch (ZGB; SR 210) stellt den beweglichen körperlichen Sachen Naturkräfte trotz ihrer (teilweisen) Unkörperlichkeit gleich bzw. wendet die Regeln des Fahrniseigentums analog an,²⁰ sofern die jeweiligen Naturkräfte der rechtlichen Herrschaft unterworfen werden können und nicht zu den Grundstücken gehören. Unter diesen rechtlichen beherrschbaren Naturkräften sind namentlich Energien hydraulischer, elektrischer, chemischer oder nuklearer Natur einzuordnen (Wasserkraft, Elektrizität, Nuklearkraft).²¹ Unter Energie elektrischer Natur ist gemäss Bundesgericht das Zuliefern, Zuteilen und Zurverfügungstellen von Strom, zu verstehen.²² Eine Ausdehnung dieses Begriffs auf mittels elektrischer Energie produ-

¹³ KATIE SZILAGYI, A Bundle of Blockchains? Digitally Disrupting Property Law, 1 Cumberland Law Review 48 2018 (forthcoming), S. 15.

¹⁴ Fiktiv impliziert unkörperlich, aber nicht umgekehrt. So sind zum Beispiel Daten unkörperlich, aber nicht fiktiv; Von allen genannten Vermögensarten kommt Bitcoin wohl dem Bargeld am nächsten. Nur wird das Papier, welches Bargeld exklusiv an genau einen physischen Ort bindet, durch die Blockchain ersetzt, welche Bitcoins exklusiv jeweils genau einer abstrakten Adresse zuordnet.

¹⁵ WIEGAND (Fn. 11), N 6 zu Vor Art. 641 ff.; RUTH ARNET, in: Peter Breitschmid/Alexandra Rumo-Jungo (Hrsg.), Handkommentar zum Schweizer Privatrecht, Sachenrecht Bd. 3, 3. Aufl. 2016, N 6 zu Art. 641 ZGB; ARTHUR MEIER-HAYOZ, Berner Kommentar, Systematischer Teil und Allgemeine Bestimmungen, Art. 641–654 ZGB, 5. Aufl., Bern 1981, N 115 zu Sachen und andere Rechtsobjekte; REY (Fn. 11), Rz. 66 ff.

¹⁶ MEIER-HAYOZ (Fn. 15), N 115 zu Sachen und andere Rechtsobjekte; REY (Fn. 11), Rz. 68.

¹⁷ MEIER-HAYOZ (Fn. 15), N 115 zu Sachen und andere Rechtsobjekte; REY (Fn. 11), Rz. 115 f.; WIEGAND (Fn. 11), N 6 f. zu Vor Art. 641 ff.

¹⁸ Gl.M. HARALD BÄRTSCHI/CHRISTIAN MEISSER, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, S. 141; BENEDIKT MAURENBRECHER/URS MEIER, Insolvenzzrechtlicher Schutz der Nutzer virtueller Währungen, in: Jusletter 4. Dezember 2017, Rz. 20; JEAN-MARC SCHALLER, Blockchain-Serie | #2 Use-Cases: Rechtsprobleme und Lösungen, blogpost 33 vom 15. März 2018, www.finblog.ch, Rz. 10; selbstredend erfüllt aber ein unkörperliches Gut wie z.B. eine Software oder eine Datensammlung, die auf einem physischen Datenträger gespeichert wird das Kriterium der Körperlichkeit und qualifiziert unter Vorbehalt der weiteren für die Sachqualität notwendigen Kriterien als Sache.

¹⁹ WIEGAND (Fn. 11), N 10 zu Vor Art. 641 ff.; ARNET (Fn. 15), N 10 zu Art. 641 ZGB; MEIER-HAYOZ (Fn. 15), N 117 zu Sachen und andere Rechtsobjekte; REY (Fn. 11), Rz. 81.

²⁰ JÖRG SCHMID/BETTINA HÜRLIMANN-KAUP, Sachenrecht, 5. Aufl. 2017, Rz. 1080; REY (Fn. 11), Rz. 86.

²¹ SCHMID/HÜRLIMANN-KAUP (Fn. 20), Rz. 1079; IVO SCHWANDER, in: Heinrich Honsell/Nedim Peter Vogt/Thomas Geiser (Hrsg.), Basler Kommentar, Zivilgesetzbuch Bd. II, 5. Aufl. 2014, N 8 zu Vor Art. 713.

²² BGE 48 II 366 E.2.

zierte oder betriebene unkörperliche Güter ist u.E. nicht zulässig, weshalb Bitcoins gegenwärtig auch nicht unter die von der herrschenden Lehre verwendete Auslegung des Begriffs «Naturkräfte» subsumiert werden können.

3.3. Rechtsnatur des Private-Keys und der Adresse

[Rz 7] Im Gegensatz zu den Bitcoins selbst bestehen die Private-Keys und die Adressen aus einer beliebig kopierbaren Folge von Zeichen und qualifizieren deshalb als Daten.

[Rz 8] Bei der rechtlichen Einordnung von Daten wird zwischen Personendaten und Sachdaten unterschieden.²³ Beide Arten sind von Natur aus öffentliche Güter und nicht rivalisierend, was bedeutet, dass wenn eine Person Daten nutzt, können weitere Personen die gleichen Daten nutzen, ohne dass die Verwendung der ersten Person beeinträchtigt wird. Natürlich könnte der wirtschaftliche Wert der Daten durch die Nutzung durch weitere Personen negativ beeinflusst werden, was aber lediglich eine ökonomische Konsequenz, aber nicht eine Einschränkung in der Nutzung ist. Aus diesem Grund sind Daten in der Regel nicht schutzfähig und können unter geltendem Recht u.E. mangels Körperlichkeit und tatsächlicher und rechtlicher Beherrschbarkeit nicht als Sache gelten.²⁴ Eine entgegengesetzte Auslegung würde dem positiven Recht widersprechen, welches nur an Personendaten sowie gewissen Sachdaten eine eigentumsähnliche Rechtsposition einräumt (z.B. Personendaten, Sachdaten, die eine geistige Schöpfungen mit individuellem Charakter darstellen, Marken etc.), und durch die Korrelation mit dem Immaterialgüterrecht zu erheblicher Rechtsunsicherheit führen.

[Rz 9] Der Umgang mit Personendaten ist im Bundesgesetz über den Datenschutz (DSG; SR 235.1) geregelt. Darin wird den von einer Bearbeitung ihrer Personendaten betroffenen Personen gewisse Rechte zugesprochen. Diese Rechte sind aber trotz eigentumsähnlichen Charakter nicht mit den Eigentumsrechten aus dem Sachenrecht vergleichbar. Sie beschränken sich hauptsächlich auf Auskunftsrechte und Rechte bzgl. der Berichtigung, Sperrung oder Löschung von Personendaten.

[Rz 10] Auch Sachdaten sind nicht in jedem Fall geschützt. Damit Sachdaten urheberrechtlichen Schutz geniessen, muss es sich um eine geistige Schöpfungen der Literatur und Kunst mit individuellen Charakter handeln (Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, Urheberrechtsgesetz [URG; SR 231.1]). Die Rechte der ausübenden Künstler sind zudem in Art. 33 URG geschützt, die sich auf Ton- Bildaufnahmen beziehen. Ein markenrechtlicher Schutz von Daten (z.B. einer Zeichenfolge oder Buchstabenfolge) kommt nur in Frage, sofern kein absoluter oder relativer Ausschlussgrund vorliegt (Art. 2 und Art. 3 Bundesgesetz über den Schutz von Marken und Herkunftsangaben, Markenschutzgesetz [MSchG; SR 232.11]).

[Rz 11] Weitere normative Grundlage wie das Wettbewerbs-, Delikts-, Straf- und Vertragsrecht verleihen dem an Daten berechtigten keine ausschliesslichen Rechte «*erga omnes*» und auch keine positiven Herrschaftsrechte, sondern es werden lediglich gewisse Handlungen untersagt oder unter Strafe gestellt.²⁵ So zum Beispiel ist es untersagt, marktreife Arbeitsergebnisse zu über-

²³ FLORENT THOUVENIN, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 113/2017, S. 21 f.

²⁴ Gl. M. FLORENT THOUVENIN/ALFRED FRÜH/ALEXANDRE LOMBARD, Eigentum an Sachdaten: Eine Standortbestimmung, SZW 2017, S. 26; BÄRTSCHI/MEISSER (Fn. 18), S. 141; MAURENBRECHER/MEIER (Fn. 18), Rz. 20; SCHALLER (Fn. 18), Rz. 10; GIANNI FRÖHLICH-BLEULER, Eigentum an Daten?, in: Jusletter 6. März 2017, Rz. 15.

