

# Privatrechtliche Einordnung virtueller Währungen

Oliver Völkel

**Mit der Verbreitung virtueller Währungen wie Bitcoin muss sich die Rechtswissenschaft die Frage stellen, wie mit diesem neuen Phänomen privatrechtlich umzugehen ist. Die unternehmerische Praxis ist derzeit augenscheinlich noch verunsichert oder lebt nach dem Prinzip *Ubi non accusator, ibi non iudex*. Dieser Beitrag zeigt auf, wo eine Klärung offener Fragen geboten ist, und bietet erste Ansatzpunkte für die Behandlung des derivativen Erwerbs durch Rechtsgeschäft sowie die Nutzung virtueller Währungen als Sicherheiten. Keinesfalls erhebt der Autor mit diesem Beitrag einen Anspruch auf letztgültige Lösung, vielmehr soll der Beitrag als Grundlage für den weiteren Diskurs dienen.**

Stichwörter: Virtuelle Währung, Kryptowährung, Bitcoin, Ether, Blockchain, Privatrecht, Kauf, Tausch, Pfandrecht, derivativer Erwerb, originärer Erwerb, smart contracts.

JEL-Classification: E 42, K 11.

With the spread of virtual currencies such as Bitcoin, the legal science must also start asking how this new phenomenon is to be treated in private law. At the moment, the entrepreneurial practice is still unsettled or lives according to the principle of *Ubi non accusator, ibi non iudex*. This paper shows where clarification of open questions is needed and discusses how derivative acquisition of virtual currencies can be achieved as well as how virtual currencies can serve as collateral. In any case, the author does not claim to provide ultimate solutions to these question; rather, the contribution is intended as a basis for further discourse.

## 1. Einleitung: Virtuelle Währungen in der Praxis

In der Praxis besteht großes Interesse an der Frage, wie virtuelle Währungen (Kryptowährungen) privatrechtlich ein-

zuordnen sind. Jeder Unternehmer, dessen Geschäftsmodell den Umgang mit virtuellen Währungen betrifft, benötigt klare Antworten. Die Verwirrung in der Praxis beginnt bereits bei so grundsätzlichen Angelegenheiten wie der Verschaffung von Eigentum bzw. Rechtszuständigkeit an den neuartigen Werten. Was, wenn mein Vormann gar nicht darüber verfügen durfte?

Für heimische Banken scheinen virtuelle Währungen derzeit überhaupt noch ein rotes Tuch zu sein. Es ist eine deutliche Abneigung zu bemerken, überhaupt mit Unternehmen aus der neuen Branche Geschäftsbeziehungen einzugehen. Bloß der Gedanke an die Gewährung einer Finanzierung scheint Kopfschmerzen zu bereiten. Diese Haltung ist nicht unverständlich, immerhin sind für die Bankenpraxis grundlegende Fragen bislang ungeklärt. Wie sicher ist die Eigentumsposition bei virtuellen Währungen? Können Kryptowährungen eines Kunden als Pfand taugen? Wie kann an ihnen wirksam ein Pfandrecht bestellt werden?

Ebenfalls von auffallendem Interesse in der Praxis ist die Frage nach der Rückabwicklung von Transaktionen. Eine spurlose Rückabwicklung ist wegen der verwendeten Technologie ausgeschlossen. Jede Übertragung von virtuellen Währungseinheiten wird permanent in einem zentralen Verzeichnis vermerkt. Wie wirkt sich dies beispielsweise bei der Geltendmachung von sachenrechtlich *extunc* wirkenden Mängeln im Vertragsrecht aus?

Eng mit den oben genannten Aspekten verbunden ist auch die Frage des Schicksals virtueller Währungen im Fall der Insolvenz eines Unternehmens. Können Ab- und Aussonderungsrechte wirksam geltend gemacht werden und wenn ja, unter welchen Voraussetzungen? Kryptowährungen erfüllen in der Regel Zahlungsfunktion, solche Rechtsfolgen sind also nicht immer gewünscht.

Der Beitrag basiert auf einem Vortrag vom 30. März 2017 am Juridikum Wien. Der Autor möchte an dieser Stelle Dr. Koji Takahashi danken, Professor an der Doshisha University Law School (Kyoto, Japan). Prof. Takahashi forscht unter anderem im Bereich Blockchain und internationaler Handel. Die Idee für diesen Artikel ist beim gemeinsamen Gespräch



Photo: privat

RA Dr. Oliver Völkel, LL.M.,  
Stadler Völkel Rechtsanwälte  
GmbH;  
e-mail: oliver.voelkel@svlaw.at

Neugründungen von Unternehmen, die mit virtuellen Währungen umgehen, haben nach der Wahrnehmung des Autors derzeit Hochkonjunktur. Banken beginnen, die rechtlichen Rahmenbedingungen zu sondieren. In der Praxis werden Kryptowährungen oft eingesetzt, ohne sich mit Rechtsfragen lange auseinanderzusetzen. Die Nutzer beugen sich der Technik.

