



Nicolas Jacquemart / Stephan D. Meyer*

Der Bitcoin-/Bitcoin-Cash-Hardfork

Die auftragsrechtliche Ablieferungspflicht bei Kryptowährungs-Dienstleistungen im Lichte der bundesgerichtlichen Rechtsprechung



Inhaltsübersicht

- I. Einleitung
- II. Bitcoin, Blockchain-Forks und die Geburtsstunde von Bitcoin Cash
 1. Bitcoin
 - 1.1 Ausgewählte Grundlagen von Bitcoin
 - 1.2 Die Bedeutung der Private Keys
 2. Typologie der Blockchain-Gabelungen
 - 2.1 Vorübergehende, unbeabsichtigte Blockchain-Gabelung im Normalbetrieb
 - 2.2 Beabsichtigte Protokoll-Gabelung zur Schaffung eines neuen Blockchainsystems
 - 2.3 Beabsichtigte Gabelung eines bestehenden Blockchainsystems
 3. Die Geburtsstunde von Bitcoin Cash
- III. Die auftragsrechtliche Ablieferungspflicht
 1. Das Auftragsverhältnis im Allgemeinen
 2. Die Rechenschaftspflicht nach Art. 400 OR
 3. Die Ablieferungspflicht im Besonderen
 - 3.1 Gegenstand der Ablieferungspflicht
 - 3.2 Begrenzung der Ablieferungspflicht durch «inneren Zusammenhang»
 - 3.3 Dispositive Natur der Ablieferungspflicht
- IV. Fallgruppen
 1. Fremdverwaltung der Bitcoin Private Keys
 2. Auftrag zur Beschaffung von Bitcoin
 3. Kontoführung lautend auf Bitcoin
- V. Auftragsrechtliche Ablieferungspflicht beim Bitcoin-Hardfork
 1. Unterschied zur Retrozessionsthematik
 2. Bitcoin Cash als Vermögenswert
 3. Blockchain-Gabelung als indirekter Vorteil
 4. Innerer Zusammenhang
 - 4.1 Abgrenzung gemäss Lehre und Rechtsprechung
 - 4.2 Natürliche und adäquate Kausalität zwischen Auftragsausführung und Vermögenswert
 - 4.3 Zweck des Vertrages bei Fremdverwaltung von Bitcoin Private Keys
 - 4.4 Zweck des Vertrages bei Auftrag zur Beschaffung von Bitcoin
 - 4.5 Zweck des Vertrages bei Kontoführung lautend auf Bitcoin

VI. Ergebnis

1. Kryptowährungen als technische Herausforderung des Rechts
2. Grenzen der bundesgerichtlichen Rechtsprechung zur Ablieferungspflicht
3. Schluss

I. Einleitung

In den letzten Jahren ist Bitcoin (nachfolgend BTC) zur bekanntesten virtuellen Währung aufgestiegen. BTC basiert auf einer sogenannten *Blockchain*. Sowohl in Alltagsmedien¹, in denen sich die Berichterstattung zwischen kritischen und euphorischen Meinungen bewegt, als auch in der juristischen Fachliteratur² hat die Entstehung und Verbreitung von BTC und der zugrundeliegenden Blockchain-Technologie erhebliche Beachtung gefunden. Die Marktkapitalisierung von BTC stieg seit Anfang des Jahres 2017 um über 1000 % und beläuft sich zurzeit auf rund 190 Milliarden Schweizer Franken. Ein einzelner BTC hat damit einen Marktwert von über elftausend Schweizer Franken. Unter anderem aufgrund der stetig zunehmenden Nachfrage nach BTC

¹ Illustriert am Beispiel der tendenziell kritisch gestimmten Neuen Zürcher Zeitung: CHRISTOF LEISINGER, Kryptowährungen: Bitcoin-Märchen ohne Happy End?, NZZ vom 29.1.2016; LUZIUS MEISSER, Blockchain: Eine Chance für den Finanzplatz, NZZ vom 27.9.2016; WERNER GRUNDEHNER, Kryptowährungen: Ein gutes Jahr für Bitcoin-Besitzer, NZZ vom 23.12.2016; MATTHIAS SANDER, Digitale Währung: Bitcoin droht eine Spaltung, NZZ vom 27.7.2017.