²⁵ THOUVENIN/FRÜH/LOMBARD (Fn. 24), S. 30.

nehmen (Art. 5 lit. c Bundesgesetz über den unlauteren Wettbewerb [UWG; SR 241]), unbefugt Geschäftsgeheimnisse zu verwerten (Art. 6 UWG) oder gegen die Generalklausel bzgl. Verhalten im Wettbewerb zu verstossen (Art. 2 UWG). Das Deliktsrecht ist nur relevant, sofern neben dem Schaden und der Kausalität ein widerrechtliches Verhalten sowie ein Verschulden vorliegt. Die Widerrechtlichkeit kann sich im Zusammenhang mit Daten unter anderem aus Art. 162 Schweizerisches Strafgesetzbuch (StGB; SR 311.0), Art. 143 StGB, Art. 143^{bis} StGB und Art. 144^{bis} StGB ergeben. Im Unterschied zu den mit einer Sache verbundenen Rechte, können aber allfällig Ansprüche auf Naturalrestitution nur gegenüber dem Verletzer geltend gemacht werden. Dies gilt auch für vertragliche Vereinbarungen, die nur «*inter partes*» verbindlich sind.

[Rz 12] Der Private-Key und die Adresse sind Sachdaten, die aber keine geistige Schöpfung im Sinne des Urheberrechtsgesetzes darstellen, weswegen kein urheberrechtlicher Schutz besteht. Eine Registrierung als Marke wäre rechtlich allenfalls zulässig, würde aber dem Zweck der Adresse und des Private-Keys widersprechen.²⁶ Folglich können in Zusammenhang mit dem Private-Key und der Adresse höchstens Ansprüche auf Naturalrestitution gegenüber dem Verletzer geltend gemacht werden.

3.4. Analoge Anwendung von Prinzipien des Sachenrechts

[Rz 13] Wie bereits ausgeführt, definiert die herrschende Lehre Sachen als unpersönliche, körperliche, und abgrenzbare Gegenstände, welche der tatsächlichen und rechtlichen Beherrschung zugänglich sind. Den beweglichen körperlichen Sachen werden Naturkräfte gleichgestellt bzw. finden die Regeln des Fahrniseigentums analog Anwendung,²⁷ vorausgesetzt die jeweiligen Naturkräfte sind tatsächlich und rechtlich beherrschbar. Die tatsächliche Beherrschbarkeit hängt nicht vom Rechtsobjekt ab, sondern vom Rechtssubjekt und seiner Möglichkeit, ein Gut zu beherrschen.²⁸ Als rechtlich beherrschbar (verkehrsfähig) gilt ein Gut, wenn das positive Recht die Herrschaft darüber zulässt bzw. daran Rechte begründet werden können.²⁹

[Rz 14] Neben der tatsächlichen und rechtlichen Beherrschbarkeit sind die Rechtssicherheit und das damit zusammenhängende Publizitätsprinzip weitere wichtige Elemente des Sachenrechts, um den dinglichen Rechten als absolute Rechte im Rechtsverkehr eine genaue Abgrenzung und zuverlässige Erkennbarkeit für jedermann zu verschaffen.³⁰ Publizitätsmittel für Rechte an beweglichen Sachen ist vor allem der Besitz, das Innehaben der tatsächlichen Gewalt über einen Gegenstand (aber auch bestimmte Register wie z.B. das Eigentumsvorbehaltsregister) und für Rechte an unbeweglichen Sachen das Grundbuch.³¹

[Rz 15] Die Verfügungsmacht (analog zu Besitz, siehe unten) über Bitcoins erfolgt über den Private-Key und die Zuordnung über die öffentliche, für jedermann zugängliche, dezentrale

²⁶ Die Adresse soll nicht gegen einen Gebrauch durch Dritte geschützt werden, weil sie zum Empfang von Bitcoins benötigt wird. Über den Private-Key ist gezwungenermassen strikte Geheimhaltung auszuüben. Eine Markenregistrierung würde dem entgegenwirken und rasch zum Verlust der Berechtigung an den Bitcoins führen.

²⁷ SCHMID/HÜRLIMANN-KAUP (Fn. 20), Rz. 1080; MEIER-HAYOZ (Fn. 15), N 118 zu Sachen und andere Rechtsobjekte.

²⁸ KÄLIN (Fn. 11), S. 56; WIEGAND (Fn. 11), N 12 zu Vor Art. 641 ff. ZGB: «*Tatsächliche Beherrschbarkeit: [...] die Möglichkeit, Gegenstände dem menschlichen Willen zu unterwerfen.*»

²⁹ KÄLIN (Fn. 11), S. 58; WIEGAND (Fn. 11), N 13 zu Vor Art. 641 ff. ZGB.

³⁰ FRÖHLICH-BLEULER (Fn. 24), Rz. 15; MEIER-HAYOZ (Fn. 15), N 57 ff. zu Quellen und Hilfsmittel. REY (Fn. 11), Rz. 272 ff.; ARNET (Fn. 15), N 20 zu Art. 641 ZGB.

³¹ REY (Fn. 11), Rz 278 ff.

Bitcoin-Blockchain. Auch wenn das Bitcoin-System als Ganzes kopiert werden könnte, gibt es nur eine «wahre» Bitcoin-Blockchain und die Anzahl Bitcoins ist auf 21 Millionen beschränkt.³² Eine nicht-rivalisierende Nutzung von Bitcoins ist deshalb ausgeschlossen, selbst wenn mehrere Personen Zugang zu einem Private-Key mit Einzelsignatur haben, weil die Nutzung durch eine Person die anderen Personen in deren Nutzung einschränkt. Bei Bitcoins dient aufgrund der rivalisierenden Eigenschaft die Verfügungsmacht analog zu Besitz als Publizitätsmittel. Bitcoins als «*rivalisierende, fiktive, unkörperliche Vermögenswerte sui generis*» sind folglich gewissermaßen einzigartig und können durch den Zugang zum Private-Key tatsächlich und auch rechtlich beherrscht (erworben, angeeignet, benutzt) werden. Eine analoge Anwendung gewisser sachenrechtlicher Prinzipien und eine Unterscheidung von Verfügungsmacht in Analogie zu Besitz und Verfügungsrecht als «*absolutes Recht besonderer Art*» in Analogie zu Eigentum als dingliches Recht erscheint deshalb statthaft. Dabei ist stets kritisch zu prüfen, ob und gegebenenfalls wie weit eine Norm des Sachenrechts gelten kann und gelten soll.

[Rz 16] Im Gegensatz zu Bitcoins sind der Private-Key und die Adresse als Sachdaten nicht rivalisierend, weil die Nutzung des Private-Keys und der Adresse durch eine Person, deren Nutzung durch andere Personen – abgesehen von ökonomischen Wertverlusten, die aber für die Beurteilung der Rivalität irrelevant sind – nicht einschränkt.

3.5. Verfügungsmacht und Verfügungsrecht

[Rz 17] Die Verfügungsmacht über Bitcoins hat, wer unmittelbar bestimmen kann, welcher Adresse diese als nächstes zugeordnet werden. Die Verfügungsmacht wird normalerweise mittels Private-Key ausgeübt. Welche Private-Keys in welcher Kombination dazu nötig sind, wird über die jeweilige Adresse definiert, zu der die Bitcoins zugeordnet sind. In den meisten Fällen gibt es genau einen Private-Key pro Adresse, und wer diesen kennt, kann die darauf liegenden Bitcoins mittels einer signierten Transaktion an eine neue Adresse übertragen. Die verwendeten Signaturen sind unpersönlich und lauten anders als die qualifizierten elektronischen Signaturen aus dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (ZertES; SR 943.03) nicht auf einen Namen und enthalten auch sonst keine Personendaten. Es können auch Adressen erstellt werden, die mit mehreren Private-Keys verbunden sind, so dass man eine «*Unterschrift zu zweien*» oder ähnlich direkt im System abbilden kann. In solchen Fällen spricht man von «*multi-signature*» Adressen. Zum Beispiel ist das Vereinsvermögen der Bitcoin Association Switzerland einer «*zwei von sechs multi-signature*» Adresse zugeordnet. Jedes der sechs Vorstandsmitglieder hat einen Private-Key und zwei davon sind nötig, um über die der Adresse zugeordneten Bitcoins zu verfügen.³³

[Rz 18] Die Verfügungsmacht über bestimmte Bitcoins muss nicht unbedingt direkt im Bitcoin-System abgebildet sein, um wirksam zu sein. Sie kann auch durch technische Massnahmen ausserhalb des Bitcoin-Systems geregelt werden. Ein bekanntes Beispiel dafür sind die physischen

³² Es steht jedem frei, das Bitcoin-System als Ganzes zu kopieren und diese Kopie durch geeignete Massnahmen vom Originalsystem abzugrenzen. Damit entstehen aber nicht zusätzliche Bitcoins, sondern eine neue Währung. Bekannte Kopien sind «Litecoin» und «Bitcoin Cash». Oft entstehen diese aufgrund eines Richtungsstreits unter den Entwicklern.