Gerichtliche Entscheidungen sind weltweit bislang rar. Zumindest wissen wir, dass der An- und Verkauf von Bitcoin – der wohl bekanntesten virtuellen Währung – nicht umsatzsteuerpflichtig ist.<sup>1)</sup> Mit der weiteren Verbreitung virtueller Währungen werden erste gerichtliche Auseinandersetzungen jedoch nicht mehr lange auf sich warten lassen. Umso wichtiger, dass die Rechtswissenschaft darauf vorbereitet ist.

In diesem Beitrag wird zunächst der technische Hintergrund virtueller Währungen erläutert. Daran anschließend wird eine Subsumption unter den bürgerlich-rechtlichen Sachbegriff vorgenommen.

entstanden. Viele wertvolle Überlegungen finden sich auf Prof. Takahashis Blog unter <http://cryptocurrencylaw.blogspot.co.at>. Weiters spricht der Autor Philipp Ley seinen Dank aus, der in der Vorbereitung dieses Artikels einen wertvollen Beitrag geleistet hat.

1) EuGH 22.10.2015, C-264/14.

Es folgt die Auseinandersetzung mit dem derivativen Erwerb durch Rechtsgeschäft sowie bestimmten Formen des originären Erwerbs. Den Abschluss bilden erste Überlegungen zur Frage der Sicherheitbestellung.

## 2. Definition und technischer Hintergrund

Virtuelle Währungen sind ein recht junges Phänomen. Es verwundert also nicht, dass bis heute noch keine Legaldefinition existiert. Ein erster Versuch einer gesetzgeberischen Annäherung findet derzeit mit der Erarbeitung der fünften Geldwäscherichtlinie statt. Der aktuelle Entwurf<sup>2)</sup> definiert virtuelle Währungen (*virtual currencies*) als:

*“digital representation of value that can be digitally transferred, stored or traded and functions as a medium of exchange, but does not have legal tender status in any jurisdiction and which is not funds as defined in point (25) of Article 4 of the Directive 2015/2366/EC nor monetary value stored on instruments exempted as specified in Article 3(k) and 3(l) of that Directive”.*

Diese Legaldefinition wird den Besonderheiten virtueller Währungen allerdings nicht gerecht. Um diese Besonderheiten rechtlich würdigen zu können, ist ein Verständnis der zugrunde liegenden Blockchain-Technologie (auch als *distributed ledger* bezeichnet) unerlässlich.

Ein *distributed ledger* ist ein öffentliches, dezentral geführtes Kontobuch. Es dient dazu, im digitalen Zahlungs- und Geschäftsverkehr Transaktionen von Nutzer zu Nutzer aufzuzeichnen. „Öffentlich“ bedeutet, dass jeder Nutzer in jede stattgefunden Transaktion Einsicht nehmen kann. Im Kontobuch wird die gesamte Transaktionshistorie abgespeichert. „Dezentral“ bedeutet, dass es keine zentrale Stelle gibt, die das Kontobuch führt. Die Verwaltung wird in einem *peer-to-peer*-Netzwerk zwischen etlichen Knoten synchronisiert. Jeder kann an der Verwaltung des Kontobuchs teilnehmen.

Die Nutzer virtueller Währungen können in der Regel eine beliebige Anzahl neuer leerer Konten im Kontobuch erschaffen. Diese Konten werden technisch als Adresse bezeichnet. Bei der Adresse handelt es sich um eine alphanumerische Zeichenfolge, beispielsweise: „3LLd3dVrhCWxo9igTUWDoXPsqCFdzxqkBm“. Aus dem Kontobuch ist ersichtlich, wel-

cher Betrag einer virtuellen Währung welcher Adresse zugewiesen ist.

Die Blockchain-Technologie stellt sicher, dass unter allen Teilnehmern im *peer-to-peer*-Netzwerk stets Einigkeit darüber besteht, ob und wann eine Transaktion stattgefunden hat. Um dies zu erreichen, werden zunächst alle neuen Transaktionen in einem Pool unbestätigter Transaktionen gesammelt. Jede einzelne Transaktion beschreibt, welche Menge einer virtuellen Währungseinheit von welcher Absender-Adresse an welche Empfänger-Adresse übertragen werden soll.

Zur Bestätigung der Transaktionen prüfen alle im *peer-to-peer*-Netzwerk arbeitenden Rechner parallel, ob die gepoolten Transaktionen im Widerspruch zur bisherigen Transaktionshistorie stehen. Erscheinen die neuen Transaktionen legitim, weil kein Widerspruch zu erkennen ist (etwa eine Doppelübertragung von Einheiten), so werden die Transaktionen bestätigt. Die Bestätigung erfolgt durch das Lösen einer komplexen mathematischen Aufgabe. Der Rechner, der die gepoolten Transaktionen als erster durch Lösen dieser Aufgabe bestätigen kann, hält dies in Form eines neuen „Blocks“ fest. Dieser neu errechnete Block an Transaktionsinformationen wird an alle anderen teilnehmenden Rechner im Netzwerk verteilt. Sobald ein Block errechnet und im Netzwerk verteilt wurde, beginnt die Bestätigung des nächsten Blocks an Transaktionen. Im Laufe der Zeit reiht sich so ein Block mit bestätigten Transaktionen an den nächsten, daher der Name „Blockchain“.