² Vgl. mit weiteren Hinweisen: HARALD BÄRTSCHI/CHRISTIAN MEISSER, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: WEBER/THOUVENIN (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 111 ff.; SABINE GLESS/PETER KUGLER/DARIO STAGNO, Was ist Geld? Und warum schützt man es?, recht 2015, 82 ff.; LUZIUS MEISSER, Kryptowährungen: Geschichte, Funktionweise, Potential, in: WEBER/THOUVENIN (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 73 ff.; DANIEL STOLL, Le bitcoin et les aspects pénaux des monnaies virtuelles, forumpoenale 2015, 99 ff.; MIRJAM EGGEN, Chain of Contracts, AJP 2017, 3 ff.; STEPHAN D. MEYER/BENEDIKT SCHUPPLI, «Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht, recht 2017, 204 ff.; THOMAS LINDER/STEPHAN D. MEYER, Die steuerliche Behandlung von Bitcoin und anderen Kryptowährungen, ZStP 2017, 191 ff.; ALEXANDER F. WAGNER/ROLF H. WEBER, Corporate Governance auf der Blockchain, SZW 2017, 59 ff.

* NICOLAS JACQUEMART, M.A. HSG in Law, Rechtsanwalt und STEPHAN D. MEYER, MLaw, LL.M.; beide Doktoranden an der Universität Zürich und Mitarbeiter des interdisziplinären Projekts des Schweizerischen Nationalfonds (Nr. 10001A_162442) über virtuelle Währungen an der ZHAW School of Management and Law. Die Autoren bedanken sich bei Prof. Dr. HARALD BÄRTSCHI und Dr. CHRISTIAN DECKER für die wertvollen rechtlichen bzw. technischen Hinweise.

und der damit verbundenen Anzahl an Transaktionen stiess die zugrunde liegende technische Infrastruktur an ihre Grenzen. Die Folge waren längere Wartezeiten, bis Transaktionen erfolgreich auf der BTC-Blockchain validiert wurden.³ Aus diesem Grund diskutierte die BTC-Nutzergemeinschaft bereits seit längerem über mögliche Änderungen des Blockchain-Protokolls zur Erhöhung der Transaktionsgeschwindigkeit, wobei es betreffend das konkrete Vorgehen unterschiedliche Ansichten gab.

Eine Folge dieser Uneinigkeit innerhalb der BTC-Gemeinschaft war der am 1. August 2017 durchgeführte sog. *Hardfork* der BTC-Blockchain in zwei separate Blockchains für BTC einerseits und für die neu erschaffene Konkurrenzwährung Bitcoin Cash (nachfolgend BCC) andererseits. Diese beiden Kryptowährungen teilen sich eine gemeinsame Transaktionshistorie, sind jedoch ansonsten nicht kompatibel (siehe unten II.2.3). Die auf der BTC-Blockchain zum Zeitpunkt der harten Gabelung existierenden Währungseinheiten erschienen auch auf der BCC-Blockchain. Bei der Gabelung entstand für jeden BTC ein BCC. Diejenigen BTC-Nutzer, die direkten Zugriff auf ihre BTC hatten, verfügten im gleichen Umfang ebenfalls über die neu angefallenen BCC.

Eine zunehmende Anzahl Anleger nimmt zur Verwaltung oder zum Kauf und Handel ihrer BTC die Dienstleistungen von Kryptowährungsbörsen oder anderen Dienstleistern in Anspruch. Da entsprechende Dienstleistungsverträge nach schweizerischem Recht regelmässig auftragsrechtlichen Charakter haben, wollen wir in diesem Aufsatz der Frage nachgehen, ob den Dienstleistern aus der Ablieferungspflicht von Art. 400 OR eine Pflicht erwächst, die neu anfallenden BCC ihren jeweiligen Auftraggebern abzuliefern. Aufgrund der zunehmenden Anzahl an Unternehmen, die Dienstleistungen in Kryptowährungen anbieten, ist diese Frage von praktischer Bedeutung.

Der vorliegende Beitrag beschreibt nach einer kurzen Darstellung der Grundlagen der BTC-Blockchain-Technologie (II.1) zunächst die verschiedenen Arten von *Forks* (zu Deutsch: Gabelungen), welche auf einer solchen Blockchain vorkommen (II.2) und erläutert die Entstehung von BCC (II.3). Danach wird die Rechtsprechung des Bundesgerichts im Zusammenhang mit der Ablieferungspflicht im Auftragsrecht untersucht (III.1 bis III.3), und es werden typisierte Fallgruppen aus dem Dienstleistungssegment für Kryptowährungen gebildet (IV.1 bis IV.3). Dann wenden wir die bundesgerichtliche Rechtsprechung auf die Fallgruppen an (V.1 bis V.4.5).