³³ Da die Adresse öffentlich bekannt ist, und alle Transaktionen im Bitcoin-System öffentlich sichtbar sind, kann man den Kontostand der Bitcoin Association jederzeit einsehen, zum Beispiel unter blockchain.info/address/35TTXLEtU8ZKAeTEBkx6qG7Cox8RyDw3uW.

Bitcoin-Münzen, die öfters in den Medien abgebildet werden. Bei diesen befindet sich der Private-Key hinter einem Siegel. Somit wird es möglich, die Verfügungsmacht an einem Bitcoin durch Übergabe eines physischen Objekts zu übertragen. Im Allgemeinen werden Lösungen zur Verwaltung von Private-Keys Wallets genannt. Ein Wallet hilft dabei, Private-Keys sicher aufzubewahren und vereinfacht die Handhabung von Kryptowährungen. Je nach Ausprägung des Wallets überträgt der Benutzer dem Wallet-Anbieter die Verfügungsmacht über die Bitcoins zu einem unterschiedlichen Grad.³⁴ Die entscheidende Frage ist, wessen Mitwirken nötig ist, um über die Bitcoins verfügen zu können. Diese Verfügungsmacht ist analog zum Besitz bei Sachen zu verstehen, wobei regelmässig auch Mitgewahrsam vorliegen kann.³⁵ Ergänzend zur Verfügungsmacht steht das Verfügungsrecht analog zum Eigentum als dingliches Recht, zu dessen Klärung die vertraglichen Verhältnisse berücksichtigt werden müssen.³⁶

4. Konkurs des Aufbewahrers und Konsequenzen für den Berechtigten

4.1. Einleitung

[Rz 19] Bitcoins sind mangels Körperlichkeit keine Sachen gemäss dem Gesetzeswortlaut. Ob eine Qualifikation von Bitcoins als Sache, mit der Konsequenz der Anwendung sämtlicher sachenrechtlicher Bestimmungen, überhaupt wünschenswert wäre, wird in diesem Beitrag nicht untersucht. Von praktischer Bedeutung ist zurzeit insbesondere die Frage, unter welchen Umständen Bitcoins in die Konkursmasse eines Bitcoin-Aufbewahrers fallen und ob ein Aussonderungsrecht daran besteht.

[Rz 20] Nachfolgend wird aufgezeigt, dass für Bitcoins als vollkommen neue Erscheinung eine Gesetzeslücke im Konkursrecht besteht. Aufgrund der Eigenschaften von Bitcoins bietet sich für die Füllung dieser Lücke die Anwendung von sachenrechtlichen Prinzipien an. Dies führt denn auch zu Ergebnissen, die dem mutmasslichen Willen des Gesetzgebers entsprechen.

4.2. Vorliegen einer Gesetzeslücke

4.2.1. Grundsatz

[Rz 21] In der heutigen Lehre und Rechtsprechung wird eine Gesetzeslücke definiert als eine planwidrige Unvollständigkeit innerhalb des Gesetzes. Planwidrig ist die Unvollständigkeit dann, wenn das Gesetz nach seiner Auslegung eine Antwort schuldig bleibt, obgleich nach seinem Zweck eine Antwort geboten wäre, oder wenn dem Gesetz eine Ausnahme fehlt, obwohl es nach seinem Zweck eine Ausnahme enthalten müsste. Keine Lücke liegt demgegenüber vor, wenn das Gesetz erkennbar eine Regelung enthält, die nur im Ergebnis sachlich nicht befriedigt. Während es die Aufgabe der Gerichte ist, eine planwidrige Unvollständigkeit des Gesetzes zu

³⁴ Siehe MAURENBRECHER/MEIER (Fn. 18) für eine genauere Unterscheidung verschiedener Wallet-Typen.

³⁵ Ein Beispiel für Mitgewahrsam ist der Service <https://blockchain.info>, bei welchem die geheimen Schlüssel des Benutzers verschlüsselt gelagert werden, ohne dass der Anbieter das Passwort des Benutzers kennt, das zur Entschlüsselung und damit der Verwendung der gelagerten Schlüssel notwendig ist.

³⁶ Wir danken Benedikt Maurenbrecher für die Idee zur Unterscheidung zwischen Verfügungsmacht und Verfügungsbefugnis bzw. Verfügungsrecht.

beheben, steht es ihnen grundsätzlich nicht zu, sachlich unbefriedigende Lösungen des Gesetzgebers zu korrigieren.³⁷

[Rz 22] Eine Lücke kann insbesondere «aus der Änderung des technischen, wirtschaftlichen oder sozialen Rechtsanwendungskontexts»³⁸ entstehen. Die Vollständigkeit oder Unvollständigkeit des Gesetzes ist nach den immanenten Zwecken des Gesetzes zu beurteilen.³⁹

4.2.2. Immanenter Zweck des Konkursrechts

[Rz 23] Das Bundesgesetz über Schuldbetreibung und Konkurs (SchKG; SR 281.1) soll ganz allgemein eine geordnete Zwangsvollstreckung von Ansprüchen auf Geldleistungen durch den Staat gewährleisten.⁴⁰ Im Konkurs speziell wird in der sog. Generalexekution das gesamte schuldnerische Vermögen zur Befriedigung sämtlicher Gläubiger herangezogen.⁴¹ Der immanente Zweck des Konkursrechts ist also die Befriedigung der Gläubiger des Gemeinschuldners aus dessen Vermögen.⁴² Mit der Konkurseröffnung über einen Gemeinschuldner wird hierfür ein Sondervermögen gebildet, die sog. Konkursmasse, das aus sämtlichen pfändbaren und verwertbaren⁴³ Vermögenswerten besteht, die dem Schuldner zum Zeitpunkt der Konkurseröffnung gehören,⁴⁴ und umfasst die ganze Aktivmasse⁴⁵ (vgl. Art. 197 Abs. 1 SchKG).

[Rz 24] Es ist jedoch gerade nicht Zweck des Konkursrechts, Vermögenswerte, die nicht dem Gemeinschuldner gehören bzw. nicht in dessen Aktivmasse fallen, für die Befriedigung der Gläubiger hinzuzuziehen, selbst wenn der Gemeinschuldner über solche Vermögenswerte alleine verfügen könnte.

[Rz 25] Dies spiegelt sich denn auch in der Regel wider, dass das Konkursvermögen das sein soll «was nach aussen, für Dritte, als Eigentum des Gemeinschuldners erscheint».⁴⁶

[Rz 26] Dieser Grundsatz soll unsere Richtschnur sein bei der Auslegung des Konkursrechts in Bezug auf die Frage, unter welchen Umständen Bitcoins in die Konkursmasse fallen, und ob eine Aussonderung bzw. Admassierung möglich sein soll. Zunächst wird auf die bestehenden Regelungen im Konkursrecht eingegangen und aufgezeigt, dass in der Praxis bereits für (nicht-rivalisierende) Sachdaten trotz klarerer gesetzlicher Regelung eine Lückenfüllung vorgenommen

³⁷ SUSAN EMMENEGGER/AXEL TSCHENTSCHER, Berner Kommentar zum Schweizerischen Zivilgesetzbuch, Band I Nr. 1, 2012, Art. 1–9 ZGB, N 344 f.

³⁸ EMMENEGGER/TSCHENTSCHER (Fn. 37), N 354

³⁹ EMMENEGGER/TSCHENTSCHER (Fn. 37), N 346

⁴⁰ JOLANTA KREN KOSTKIEWICZ, Schuldbetreibungs- und Konkursrecht, 2. Auflage, 2014, N 1 ff.

⁴¹ KREN KOSTKIEWICZ (Fn. 40), N 52.