Während ein Block errechnet wird, langen im Netzwerk freilich laufend neue Transaktionen ein, die auf eine Bestätigung warten. Es kann auch vorkommen, dass zwei Rechner zeitgleich einen neuen Block errechnen. Die Blockchain hat in einem solchen Fall plötzlich zwei Enden mit möglicherweise unterschiedlichen bestätigten Transaktionen. Für dieses Problem besteht eine Lösung. Anfangs werden beide neuen Enden der Blockchain vom Netzwerk als gültig betrachtet und gleichwertig behandelt. Die Rechner im Netzwerk arbeiten parallel an beiden Enden, um die Blockchain weiterzurechnen. An einem der beiden Enden wird ein neuer Transaktionsblock jedoch schneller errechnet werden als an dem anderen Ende. Ein Ende der Kette ist dann länger als das andere. Das Blockchain-Protokoll sieht vor, dass nur die längste Verzweigung weitergerech-

net wird, also jenes Kettenende mit den meisten Transaktionsblöcken. Binnen kurzer Zeit herrscht also im Netzwerk wieder Einigkeit darüber, welches Kettenende gültig sein soll. Alle Transaktionen, die in der anderen Verzweigung abgespeichert wurden, fallen automatisch in den Pool der nicht bestätigten Transaktionen zurück. Diese Transaktionen werden dann an einer späteren Stelle in der Blockchain bestätigt.

Eine weitere Besonderheit virtueller Währungen ist der Einsatz von digitalen Signaturen zur Bestätigung von Transaktionen. Beim Anlegen einer neuen Adresse – also dem Anlegen eines neuen Kontos im Kontobuch – wird ein privater Schlüssel (*private key*) zur Signierung von Transaktionen erzeugt. Zu jeder Adresse besteht ein solcher privater Schlüssel. Er ist nur demjenigen bekannt, der die Adresse angelegt hat.

Um Einheiten einer virtuellen Währung zu empfangen, genügt die Nennung der Adresse. Für das Übertragen von einer Absender-Adresse an eine Empfänger-Adresse ist hingegen die Kenntnis des privaten Schlüssels erforderlich. Nur diejenige Person, die den privaten Schlüssel kennt, kann die Übertragung an eine andere Adresse ermöglichen.

Der private Schlüssel kann digital abgespeichert oder aber auch ausgedruckt und abgelegt werden. Oft wird der private Schlüssel bei einem Dritten hinterlegt. Dies ist bei der Benutzung einer Wallet der Fall. Bei einer Wallet handelt es sich um eine Anwendung, mit der Nutzer Adressen einer virtuellen Währung und die dazugehörigen privaten Schlüssel für die Freigabe einer Transaktion verwalten. Die Schlüsselverwaltung wird dabei in der Regel im Hintergrund automatisch bewerkstelligt, sodass Nutzer diesen Prozess oft nicht bewusst wahrnehmen. In der Praxis kann es freilich schwarze Schafe geben, konzeptuell sollten Wallet-Anbieter jedoch keinen Zugriff auf die privaten Schlüssel ihrer Nutzer haben.

Für die Zwecke dieses Beitrags wird die Bezeichnung „virtuelle Währung“ ausschließlich für solche digitalen Güter verwendet, die auf der Blockchain-Technologie basieren. Zur Frage, ob die nachfolgend angestellten Überlegungen auf ein bestimmtes digitales Gut anwendbar sind, ist daher als Vorfrage zu klären, ob die eingesetzte Technologie mit der Blockchain zumindest vergleichbar ist. Wesentlich dafür sind drei Aspekte: erstens die Aufzeichnung aller Transaktionen in einem Verzeichnis, zweitens

2) Vorschlag einer Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien (EU) 2015/849

und 2009/101 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismus-

finanzierung vom 20.12.2016.

die Unveränderlichkeit einmal durchgeführter Transaktionen sowie drittens die Notwendigkeit der Kenntnis eines privaten Schlüssels, um Transaktionen durchzuführen.

### 3. Privatrechtliche Einordnung

In der technischen Einleitung war regelmäßig vom Kontobuch als Basis von Kryptowährungen die Rede. Dies legt eine Analogie zum Bankkonto und damit zu Buchgeld nahe. Anders als bei Buchgeld gibt es bei virtuellen Währungen jedoch keinen Dritten, dem gegenüber eine Forderung bestünde. Bei virtuellen Währungseinheiten handelt es sich nicht um Forderungsrechte. Es handelt sich lediglich um Datensätze im digitalen Kontobuch.

Der Wert virtueller Währungen ergibt sich aus der Möglichkeit, sie an andere zu übertragen, wobei nur derjenige eine Übertragung veranlassen kann, der in Kenntnis des privaten Schlüssels ist. Wer den privaten Schlüssel besitzt, kann also über die Währungseinheiten verfügen und jeden anderen davon ausschließen. Dies ist das eigentliche Recht, das den virtuellen Währungen zugrundeliegt.

#### 3.1. Sache im Sinne des § 285 ABGB

Das ABGB definiert den Begriff der Sache sehr weit und bezieht nicht nur Gegenstände in den Sachbegriff mit ein, die im allgemeinen Sprachgebrauch als Sache bezeichnet werden.<sup>3)</sup> Dies hat den Vorteil, dass sich auch neue Entwicklungen wie Software oder die Internet-Domain problemlos in das österreichische Recht als Sachen einordnen lassen.<sup>4)</sup>

Der bürgerlich-rechtliche Sachbegriff setzt sich aus zwei Elementen zusammen. Zunächst muss sich die Sache von der Person unterscheiden lassen. Zusätzlich muss die Sache dem Gebrauch des Menschen dienen, was durch das Merkmal der Beherrschbarkeit ergänzt wird.<sup>5)</sup> Dementsprechend sollen nicht beherrschbare Phänomene wie die freie Luft, das offene Meer oder das fließende Wasser keine Sachen sein.

Beide Elemente des Sachbegriffs liegen bei virtuellen Währungen vor. Sie dienen dem Gebrauch des Menschen als Tausch- oder Zahlungsmittel und lassen

sich von diesem auch beherrschen. Bei virtuellen Währungen ist die Beherrschbarkeit im Vergleich zu anderen digitalen Gütern sogar besonders stark ausgeprägt. Ohne Kenntnis des privaten Schlüssels ist eine Übertragung der Einheiten an eine andere Adresse ausgeschlossen. Man vergleiche dies mit der Beherrschbarkeit von Software oder Musikdateien, die in der Regel beliebig oft kopiert werden können und auch als Sachen angesehen werden. Virtuelle Währungseinheiten sind also jedenfalls Sachen im Sinn des § 285 ABGB.

Für eine sinnvolle rechtliche Auseinandersetzung mit virtuellen Währungen ist eine genauere Einordnung notwendig. Sachen werden in körperliche und unkörperliche eingeteilt (§ 292 ABGB), in bewegliche und unbewegliche (§§ 293 ff ABGB), verbrauchbare und unverbrauchbare (§ 301 ABGB) sowie schätzbare und unschätzbare (§§ 303 ff ABGB). Daneben wird unter anderem zwischen vertretbaren und unvertretbaren Sachen unterschieden.

#### 3.1.1. Unkörperliche Sache

Zunächst ist die Frage relevant, ob es sich bei virtuellen Währungseinheiten um körperliche oder unkörperliche Sachen handelt. An diese Unterscheidung knüpft sich als Rechtsfolge, ob die Regeln zur Übertragung von Besitz und Eigentum auf sie anwendbar sind.

Körperliche Sachen sind solche, „welche in die Sinne fallen“, also mit den menschlichen Sinnen wahrgenommen werden können. Das Abgrenzungskriterium der Sinneswahrnehmung wird von der hL<sup>6)</sup> als räumliche Abgrenzbarkeit interpretiert, weil nur dann die notwendige Beherrschbarkeit vorliegen könne. „Nur durch die räumliche Abgrenzung bzw Beherrschbarkeit wird die Sache zum tauglichen Objekt körperlicher Gewahrsame und dinglicher Herrschaftsrechte, sodass die Mehrzahl der sachenrechtlichen Bestimmungen des ABGB (insbesondere zum Besitz- und Eigentumserwerb) nur auf körperliche Sachen Anwendung finden.“<sup>7)</sup>

Wie eingangs dargestellt, sind virtuelle Währungseinheiten lediglich ein Datensatz im Kontobuch. Aus diesen Datensätzen ergibt sich, welche Adresse welchen Wert enthält. Dies spricht dafür, Kryptowährungen als unkörperliche Sachen einzuordnen<sup>8)</sup> und deckt sich auch

mit der Einordnung anderer Phänomene des Internetzeitalters wie etwa Domain-Namen.<sup>9)</sup> Virtuelle Währungseinheiten sind somit als unkörperliche Sachen zu qualifizieren.