⁴² Eine weitere konkursrechtliche Haftung des Schuldners, wie etwa mit der altrömischen *Klage auf Handanlegung* gegen den Schuldner, ist nicht Gesetzeszweck; HANSJÖRG PETER, 125 Jahre SchKG – 125 Jahre Rechtsprechung zum SchKG, in: Blätter für Schuldbetreibung und Konkurs 2017, S. 45–62, S. 48.

⁴³ Zur Voraussetzung der Verwertbarkeit bei Bitcoins: OLIVIER HARI, La revendication et la distraction d'office d'actifs dans une procédure d'insolvabilité: application des principes aux monnaies cryptographiques, in: GesKR 2017, S. 462.

⁴⁴ KREN KOSTKIEWICZ spricht auch vom Vermögen, das dem Schuldner «rechtlich zusteht»: KREN KOSTKIEWICZ (Fn. 40), N 1194.

⁴⁵ JOLANTA KREN KOSTKIEWICZ, in: Daniel Hunkeler (Hrsg.), Kurzkommentar Schuldbetreibungs- und Konkursrecht, 2. Auflage, 2014, Art. 197, N 2; Zur Voraussetzung der Verwertbarkeit: HARI (Fn. 43), S. 462.

⁴⁶ LUKAS HANDSCHIN/DANIEL HUNKELER, in: Daniel Staehelin/Thomas Bauer (Hrsg.), Basler Kommentar zum Bundesgesetz über Schuldbetreibung und Konkurs II, 2. Auflage, 2017, Art. 197 N 71.

wird. Sodann erörtern wir die zweckgemässe Auslegung des Konkursrechts bei Bitcoins als «*rivalisierende, fiktive, unkörperliche Vermögenswerte sui generis*».

4.2.3. Regelungen im Konkursrecht

[Rz 27] Die grundlegenden Bestimmungen des Konkursrechts in Bezug auf die Konkursmasse fassen auf zwei Konzepten des römischen Rechts, die heute selbstverständlich erscheinen: Das rechtliche Konstrukt des Eigentums als konkurssicheres, absolutes Recht, das eine Sache rechtlich einer Person zuordnet, und die Obligation, ein nicht konkurssicheres, relatives Recht bestehend aus Forderung und Schuld.⁴⁷ Um dem wirtschaftlichen und technologischen Fortschritt Rechnung zu tragen, kamen über die Jahre diverse spezialgesetzlichen Regelungen hinzu. So geniessen nun auch gewisse immaterielle Güter, insbesondere geistiges Eigentum, absoluten Schutz. Darüber hinaus finden sich diverse weitere Neuregelungen, u.a. im Bankgesetz (BankG; SR 952.0), im Versicherungsvertragsgesetz (VVG; SR 221.229.1), im Bundesgesetz über Verpfändung und Zwangsliquidation von Eisenbahn- und Schifffahrtsunternehmungen (VZEG; SR 742.211) u.v.m. Weiter bietet das Datenschutzrecht dem Datensubjekt gewisse absolute Rechte, die im Konkurs einer Verwertung von Personendaten entgegenstehen oder gar einen Herausgabeanspruch begründen können.

[Rz 28] Bereits bei Personendaten, jedoch insbesondere bei Sachdaten, steht die Konkursverwaltung vor Rechtsfragen, für die das Gesetz heute keine oder zumindest keine befriedigende Lösung bereithält: Sachdaten geniessen keinen absoluten Rechtsschutz, und die zentralen vertraglichen (relativen) Ansprüche des «*Eigentümers*» der Sachdaten, die (i) die Nutzung oder Verwertung der Daten durch den Schuldner beschränken, und (ii) einen Herausgabeanspruch begründen, sind für die Konkursmasse unverbindlich (Art. 211 SchKG).⁴⁸ Sachdaten sind indes auf einem physischen Datenträger gespeichert, so dass zumindest die sachenrechtlichen Bestimmungen indirekt zur Anwendung gebracht werden können.

[Rz 29] Gar keine spezifische Regelung enthält das Konkursrecht für Kryptowährungen wie Bitcoins, die weder Sachdaten noch Sachen sind und auch nicht auf einem Datenträger gespeichert sind. Ein in der Lehre diskutierter Ansatz wäre der Fokus auf den Private-Key als nicht-rivalisierendes Sachdatum – die sich daraus ergebenden Folgen stehen indes in offensichtlichem Widerspruch zum Gesetzeszweck. Vor dem Hintergrund der Neuartigkeit von Bitcoins liegt es nahe, dass es sich um eine planwidrige Unvollständigkeit des Gesetzes handelt.

4.3. Lückenfüllung

4.3.1. Unbefriedigende Lösung bei Sachdaten

[Rz 30] Die Schwierigkeit, für Sachdaten ein absolut geschütztes, konkurssicheres Eigentumsrecht zu konstruieren, ergibt sich aus der Tatsache, dass es ihnen an der Eigenschaft der Rivalität fehlt. Eine klare Zuordnung von Sachdaten zu einem Vermögen – also ein «*gehören*» – ist nicht oder nur schwierig zu konstruieren. Da Sachdaten zudem gezwungenermassen auf physi-

⁴⁷ PETER (Fn. 42), S. 45.

⁴⁸ KREN KOSTKIEWICZ (Fn. 40), N 1249 ff.

schen Datenträgern gespeichert sind, und Datenträger als Sache klar einem Vermögen zugeordnet werden können, folgen Sachdaten mangels anderweitiger Regelung dem physischen Datenträger. Dies führt dann zu Problemen, wenn jemand «*seine*» Sachdaten auf dem Datenträger des Konkursiten gespeichert hat. Gemäss klarem Gesetzeswortlaut fallen die Datenträger in die Konkursmasse des am physischen Datenträgers Berechtigten (Hosting-Provider). Die Datenträger sind sodann als Sachen zu verwerten. Die Sachdaten folgen mangels anderer Regelung dem Schicksal des Datenträgers. Ein gesetzlicher Herausgabeanspruch eines Kunden des Hosting-Providers in Bezug auf «*dessen*» Daten besteht nicht. Die Daten könnten somit entweder einfach vernichtet oder, falls diesen ein Verkehrswert zukommt und diese überhaupt ohne Mitwirkung des Kunden entschlüsselt werden können, mitsamt dem Datenträger verwertet werden.

[Rz 31] Bei einer teleologischen Auslegung des Begriffs «*gehören*» verstösst zumindest die Verwertung⁴⁹ u.E. auch gegen den Grundsatz, dass die Konkursmasse aus dem Vermögen des Schuldners gebildet wird, was insbesondere das sein soll, was nach aussen, für Dritte, als Eigentum des Gemeinschuldners erscheint: Ein Gläubiger eines Hosting-Providers wird kaum erwarten, dass die auf den Datenträgern von Dritten gespeicherten Sachdaten in die Aktivmasse des Hosting-Providers fallen. Problematisch ist jedoch bei dieser Auslegung, dass wegen der Eigenschaft von Sachdaten als üblicherweise nicht rivalisierend eine klare Zuordnung zu einem bestimmten Vermögen, ein «*gehören*», kaum möglich ist.

[Rz 32] Ein gewisser Schutz vor Verwertung mag zwar das Wettbewerbs- und Strafrecht bieten, wenn es sich um spezielle Kategorien von Sachdaten, wie bspw. Geschäftsgeheimnisse, handelt. Ein Herausgabeanspruch – was in der Praxis das grösste Bedürfnis sein dürfte – lässt sich aus diesen Bestimmungen indes nicht ableiten.

[Rz 33] In Luxemburg wurde dieser Mangel des Gesetzes bereits durch den Gesetzgeber behoben.⁵⁰ In der Schweiz hat indessen der Bundesrat den Handlungsbedarf (noch) nicht anerkannt,⁵¹ dafür füllen diverse Konkursämter in Anwendung der gesetzlichen Prinzipien und «*common sense*» die bestehende Regelungslücke und würden, nach eigenen Angaben, Geschäftsdaten regelmässig an Kunden von Konkursiten Hosting-Providern herausgeben.⁵²

[Rz 34] Dies zeigt, dass in der Praxis sogar bei Sachdaten unbefriedigende Resultate in konkursamtlicher Lückenfüllung gemäss dem Gesetzeszweck korrigiert werden. Ob bei der Regelung bezüglich Sachdaten tatsächlich eine Lücke besteht, die von der Judikative zu füllen ist, oder le-

⁴⁹ Zur Verwertung von Daten: DAVID SCHWANINGER/STEPHANIE S. LATTMANN, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter 11. März 2013, Rz. 58 ff.