#### 3.1.2. Bewegliche Sache

Für die Unterscheidung zwischen beweglichen und unbeweglichen Sachen kommt es nach dem Gesetz darauf an, ob eine Ortsveränderung der Sache ohne Substanzverletzung möglich ist. Die Unterscheidung ist nach einhelliger Auffassung nur für körperliche Sachen sinnvoll.<sup>10)</sup> In analoger Anwendung der Überlegungen zur Internet-Domain sind virtuelle Währungseinheiten als bewegliche Sachen anzusehen.<sup>11)</sup>

#### 3.1.3. Verbrauchbare Sache

Für die Unterscheidung zwischen verbrauchbaren und unverbrauchbaren Sachen kommt es nach dem Gesetz darauf an, ob der bestimmungsgemäße Gebrauch der Sache zu ihrer „Zerstörung und Verzehrung“ führt (§ 301 ABGB). Geld zählt zu den verbrauchbaren Sachen, weil dessen bestimmungsgemäßer Gebrauch darin besteht, es auszugeben, womit es seinem Besitzer verloren geht. Verallgemeinernd wird vertreten, dass alle Sachen verbrauchbar sind, bei denen die Veräußerung bestimmungsgemäßer Verbrauch ist.<sup>12)</sup>

Im Gegensatz zu anderen digitalen Gütern wie Musikdateien oder Software können virtuelle Währungseinheiten nicht kopiert werden. Werden sie von einer Adresse auf eine andere übertragen, kann der bisherige Inhaber nicht mehr über sie verfügen. Bei bestimmungsgemäßem Gebrauch gehen die virtuellen Währungseinheiten ihrem Besitzer verloren, es handelt sich also um verbrauchbare Sachen.

#### 3.1.4. Schätzbare Sache

Das ABGB unterscheidet weiters zwischen schätzbaren und unschätzbaren Sachen. Der Wert einer schätzbaren Sache kann durch den Vergleich mit anderen verkehrsfähigen Sachen ermittelt werden. Bei unschätzbaren Sachen kann der Wert auf diese Weise nicht ermittelt werden.<sup>13)</sup> Virtuelle Währungen werden an Handelsplätzen zu klar festgelegten Preisen gehandelt. Ihr Wert bestimmt sich durch Angebot und Nachfrage. Virtuelle Währungseinheiten zählen damit zu den

3) Vgl. *Stabentheiner* in Fenyves/Kerschner/Vonkilch, Klang<sup>3</sup> § 285 Rz 3 ff.

4) Ebd Rz 14.

5) Ebd Rz 10.

6) *Holzner* in Rummel/Lukas, ABGB<sup>4</sup> § 292 Rz 2; *Klicka* in Schwimann<sup>4</sup> § 292 Rz 1; *Eccher* in KBB<sup>4</sup> § 292 Rz 1.

7) *Kisslinger* in Fenyves/Kerschner/Von-

kilch, Klang<sup>3</sup> § 292 Rz 1.

8) Vgl. mit anderer Begründung *Aquilina/Stadler* in Eberwein/Steiner, Bitcoins 98 f.

9) *Kisslinger* in Fenyves/Kerschner/Vonkilch, Klang<sup>3</sup> § 292 Rz 25.

10) *Holzner* in Rummel/Lukas, ABGB<sup>4</sup> § 294 Rz 3 ff mwN.

11) *Klicka* in Schwimann<sup>4</sup> § 292 Rz 5 und

§ 285 Rz 10; *Kisslinger* in Fenyves/Kerschner/Vonkilch, Klang<sup>3</sup> § 292 Rz 25 mwN.

12) Vgl. *Kisslinger* in Fenyves/Kerschner/Vonkilch, Klang<sup>3</sup> § 301 Rz 3 ff mwN.

13) Vgl. *Kisslinger* in Fenyves/Kerschner/Vonkilch, Klang<sup>3</sup> § 303 Rz 1 ff.

schätzbaren Sachen im Sinn des § 303 ABGB.

### 3.1.5. Vertretbare Sache

Die Unterscheidung in vertretbare und unvertretbare Sachen findet sich nicht ausdrücklich im Gesetz. Vertretbare oder fungible Sachen können im Verkehr durch andere gleichartige ersetzt werden; es kommt nicht auf die Besonderheit des einzelnen Stücks an. Vertretbare Sachen werden im Verkehr nur nach Zahl, Maß oder Gewicht bezeichnet.<sup>14)</sup>

Wie oben dargestellt, handelt es sich bei den Einheiten virtueller Währungen lediglich um einen Datensatz auf der Blockchain. Die Einheiten unterscheiden sich nicht voneinander. Es kommt auch nicht auf die Besonderheiten des einzelnen Stücks an. Virtuelle Währungseinheiten sind also vertretbare Sachen.

## 3.2. Derivativer Erwerb

### 3.2.1. Digitale Wallet

Derivativer Erwerb von Eigentum oder Rechtszuständigkeit erfolgt durch Titel und Modus, Verpflichtungs- und Verfügungsgeschäft. Virtuelle Währungseinheiten können grundsätzlich Gegenstand aller Verpflichtungsgeschäfte sein, die auch bei anderen unkörperlichen beweglichen verbrauchbaren schätzbaren und vertretbaren Sachen infrage kommen. Kauf, Tausch, Schenkung, Darlehen und Pfandbestellungsvertrag können also ebenso virtuelle Währungseinheiten betreffen. Freilich sind bestimmte Besonderheiten zu beachten, deren Behandlung jedoch anderen Beiträgen vorbehalten bleiben muss.

Ausgangspunkt für die Frage nach dem korrekten Modus für die Übertragung virtueller Währungseinheiten ist zunächst die oben getroffene Qualifizierung als unkörperliche Sachen. Eine Übertragung nach sachenrechtlichen Grundsätzen würde damit grundsätzlich ausscheiden. Die Übertragung müsste nach schuldrechtlichen Grundsätzen durch Abtretung erfolgen (§§ 1393 ff ABGB).

Es gilt allerdings eine Besonderheit von virtuellen Währungen zu berücksichtigen. Für die technische Übertragung der Einheiten von einer Absender-Adresse auf eine Empfänger-Adresse ist ein Vermerk in der Blockchain erforderlich. Durch die Übertragung von einer Adresse auf eine andere Adresse wird technisch sichergestellt, dass nur derjenige in Kenntnis eines privaten Schlüssels zur Weiterübertragung ist, dem die virtuellen Einhei-

ten auch tatsächlich zugeordnet werden sollen.

Fraglich ist, ob diese technische Voraussetzung auch rechtliche Bedeutung erlangen kann. Zur Veranschaulichung soll nachfolgender Fall dienen: A verkauft an B fünf Bitcoin, die unter einer bestimmten Adresse abgelegt sind. Er nennt B die Adresse samt privatem Schlüssel, um über die Bitcoin verfügen zu können. Zu einem Vermerk der Übertragung auf der Blockchain ist es in diesem Fall nicht gekommen. Ist die Nennung des privaten Schlüssels ausreichend, um Rechtszuständigkeit an den fünf Bitcoin von A an B zu übertragen? Eine praktisch akzeptable Lösung lässt sich nach Ansicht des Autors nur mit einer Analogie zu sachenrechtlichen Grundsätzen finden.

Derivativer Rechtserwerb an einer körperlichen Sache setzt regelmäßig deren Übergabe voraus (§ 425 ABGB), bei Liegenschaften die Verbücherung (§ 431 ABGB). Eigentum geht erst durch tatsächliche Verwirklichung der angestrebten Sachherrschaft auf den Erwerber über, die zugleich das den Parteien nach ihrer jeweiligen Absicht zumutbare Maß an Publizität des Rechtsübergangs bewirkt.<sup>15)</sup>

Solange der Übergeber einer virtuellen Währungseinheit weiterhin darüber verfügen könnte, besteht noch keine ausreichende Verfügungsgewalt des Empfängers, um von einer Übergabe im sachenrechtlichen Sinn zu sprechen. Durch die Übertragung an eine neue Adresse kann diese Verfügungsgewalt jedoch eingeräumt werden, wenn der dazugehörige private Schlüssel ausschließlich dem Empfänger bekannt ist. Es ist den Vertragsparteien auch durchaus zumutbar, den technisch vorgesehenen Weg zu beschreiten und die Übertragung der Werteinheiten an eine neue Adresse vorzunehmen. Der Modus für die Verschaffung von Rechtszuständigkeit an virtuellen Währungseinheiten ist damit ihre Übertragung an eine neue Adresse, deren privater Schlüssel sich in der Verfügungsgewalt des Empfängers befindet.

### 3.2.2. Ausnahme: Physische Wallet

In diesem Zusammenhang ist auf einen weiteren Umstand einzugehen. Wie oben dargestellt, kann der private Schlüssel auch physisch abgelegt werden. Virtuelle Währungseinheiten können somit durch körperliche Sachen repräsentiert werden. Die virtuelle Währung Bitcoin kann mittlerweile etwa in Form von Rubbellosen oder geprägten Münzen ge-

kauft und gehandelt werden. Auf solchen „physischen Wallets“ ist die jeweilige Adresse sichtbar. Dadurch kann auf der Blockchain leicht überprüft werden, ob der versprochene Wert tatsächlich besteht. Der private Schlüssel ist hingegen in der Regel nur durch Zerstörung der physischen Wallet zugänglich, etwa durch Aufrubbeln der Lose oder Zerbrecen der Münzen. Beide Informationen sind notwendig, um den Wert an eine andere Adresse zu übertragen.