⁵⁰ «Art. 567 Abs. 2 des Luxemburgischen Handelsgesetzes legt seit 2013 fest, dass es einen Anspruch auf Rückgabe bzw. Übergabe von nichtkörperlichen beweglichen Vermögenswerten gegenüber einer konkursiten Gesellschaft gibt. Voraussetzung ist, dass der Konkursit die Daten nur innehat (und nicht rechtlicher Inhaber daran ist), dass ihm die Daten anvertraut wurden und dass die Daten separiert werden können. Die Kosten der Herausgabe muss der Ansprechende tragen.» MARK A. REUTTER, Wenn ihr Cloud Provider bankrott geht, in: Computer Woche, 25. April 2016; s.a.: <https://www.computerworld.ch/technik/digitalisierung/cloud-provider-bankrott-geht-1341186.html>.

⁵¹ Antwort des Bundesrates zur Anfrage 14.1064 von Jean Christophe Schwaab, Muss das Konkursrecht in Bezug auf Computerdaten ergänzt werden?, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaefft?AffairId=20141064>. Dabei wird der Handlungsbedarf u.A. mit dem Argument verneint, dass ein Wechsel der Inhaberschaft nicht nur im Konkurs, sondern auch bei einer Unternehmensübernahme oder im Erbfall möglich sei. Es wird dabei verkannt, dass nur im Konkurs die vertraglichen Herausgabeansprüche und Nutzungsbeschränkungen wegfallen. Dies ist jedoch genau, was das Schutzbedürfnis hervorruft.

⁵² So REUTTER (Fn. 50): «Manchmal bieten Konkursämter aus Kulanz oder Pragmatismus dennoch Hand zur Aussonderung von Daten, ungeachtet der fehlenden gesetzlichen Grundlage.»; und PETER K. NEUENSCHWANDER, Daten im Konkurs, Vortrag an der Tagung des Schweizer Forum für Kommunikationsrecht zu Dateneigentum und Datenzugang am 29. November 2017 (siehe Folien unter: http://www.sf-fs.ch/files/sf-fs_itsl_tagungsunterlagen_dateneigentum_und_datenzugang_website.pdf).

diglich ein unbefriedigendes Ergebnis, das grundsätzlich von der Legislative zu korrigieren wäre, kann für die Beurteilung der Falles Bitcoin offen bleiben: Bitcoins sind keine Daten und nicht in einem Datenträger des Konkursiten «gefangen».

4.3.2. Aufbewahrung vs. Forderung

[Rz 35] Die nachfolgenden Ausführungen finden nur auf die Aufbewahrung von Bitcoins für einen Kunden Anwendung – sobald lediglich eine Forderung des Dritten auf Auszahlung eines Betrags in Bitcoin vorliegt, sind die Bestimmungen des Konkursrechts auf Forderungen⁵³ anzuwenden. Für die Unterscheidung zwischen Forderung und Aufbewahrung sind, ähnlich dem Hinterlegungsvertrag, die vertraglichen Abmachungen der Parteien und die Art der Aufbewahrung entscheidend. In der Praxis können folgende Fallgruppen relevant sein:

- **Einzelverwahrung:** Die Bitcoins werden für den Kunden auf einer kundenspezifischen Adresse aufbewahrt oder durch andere geeignete Massnahmen voneinander getrennt. Der Aufbewahrer hat dem Kunden dieselben Bitcoins herauszugeben. Unterformen der Einzelverwahrung sind die Aufbewahrung mit alleiniger Verfügungsmacht des Aufbewahrers und die Aufbewahrung mit geteilter Verfügungsmacht (bspw. bei multi-signature Wallets wie im eingangs erwähnten Beispiel).
- **Sammelverwahrung:** Die Bitcoins werden mit ausdrücklicher Ermächtigung des Kunden auf einer speziell für die Aufbewahrung vorgesehenen Adresse, separat von den Bitcoins des Aufbewahrers, aufbewahrt. Der Aufbewahrer hat jedem Kunden nicht die gleichen, sondern lediglich die gleiche Anzahl Bitcoins aus dem Topf der Aufbewahrung herauszugeben.⁵⁴
- **Depositum irregulare:** Die Bitcoins werden mit den Bitcoins des Aufbewahrers vermischt. Der Kunde hat lediglich Anspruch auf Herausgabe der gleichen Anzahl Bitcoins.

[Rz 36] Wie bei der Hinterlegung von vertretbaren Sachen kann nur in den ersten beiden Fällen von einer Aufbewahrung gesprochen werden. Beim sog. «*depositum irregulare*» geht nach der hier vertretenen Ansicht sowohl Verfügungsmacht als auch Verfügungsrecht auf den Konkursiten über – dem Kunden bleibt im Konkurs nur die Geltendmachung einer Forderung.⁵⁵

4.3.3. Lückenfüllung bei Aufbewahrung von Bitcoins

[Rz 37] Während das Gesetz bei Sachdaten gewisse Ansatzpunkte bietet, da diese auf einem Datenträger gespeichert sind, dessen konkursrechtliche Behandlung als Sache geregelt ist, stehen Konkursämter bei Bitcoins als «*rivalisierende, fiktive, unkörperliche Vermögenswerte sui generis*» ganz ohne spezifische gesetzliche Regelungen da. Die wohl planwidrige fehlende gesetzliche

⁵³ Zur Frage, ob eine Forderung auf Bitcoin mittels Vollstreckung von Geldzahlungen oder der Realvollstreckung durchgesetzt werden soll: FRANÇOIS PILLER, Virtuelle Währungen – Reale Rechtsprobleme?, in: AJP 2017, S. 1426–1438, S. 1433 ff.

⁵⁴ Zu diesem Thema allgemein und insbesondere zur Unterscheidung zwischen Sammelverwahrung und depositum irregulare: EUGEN BUCHER, Schweizerisches Obligationenrecht, Besonderer Teil. 3. Aufl., Zürich 1988, §16 III.

⁵⁵ Noch weiter geht das Luxemburgische Recht in Bezug auf die Aussonderung von Daten im Konkurs des Hosting-Providers: Danach genügt sogar, dass die Daten im Konkursverfahren trennbar sind. Eine getrennte Aufbewahrung davor ist nicht notwendig (<https://www.internationallawoffice.com/Newsletters/Insolvency-Restructuring/Luxembourg/NautaDutilh-Avocats-Luxembourg/New-right-to-reclaim-data-from-bankrupt-cloud-computing-providers>).

Regelung zu dieser neuen technischen Erscheinungsform von Vermögenswerten kann mit einer teleologischen Auslegung des Konkursrechts geschlossen werden.⁵⁶

[Rz 38] Wir zeigen nachfolgend auf, wie eine teleologische Auslegung des Konkursrechts⁵⁷ mit einer Behandlung von Bitcoins als «*rivalisierende, fiktive, unkörperliche Vermögenswerte sui generis*» zu sachgemässen Lösungen in der Praxis führt, die durch amtliche Lückenfüllung dem gesetzgeberischen Willen und den technologischen und wirtschaftlichen Umständen Genüge tun.

[Rz 39] Hierfür ist insbesondere der im Konkursrecht zentrale Begriff «*gehören*» gemäss dem Gesetzeszweck auszulegen und bei Strittigkeit über die Zugehörigkeit eines Bitcoins zur Konkursmasse die Aussonderung und Admassierung gemäss Art. 242 SchKG analog zur Anwendung zu bringen.

4.3.4. Was heisst «gehören»?

[Rz 40] Der Duden definiert «*gehören*» als «*jemandes Besitz, jemandes Eigentum sein*», oder als «*zu etwas zählen*». Der Wortsinn von «*gehören*» nach Art. 197 SchKG geht klarerweise über das Sacheigentum hinaus und schliesst auch andere Vermögenswerte, die zum Vermögen des Gemeinschuldners zu zählen sind, ein. Dies geht auch aus der französischen Version hervor, in der die Zugehörigkeit mit der Präposition «*du*» zum Ausdruck gebracht wird («*Tous les biens saisissables du failli*»). In diesem Sinne stützen wir die nachfolgende Beurteilung auf folgende Definition des Begriffs «*gehören*»:

[Rz 41] «*Gehören*» bedeutet, dass ein bestimmter Vermögenswert einem bestimmten Vermögen zugeordnet werden kann.

4.3.5. Sachen

[Rz 42] Für die Bestimmung des Begriffs «*gehören*» wird bei Sachen auf das sachenrechtliche *Eigentum* und nicht auf den *Besitz* abgestützt.⁵⁸ Entscheidend ist also, wer über eine Sache rechtlich verfügen *darf*, nicht wer faktisch über eine Sache verfügen *kann*.

4.3.6. Daten

[Rz 43] Nicht-rivalisierende Daten können regelmässig nicht klar einem (einigen) Vermögen zugeordnet werden: Sachdaten können gleichzeitig in zwei oder mehr Vermögen fallen, ohne dass dies den Wert, und somit die Verwertbarkeit im Konkurs, zwingend einschränkt. Eine analoge

⁵⁶ Eine parlamentarische Initiative zur Beseitigung dieser Gesetzeslücke im Sinn des vorliegenden Artikels ist pendent. Vgl. Parlamentarische Initiative von Marcel Dobler, Daten sind das höchste Gut privater Unternehmen. Datenherausgabe beim Konkurs von Providern regeln, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaefft?AffairId=20170410>.

⁵⁷ Es ist fraglich, ob sich die Gesetzeslücke auf Ebene des Zivilgesetzbuches findet, da Bitcoin darin *de lege lata*, nicht als Sache qualifiziert werden, oder ob die Gesetzeslücke im Schuld- und Konkursrecht besteht. Unseres Erachtens scheint es jedoch sachgemäss, die Analogie zum Sachenrecht nur in spezifischen Punkten zu erlauben. Eine generelle Behandlung von Bitcoins als Sache mag denn wiederum unsachgemässe Konsequenzen nach sich ziehen. Zudem besteht nach heutigem Diskussionsstand in der Lehre die grösste Lücke darin, dass die Aussonderung von Bitcoins im Konkurs nicht möglich ist.

⁵⁸ HANDSCHIN/HUNKELER (Fn. 46), Art. 197 N 8.

Anwendung des Sachenrechts erweist sich deshalb als äusserst zweifelhaft.⁵⁹ Für die konkursrechtliche Behandlung von Daten wird deswegen beim Eigentum am Datenträger angeknüpft: Fällt der Datenträger in die Konkursmasse, fallen gemäss Gesetz damit auch die darauf gespeicherten Daten in die Konkursmasse.⁶⁰

4.3.7. Bitcoins

[Rz 44] Im Unterschied zu Daten sind Bitcoins immer rivalisierend, das heisst Bitcoins können – im Gegensatz zu Daten und gleich wie Sachen – einem spezifischen Vermögen zugeordnet werden. Gleichzeitig führt das Wesen von Bitcoin als rivalisierender Vermögenswert dazu, dass diese nicht gleichzeitig mehreren Vermögen zugeordnet werden können. Die Rivalität von Bitcoins ermöglicht also nicht nur eine klare Zuordnung der Bitcoins in das Vermögen des Schuldners oder in das Vermögen eines Dritten im Konkursfall, sondern macht eine solche Zuordnung notwendig. Für die Bestimmung der Zugehörigkeit drängt es sich dabei auf, in Anlehnung zum Sachenrecht zwischen «*Verfügungsmacht*» (analog Besitz) und «*Verfügungsrecht*» (analog Eigentum) zu unterscheiden. Die Verfügungsmacht ergibt sich regelmässig aus dem Private-Key.⁶¹ Wie beim Besitz von Sachen kann die Verfügungsmacht geteilt oder nicht ausschliesslich sein. Um dem Gesetzeszweck gerecht zu werden, soll u.E. jedoch für die Zuordnung zu einem Vermögen auf das «*Verfügungsrecht*» abgestützt werden. Für das Verfügungsrecht sind die tatsächlichen, wirtschaftlichen und vertraglichen Umstände zu berücksichtigen. Dabei ist unter Beizug des Gesetzeszwecks und zum Gläubigerschutz auf die Erwartung der Gläubiger zu achten: «*Welche Bitcoins erwartet der Gläubiger in der Konkursmasse?*»

4.4. Was fällt in die Konkursmasse?

[Rz 45] Grundsätzlich fällt nur in die Konkursmasse, was dem Konkursiten «*gehört*». Nicht in die Konkursmasse fallen Vermögenswerte, die einem Dritten gehören.⁶² Bei rivalisierenden Vermögenswerten Mit- und Gesamteigentum und in strittigen Fällen sind weitere Differenzierungen für die Zuordnung eines Vermögenswerts in die Konkursmasse vorzunehmen.

[Rz 46] Vermögenswerte, die lediglich im «*Besitz*» des Schuldners stehen, sind, mit Ausnahme von offensichtlichen Fällen⁶³, mit dem Vermerk des Dritt-, Mit-, oder Gesamteigentums in das Inventar aufzunehmen. Diese fallen aber nicht in die Konkursmasse, sondern nur etwaige dem

⁵⁹ So kommen THOUVENIN/FRÜH/LOMBARD zum Schluss: «*Der Überblick über den Stand der Diskussion hat gezeigt, dass sich derzeit nicht sagen lässt, ob und gegebenenfalls in welcher Form ein Dateneigentum eingeführt werden sollte.*» Zudem: «*Eine Orientierung an den Leistungsschutzrechten oder am UWG scheint gegenwärtig am naheliegendsten. Diese Instrumente können mit dem nicht-rivalisierenden Charakter von Daten angemessen umgehen [. . .]*», THOUVENIN/FRÜH/LOMBARD (Fn. 24), S. 33 f. BENHAMOU/TRAN verweisen in ihrem differenzierten Beitrag auf ausländische Entscheide, in denen Domainnamen analog zum Sachenrecht behandelt werden – unseres Erachtens ein gutes Beispiel von *rivalisierenden* Sachdaten. YANIV BENHAMOU/LAURENT TRAN, *Circulation des biens numériques: de la commercialisation à la portabilité*, in: sic! 2016, S. 571–591, S. 575.

⁶⁰ REUTTER (Fn. 50); PETER K. NEUENSCHWANDER/SIMON OESCHGER, *Daten im Konkurs*, in: Jusletter IT Flash 11. Dezember 2017.

⁶¹ Vgl. MAURENBRECHER/MEIER (Fn. 18), welche sich allein am Private-Key orientieren. Diese Betrachtung greift unseres Erachtens zu kurz, was insbesondere bei Berücksichtigung der Möglichkeit des Mitgewahrns deutlich wird.

⁶² KREN KOSTKIEWICZ (Fn. 45), Art. 197 N 3.

⁶³ KREN KOSTKIEWICZ (Fn. 40), N 1345.

Schuldner sich daraus ergebenden Beteiligungsrechte.⁶⁴ Sind die Eigentumsverhältnisse strittig, ist der Gewahrsam entscheidend, um die Zuordnung zur Konkursmasse zu bestimmen (dies ist insbesondere für die Zuteilung der Klägerrolle bei der Aussonderung aus der Konkursmasse bzw. Admassierung zur Konkursmasse relevant). Dabei gilt: Nur, wenn der Schuldner ausschliesslichen Gewahrsam am Vermögenswert hat, fällt dieser in die Masse und es muss der Drittsprecher gegen die Konkursmasse klagen. In allen anderen Fällen muss die Masse gegen den Dritten klagen.⁶⁵ Ist das Eigentum des Drittsprechers von vornherein als bewiesen zu betrachten, kann die Konkursverwaltung den Gegenstand vor Abschluss des Konkursverfahrens herausgeben (Art. 51 Verordnung über die Geschäftsführung der Konkursämter [KOV; SR 281.32]).

[Rz 47] Es sind bei Sachen also zwei Voraussetzungen notwendig, um von vornherein zur Masse zugeordnet zu werden:

1. Die Sache gehört dem Konkursiten alleine, das heisst es liegt kein Dritt-, Mit-, oder Gesamteigentum vor.
2. Ist das Eigentum an der Sache strittig, muss die Sache zudem im «*ausschliesslichen*» Gewahrsam des Konkursiten sein.

4.5. Analoge Anwendung auf Bitcoin

[Rz 48] Wie oben dargelegt, liegt mit Bitcoin ein «*rivalisierender, fiktiver, unkörperlicher Vermögenswert sui generis*» vor, der mit Ausnahme der Körperlichkeit alle Eigenschaften von Sachen vorweist. Mangels spezifischer gesetzlicher Regelung drängt sich eine analoge Anwendung der Rechtsprechung zum Begriff des «*Gehörens*» bei Sachen auf Bitcoins auf. Dabei helfen die Begriffe der Verfügungsmacht und des Verfügungsrechts.⁶⁶

[Rz 49] Um Mängel in der Zuordnung zur Konkursmasse zu korrigieren, ist die Admassierung und Aussonderung für die Erreichung des Gesetzeszwecks ein notwendiger nächster Schritt. Ohne Aussonderung würden entgegen dem Gesetzeszweck Vermögenswerte, die nicht dem Gemeinschuldner gehören, der Masse zufallen.