Die Übertragung von Besitz und Eigentum an der physischen Wallets folgt selbstverständlich allgemeinen sachenrechtlichen Grundsätzen. Dieser Vorgang darf jedoch nicht mit der Übertragung der virtuellen Währungseinheit selbst vermengt werden. Freilich wäre in diesem Fall eine Analogie zu dem auf Wertpapiere anwendbaren Recht sinnvoll. Soweit Rechte aus Wertpapieren an den Besitz einer Urkunde gebunden sind (Inhaber- und Orderpapiere), werden sie als körperliche Sachen angesehen.<sup>16)</sup>

Bei der Übergabe einer physischen Wallet wird die Adresse der virtuellen Währungseinheiten samt privatem Schlüssel übergeben. Ohne diese beiden Informationen kann über die Einheiten nicht verfügt werden. Es ließe sich argumentieren, dass das Recht aus der physischen Wallet – die Verfügung über die virtuellen Währungseinheiten – an den Besitz der physischen Wallet gebunden ist. In dieser Konstellation könnten virtuelle Währungseinheiten als körperliche Sachen betrachtet werden. Die Übertragung würde entsprechend den sachenrechtlichen Grundsätzen wie bei Inhaberwertpapieren erfolgen.

## 3.3. Anwendung von §§ 371, 415 ABGB?

§ 371 ABGB ordnet den originären Eigentumserwerb vertretbarer Sachen vom Nichteigentümer an, wenn sie mit eigenen vermengt werden. Vermengung liegt dann vor, wenn die zusammengebrachten Sachen nicht oder nur mit unvertretbarem Aufwand nach Eigentümern getrennt werden können.<sup>17)</sup> Ein hauptsächlich Anwendungsfall der Bestimmung ist Geld. § 415 ABGB ordnet an, dass durch die Vermengung verschiedener ununterscheidbarer Güter Miteigentum am Gemenge entsteht. Auf das Spannungsverhältnis der beiden Bestimmungen wird an dieser Stelle lediglich hingewiesen.<sup>18)</sup>

Da es sich bei virtuellen Währungen um vertretbare Sachen handelt, stellt sich die Frage nach einer analogen Anwen-

14) Ebd Rz 7 ff.

15) Holzner in Rummel/Lukas, ABGB<sup>4</sup> § 425 Rz 1 ff.

16) Klicka in Schwimann<sup>4</sup> § 292 Rz 4; Kisslinger in Fenyves/Kerschner/Vonkilch, Klang<sup>3</sup> § 292 Rz 7.

17) Winner in Rummel/Lukas, ABGB<sup>4</sup> § 371 Rz 4 ff.

18) Ebd Rz 6-10 mwN.

dung dieser Vorschriften. § 371 ABGB wird von der Rechtsprechung bereits analog auf Buchgeld angewendet.<sup>19)</sup> Dies wird in der L kritisiert, handelt es sich doch bei Buchgeld um Forderungen gegenüber der Bank.<sup>20)</sup> Bei Einheiten virtueller Währungen ist dies freilich nicht der Fall. Sie verkörpern gerade kein Forderungsrecht gegenüber einem Dritten.

Wegen der grundsätzlich gleichen Ausgangslage wie bei Geld ist eine analoge Anwendung auf virtuelle Währungen angebracht. Wie bei Buchgeld können Bitcoin eine hohe Verkehrsfähigkeit erlangen. Eine gesetzliche Regelung für den Fall ihrer Ununterscheidbarkeit auf einer Adresse scheint damit geboten.

Im Zusammenhang mit dem Spannungsverhältnis von §§ 371, 415 ABGB wird an dieser Stelle auf die eingangs gemachten technischen Ausführungen verwiesen. Wie bei Bankkonten können Transaktionen grundsätzlich gut einem Absender zugeordnet werden. Insofern könnte auch auf die zum Buchgeld herausgearbeiteten Grundsätze zur Abgrenzung zwischen § 371 und § 415 ABGB zurückgegriffen werden.

### 3.4. Begründung des Pfandrechts

Für den Erwerb des Pfandrechts ist der Abschluss eines Verpflichtungsgeschäfts notwendig sowie das Setzen eines Publizitätsakts als Modus. Als Verpflichtungsgeschäft kommt der Pfandbestellungsvertrag in Betracht. Hinsichtlich des korrekten Modus ist § 451 ABGB einschlägig. Bei beweglichen Sachen wie den Einheiten virtueller Währungen gilt das Faustpfandprinzip.

Der Pfandgläubiger muss die verpfändete bewegliche Sache daher in Verwahrung nehmen, und zwar so, dass er beliebig und ausschließlich darüber verfügen kann. Die Rechtsprechung verlangt, die verpfändete Sache der Zugriffsmacht des Pfandbestellers zu entziehen wenn irgend möglich.<sup>21)</sup> In technischer Hinsicht besteht durchaus die Möglichkeit, dem Pfandbesteller den Zugriff auf die Werteinheiten zu entziehen und ausschließlich

dem Pfandnehmer einzuräumen. Dazu ist erforderlich, die Währungseinheiten auf eine neue Adresse zu übertragen, deren privater Schlüssel ausschließlich dem Pfandnehmer bekannt ist. Die Übertragung auf eine andere Adresse ist also notwendiger und hinreichender Publizitätsakt für die Begründung des Pfandrechts an den Einheiten virtueller Währungen.