[Rz 50] Ein weiteres gewichtiges Argument für die Aussonderung von Bitcoins ist, dass die Publizitätswirkung des Besitzes an Sachen ausgeprägter ist als bei Bitcoins: Sachen im Besitz des Gemeinschuldners erscheinen regelmässig ohne dessen Zutun nach aussen, für Dritte, als dessen Eigentum. Ein Gläubiger läuft somit Gefahr, vom Sachbesitz des besitzenden Nichteigentümers über dessen Kreditwürdigkeit in die Irre geführt zu werden. Die Aussonderung von Sachen aus der Konkursmasse durchbricht die Regel, dass in die Konkursmasse fällt, was nach aussen, für Dritte, als Eigentum des Gemeinschuldners erscheint. Der Gesetzgeber hat dennoch eine Aussonderung bei Sachen (zu Recht) zugelassen.

[Rz 51] Die pseudonyme Natur der Bitcoin-Blockchain erfordert für die Publizitätswirkung im Normalfall ein aktives Zutun des Aufbewahrers, etwa mittels Demonstration der Verfügungsmacht durch Ausführung einer Transaktion. Die Gefahr, dass ein Gläubiger die Bitcoins eines

⁶⁴ HANDSCHIN/HUNKELER (Fn. 46), Art. 197 N 66.

⁶⁵ KREN KOSTKIEWICZ (Fn. 40), N 1304.

⁶⁶ Gemäss Art. 197 SchKG bildet alles, was dem Schuldner gehört, eine einzige Masse, «*gleichviel wo es sich befindet*». Dies ist ein zusätzlicher Hinweis darauf, dass der Ort (was bei Bitcoin am ehesten der Adresse und der damit verbundenen Verfügungsmacht entspricht) nicht das entscheidende Merkmal der Zuordnung ist, sondern dass die tatsächlichen Eigentumsverhältnisse (bei Bitcoin das Verfügungsrecht) entscheidend sind.

Aufbewahrsers fälschlicherweise dessen Vermögen zuordnet, ist demnach wesentlich geringer als beim Sachbesitz. Eine Aussonderung bei Bitcoins ist damit ein geringerer Eingriff in den Gläubigerschutz als bei Sachen. Wenn der Gesetzgeber nun aber eine Aussonderung bereits bei Sachen zulässt, muss dies nach dem mutmasslichen gesetzgeberischen Willen umso mehr für Bitcoins möglich sein.

[Rz 52] Es ergibt sich somit für die Zuordnung von Bitcoins in die Konkursmasse folgendes Bild:

- **Ausschliessliche Verfügungsmacht mit Verfügungsrecht:** Der Konkursit kann ohne Zutun Dritter über die Bitcoins verfügen. Die Bitcoins sind wirtschaftlich dem Vermögen des Konkursiten zuzuordnen. Die Bitcoins fallen in die Konkursmasse.
- **Ausschliessliche Verfügungsmacht ohne Verfügungsrecht:** Der Konkursit kann als einziger und ohne Zutun Dritter über die Bitcoins verfügen. Die Bitcoins sind wirtschaftlich einem Dritten zuzuordnen. Ist das Verfügungsrecht des Dritten als bewiesen zu betrachten, kann die Konkursverwaltung die Bitcoins herausgeben. Ansonsten fallen die Bitcoins in die Konkursmasse und müssten ggf. mittels Aussonderungsklage wieder herausgelöst werden.
- **Nicht ausschliessliche Verfügungsmacht mit Verfügungsrecht:** Der Konkursit kann nicht alleine oder nicht als einziger über die Bitcoins verfügen, die Bitcoins sind jedoch wirtschaftlich dem Konkursiten zuzuordnen. Ist das Verfügungsrecht strittig, fallen die Bitcoins mangels ausschliesslichem Gewahrsam nicht in die Konkursmasse, können aber ggf. mittels Admassierungsklage hinzugezogen werden.
- **Nicht ausschliessliche Verfügungsmacht ohne Verfügungsrecht:** Der Konkursit kann nicht alleine oder nicht als einziger über die Bitcoins verfügen, und die Bitcoins sind wirtschaftlich einem Dritten zuzuordnen. Die Bitcoins fallen mangels ausschliesslichem Gewahrsam und mangels Verfügungsrecht nicht in die Konkursmasse. Die Bitcoins sind, soweit der Verfügungsberechtigte nicht ohne den Schuldner über die Bitcoins verfügen kann, an den Verfügungsberechtigten zu übertragen.

[Rz 53] Die Klärung des Begriffs «gehören» für Bitcoin im Kontext von Art. 197 SchKG ist eine zwingende Voraussetzung zur Bildung der Konkursmasse. Die Frage besteht hier lediglich darin, welches die richtige Deutung des Begriffes ist, und nicht, ob eine Deutung vorgenommen werden muss. Im Gegensatz dazu muss für die Aussonderung und Admassierung zunächst die Frage beantwortet werden, ob eine Gesetzeslücke vorliegt. Wird dies bejaht und die sachähnliche Natur von Bitcoins anerkannt, sollten gemäss dem Gesetzeszweck die Aussonderung und Admassierung ebenfalls zur Anwendung kommen.

5. Mithilfe der Konkursverwaltung bei der Herausgabe

[Rz 54] Ein insbesondere praktisches Problem ist, wie die Konkursverwaltung den Bitcoin-Verfügungsberechtigten bei der Herausgabe der Bitcoins unterstützt, da dies einiges an technischer Expertise voraussetzt. Bei Sachen wird es in der Praxis regelmässig am Eigentümer sein, die Sache beim Konkursamt abzuholen. Analog hierzu drängt sich mindestens eine Kostendeckungspflicht des Bitcoin-Verfügungsberechtigten auf.

6. Beurteilung des Beispielfalls

6.1. Tezos

[Rz 55] Das Beispiel Tezos veranschaulicht das Spannungsfeld zwischen Gesetz und Gesetzeszweck bestens (Beschreibung s.o.). Würde, rein hypothetisch, die Bitcoin Suisse AG in Konkurs fallen, steht das Konkursamt vor einer delikaten Aufgabe: Soll es (i) sich auf eine grammatikalische Auslegung des Gesetzestextes stützen und Ergebnisse in Kauf nehmen, die gegen den immanenten Gesetzeszweck und den klaren wirtschaftlichen Willen und guten Glauben der involvierten Parteien verstossen; oder (ii) in einer amtlichen Lückenfüllung den mutmasslichen Willen des Gesetzgebers umsetzen und den wirtschaftlichen Gegebenheiten Rechnung tragen?

[Rz 56] Der Konkursverwalter würde bei Inventaraufnahme einen Datenträger vorfinden, auf dem der zweite Private-Key zum Bitcoin-Vermögen der Tezos Stiftung gespeichert ist. Der Private-Key der Bitcoin Suisse AG alleine verleiht keine Verfügungsmacht – nur gemeinsam mit dem Private-Key der Tezos Stiftung kann über die Bitcoins verfügt werden. Immerhin der erste Schritt des Konkursamts ist unstrittig: Der Datenträger fällt als Sache in die Konkursmasse. Als nächster Schritt steht das Konkursamt vor mehreren Möglichkeiten:

- **Fokus auf den Private-Key als Datum I:** Um eine Verletzung von etwaigen Geschäftsgeheimnissen oder Personendatenschutzrechten zu vermeiden, werden vorsichtshalber sämtliche Datenträger formatiert und der Datenträger verwertet. Das Vermögen der Tezos Stiftung wäre damit für immer verloren, womit weder den Gläubigern der Konkursmasse noch der Tezos Stiftung gedient wäre.
- **Fokus auf den Private-Key als Datum II:** Der Datenträger wird mitsamt gespeicherten Daten⁶⁷ versteigert. Der wirtschaftliche Wert des Datenträgers ergibt sich dabei hauptsächlich aus dem darauf gespeicherten zweiten Private-Key: Wieviel erwartet der Höchstbietende von der Tezos Stiftung für die Herausgabe des Private-Key zu erhalten? Sowohl aus spieltheoretischer Sicht als auch für die Gläubiger wäre dies durchaus interessant. Neben ethischen (wenn nicht gar strafrechtlichen) Bedenken führt dies jedoch aus wirtschaftlicher Sicht zu einem absurden Ergebnis: Wäre der Verwertungserlös etwa die Hälfte des Vermögens der Tezos Stiftung, würde sich die Bilanzsumme der Konkursmasse plötzlich um eine halbe Milliarde erhöhen, was im Konkursverfahren zu einem massiven Überschuss führen dürfte. Anders gesagt: Eine Bewertung der Bitcoin Suisse AG nach Liquidationswert wäre also wesentlich höher als eine Bewertung nach «going-concern» Prinzipien. Alternativ müsste die Bitcoin Suisse AG schon heute den erwarteten Verwertungserlös in ihre Bilanz aufnehmen – was mangels Bewertbarkeit ebenfalls kaum sinnvoll umzusetzen wäre. Weiter ist die Erwartung der Gläubiger zu berücksichtigen: Keiner dürfte beim Abschluss von Geschäften mit der Bitcoin Suisse AG erwartet haben, dass ein Teil des Vermögens der Tezos Stiftung der Bitcoin Suisse AG gehört.
- **Fokus auf Bitcoin als «rivalisierende, fiktive, unkörperliche Vermögenswerte sui generis» mit analoger Anwendung des Sachenrechts:** Die Konkursverwaltung nimmt die Bitcoins der Tezos Stiftung im Inventar mit dem Vermerk des Drittanspruchs auf. Da die Verhältnisse klar sind, überträgt die Konkursverwaltung in Rücksprache mit der Tezos Stiftung und mit Hilfe von Fachpersonal die Bitcoins in die alleinige Verfügungsmacht der Tezos

⁶⁷ Der Einfachheit halber wird davon ausgegangen, dass der Datenträger entschlüsselt bzw. mit Zugangscode versteigert wird.

Stiftung. Falls Zweifel am Verfügungsrecht der Tezos Stiftung an den Bitcoins bestehen, müsste die Masse auf Admassierung der Bitcoins gegen die Tezos Stiftung klagen. Die Tezos Stiftung vergütet die Konkursmasse für den entstandenen Aufwand.

6.2. Zusatzbeispiel

[Rz 57] Zum Zeitpunkt des Verfassens kann man mit folgendem Private-Key unter Verwendung einer geeigneten Wallet-App über 0.01 Bitcoins im Gegenwert von rund 80 CHF aus dem Vermögen der Autoren verfügen:



[Rz 58] Einen Private-Key zu publizieren ist etwa so vernünftig, wie ein Fahrrad am Bahnhof unabgeschlossen stehenzulassen, und es fragt sich, wie lange es geht, bis sich jemand diese 0.01 Bitcoins aneignet.⁶⁸ Doch hilft dieses Beispiel, die Problemstellung zu illustrieren: Was fällt in die Konkursmasse der Beispiel AG, wenn diese vor ihrem Konkurs

- I. diesen Artikel inkl. Private-Key ausdruckt?
- II. diesen Artikel auf Google Drive speichert?
- III. mit dem Private-Key die Bitcoins auf eine von ihr alleine kontrollierte Adresse überträgt?

[Rz 59] Gemäss der hier vertretenen Ansicht fallen die Bitcoins in den Fallbeispielen 1. und 2. nicht in die Konkursmasse mangels Ausschliesslichkeit der Verfügungsmacht. Es besteht mangels Verfügungsrecht auch keine Möglichkeit der Admassierung. Im 3. Fall werden die Bitcoins mit dem Vermerk der Verfügungsberechtigung eines Dritten inventarisiert, fallen aber nicht in die Konkursmasse (sofern entsprechend dokumentiert). Sind die Verfügungsberechtigten nicht ersichtlich, wird das Verfügungsrecht aufgrund ihrer ausschliesslichen Verfügungsmacht bei der Beispiel AG vermutet und die Bitcoins fallen in die Konkursmasse. Die Autoren könnten indes eine Herausgabe bzw. Aussonderung verlangen, sofern sie die Vermutung umstossen können und nachweisen, dass sie nach wie vor die Verfügungsberechtigten sind.

⁶⁸ Ob die 0.01 Bitcoins noch da sind, lässt sich unter sameblockchain.info/de/address/17sXedYBwciV9phuhX1HtHEXSjnZxHvHME überprüfen.

7. Best Practices für die Aufbewahrung

[Rz 60] Aufgrund der vorliegenden Erwägungen können Best Practices zur Aufbewahrung von Kryptowährungen formuliert werden. Unseres Erachtens sind dabei folgende Punkte wichtig:

1. Aus der Vertragsbeziehung zum Kunden muss hervorgehen, dass die Bitcoins vom Aufbewahrer lediglich aufbewahrt werden und es sich nicht um ein Guthaben oder eine sonstige Forderung gegenüber dem Aufbewahrer handelt.
2. Für den effektiven Gläubigerschutz darf gegen aussen nicht der Eindruck erweckt werden, dass die aufbewahrten Bitcoins dem Aufbewahrer gehören.
3. Für Bitcoins in der Verfügungsmacht des Aufbewahrers muss jederzeit der Verfügungsrechte festgestellt werden können.
4. Die Segregierung der Kundenvermögen kann, muss aber nicht, direkt auf der Blockchain durch Verwenden separater Adressen pro Kunde erfolgen. Erfolgt die Segregierung auf einer höheren Ebene, ist es von Vorteil, diese nicht nur buchhalterisch vorzunehmen, sondern auch mit geeigneten technischen Mitteln zu unterstützen. Bei einer Sammelverwahrung ist dies explizit im Vertrag zu erwähnen oder nachträglich die Zustimmung des Kunden einzuholen.
5. Der Kunde sollte idealerweise die Möglichkeit haben, in Erfahrung zu bringen, welche Bitcoins ihm zu einem bestimmten Zeitpunkt zugeordnet sind. Diese Zuordnung von Bitcoins zu einem Kunden sollte, soweit dies die operativen Anforderungen zulassen, stabil sein.
6. Die wichtigste Segregierung ist die der Kundenvermögen von dem des Aufbewahrers. Damit ist es bereits klar, welche Bitcoins in die Konkursmasse fallen, bevor im Detail festgestellt wurde, welchen Kunden diese gehören.
7. Gehen Bitcoins verloren und haftet der Aufbewahrer für den Verlust, dann haftet der Aufbewahrer konsequenterweise nur gegenüber demjenigen Kunden, dem die verlorenen Bitcoins zum Zeitpunkt des Verlustes zugeordnet waren. Im Gegensatz dazu steht die bei Forderungen übliche, gleichmässige Aufteilung des Verlustes auf die Kunden, wie diese zum Beispiel Bitfinex im Sommer 2016 vorgenommen hat. In solchen Fällen wünschenswert wäre eine entsprechende Versicherung, wie sie zum Beispiel der Aufbewahrer Xapo abgeschlossen hat.

[Rz 61] Eine technisch und rechtlich interessante, aber je nach operationellen Anforderungen auch sehr aufwändige Aufbewahrungsart ist die Aufteilung der Verfügungsmacht auf mehrere Parteien, zum Beispiel mittels 2-von-3 multi-signature Adressen, deren Schlüssel bei unabhängigen Parteien liegen. Damit kann der Kunde selbst im Konkursfall einer der Parteien ohne Mitwirken des Konkursverwalters sein Verfügungsrecht weiterhin ausüben. Da die Bitcoins unter Mitgewahrsam stehen, fallen sie ohnehin nicht in die Konkursmasse. Eine weniger aufwändige Variante des Mitgewahrsams ist das Hinterlegen von Backups der Schlüssel bei entsprechend instruierten Dritten oder beim jeweiligen Kunden. In beiden Varianten entstehen aber durch das Involvieren zusätzlicher Parteien auch zusätzlicher Risiken, so dass ein Einsatz sorgfältig abgewogen werden muss.

[Rz 62] Schlussendlich muss jede Massnahme im jeweiligen Kontext sinnvoll sein. Gerade in innovativen Geschäftsfeldern darf man sich nicht blind auf Best Practices oder andere Empfehlungen verlassen. Dementsprechend können die vorliegenden Best Practices lediglich als Orientierungshilfe dienen. Sie sind kein Ersatz für eigenen Sachverstand.

CHRISTIAN MEISSER, Rechtsanwalt, lic. iur., MBA, Regulatory Working Group Bitcoin Association Switzerland, LEXR AG.

LUZIUS MEISSER, MSc Computer Science ETH, Regulatory Working Group Bitcoin Association Switzerland, Meisser Economics AG.

RONALD KOGENS, Rechtsanwalt, LL.M., Regulatory Working Group Bitcoin Association Switzerland, FRORIEP Legal AG.