In der Praxis ist das Faustpfandprinzip unbeliebt, wenn Güter verpfändet werden, die eine hohe Umschlagshäufigkeit aufweisen. Gerade auf virtuelle Währungen trifft dies wegen der ihnen immanenten Zahlungsfunktion zu. Das Faustpfandprinzip bedeutet daher eine drastische Einschränkung. Dies kann aber nicht als Argument für eine Lockerung dienen. Stattdessen appelliert der Autor an die Bankenpraxis, technische Lösungen zu finden. Der Umgang mit virtuellen Währungen findet ohnedies automationsunterstützt statt. Die Entwicklung einer bankeigenen Wallet ist naheliegend. Dies würde es Banken erlauben, die privaten Schlüssel ihrer Kunden zu verwahren und selbst darüber zu verfügen. Transaktionen könnten entsprechend einer getroffenen Vereinbarung (etwa auch in Form selbstausführender *smart contracts*) freigegeben oder blockiert werden. Vom Prinzip her würde es sich bei diesen Wallets um ein Bankkonto für virtuelle Währungen handeln, über das genauso vertraglich verfügt werden kann, wie über jedes andere Bankkonto auch.

### 3.5. Sicherungsübereignung

Die Besicherung eines Gläubigers kann auch dadurch erreicht werden, ihm an einer Sache Eigentum zu übertragen (Sicherungsübereignung) bzw die Rechtszuständigkeit durch Abtretung zu verschaffen (Sicherungsabtretung). In der Sicherungsabrede vereinbaren der Sicherheitenbesteller und der Sicherheitennehmer, dass dieser die Sache bis zur vollständigen Bezahlung der Schuld behalten soll. Leistet der Schuldner nicht, kann sich der Gläubiger aus der übereigneten Sache befriedigen.

Es ist kein Grund ersichtlich, weshalb die Sicherungsabtretung nicht auch im Fall von virtuellen Währungen möglich sein sollte. Als Modus kommt wie oben unter Punkt 3.2 herausgearbeitet nur die Übertragung der Einheiten auf eine neue Adresse in Betracht, deren privater Schlüssel sich in der ausschließlichen Verfügungsgewalt des Sicherheitennehmers befindet.

## 4. Zusammenfassung der Ergebnisse

Im Ergebnis kann festgehalten werden, dass virtuelle Währungseinheiten zwanglos unter den bürgerlich-rechtlichen Sachbegriff zu subsumieren sind. Genauer handelt es sich um unkörperliche, bewegliche, verbrauchbare und vertretbare Sachen. Gegenstand des Rechts an virtuellen Währungseinheiten ist die ausschließliche Möglichkeit, über sie zu verfügen, und zwar durch Übertragung von einer Adresse an eine andere Adresse. Virtuelle Währungen können damit Gegenstand rechtsgeschäftlicher Vereinbarungen sein wie etwa Kauf-, Tausch-, Schenkungs- oder Darlehensvertrag.

Die Beherrschbarkeit im sachenrechtlichen Sinn ist bei virtuellen Währungen im Vergleich zu anderen unkörperlichen Sachen wegen der notwendigen Kenntnis eines privaten Schlüssels besonders stark ausgeprägt. Modus für die Verschaffung von Rechtszuständigkeit ist die Übertragung der virtuellen Währungseinheiten auf eine neue Adresse, deren privater Schlüssel sich in der ausschließlichen Verfügungsgewalt des gewollten Empfängers befindet.

Die Bestimmungen über den originären Erwerb nach § 371 ABGB (Vermengung wie bei Geld) sind auch auf die Einheiten virtueller Währungen anwendbar. Sie können wie andere Sachen auch Gegenstand der Verpfändung und der Sicherungsabtretung sein. Als Modus für die Pfandbestellung und die Sicherungsabtretung kommt ebenfalls wie beim derivativen Erwerb nur die Übertragung der virtuellen Währungseinheiten auf eine neue Adresse in Betracht, deren privater Schlüssel sich in der ausschließlichen Verfügungsgewalt des Sicherheitennehmers befindet.

## Literaturverzeichnis

Eberwein / Steiner (Hrsg), Bitcoins (2014).

Kozioł / Bydlinski / Bollenberger (Hrsg), Kurzkomentar zum ABGB<sup>4</sup> (2014).

Rummel / Lukas (Hrsg), Kommentar zum Allgemeinen bürgerlichen Gesetzbuch<sup>4</sup> (2015).

Fenyves / Kerschner / Vonkilch (Hrsg), Großkommentar zum ABGB – Klang Kommentar<sup>3</sup> (2016).

Schwimann (Hrsg), ABGB Praxiskommentar<sup>4</sup> (2011).

19) Vgl OGH 31.8.1994 8 Ob 4/94; Winner in Rummel/Lukas, ABGB<sup>4</sup> § 371 Rz 10 mwN.

20) Leupold in Klang<sup>3</sup> § 371 Rz 29 mwN.

21) OGH 29.6.1983 3 Ob 135/82.