³ Will ein Nutzer eine bestimmte Transaktion zeitnah ausgeführt wissen, so muss er entsprechend höhere Transaktionsgebühren bezahlen. Dies hatte zur Folge, dass BTC für kleinere Transaktionen unattraktiv wurde.

Nicht thematisiert werden im Nachfolgenden weitere bzw. anders geartete rechtliche Pflichten des Beauftragten, welche sich aus im Einzelfall anwendbaren Finanzmarktgesetzen (z.B. das BEHG, sowie zukünftig das FIDLEG) oder weiteren aufsichtsrechtlichen Bestimmungen ergeben können, sowie Pflichten im Zusammenhang mit Derivaten, die sich auf eine Kryptowährung wie BTC als Referenzwert beziehen.⁴

II. Bitcoin, Blockchain-Forks und die Geburtsstunde von Bitcoin Cash

1. Bitcoin

1.1 Ausgewählte Grundlagen von Bitcoin

Es existiert bereits in beträchtlichem Umfang Literatur zur Funktionsweise von auf der Blockchain-Technologie basierenden virtuellen Währungen. Dieser Aufsatz verzichtet folglich auf die erneute Erläuterung von deren grundlegender technischer Funktionsweise und beschränkt sich auf eine Beschreibung des Phänomens sogenannter *Forks*, wie sie bei Blockchainsystemen wie BTC vorkommen. Das Folgende gilt *mutatis mutandis* auch für die BCC-Blockchain.

Bei der BTC-Blockchain handelt es sich im Kern um ein für jede Person mit Zugriff auf das Internet zugängliches, offenes, pseudonymes und intermediärloses Transaktionssystem⁵ auf der Grundlage einer transparenten, dezentralen Transaktionsdatenbank, die kryptographisch gesichert ist und in einem Peer-to-Peer-Netzwerk verbreitet wird.⁶ Die für diese Transaktionsdatenbank verwendete Datenstruktur nennt sich *Blockchain*, weil es sich um eine Kette von programmtechnisch verbundenen Datenblöcken handelt, die sämtliche vergangenen Transaktionen enthalten.⁷ Die Transaktionen finden in der virtuellen Währung namens BTC statt, wobei ein BTC aktuell auf bis zu acht Stellen nach dem Komma unterteilbar ist.⁸

BTC stellen keine Forderungen gegenüber einem Dienstleister dar und es gibt keinen identifizierbaren zentralen Emittenten der Kryptowährung.⁹ Der Wert von BTC und anderen virtuellen Währungen ergibt sich aus-

⁴ Vgl. dazu, wenn auch ohne Bezug zu virtuellen Währungen: ANETTE THERESE WAYGOOD-WEINER, Rückvergütungen und Interessenkonflikte in der Finanzbranche, Diss. St. Gallen 2013, 152 ff. (= SSHW 321).

⁵ Das Vorliegen eines *Zahlungssystems* im Sinne von Art. 81 FinfraG ist u.E. mangels vertraglicher Grundlage und fehlender Zahlungsverpflichtungen zu verneinen; a.M. BÄRTSCH/MEISSER (FN 2), 119.

⁶ Vgl. GLESS/KUGLER/STAGNO (FN 2), 86 ff.; ANDREAS M. ANTONOPOULOS, *Mastering Bitcoin, Unlocking digital cryptocurrencies*, 1. Aufl., Sebastopol 2015, 15 ff.; MEISSER (FN 2), 79 ff.

⁷ MEISSER (FN 2), 83.

⁸ GLESS/KUGLER/STAGNO (FN 2), 87.

⁹ Vgl. MEISSER (FN 2), 78.

schliesslich aus der Bereitschaft anderer Marktteilnehmer, für BTC Dienstleistungen, Güter oder andere Fiat- oder virtuelle Währungen zu tauschen.¹⁰ Die Ausgabe und Verwaltung der BTC erfolgt durch ein verbundenes Netzwerk aller Computer (einzeln auch *Node* genannt), die das BTC-Protokoll betreiben.¹¹ Über den jeweils gültigen Zustand der Transaktionsdatenbank einigt sich das BTC-Netzwerk mittels eines ausgeklügelten Konsensmechanismus und unter Aufwendung erheblicher Rechenleistung.¹² Für weiterführende Erläuterungen wird auf die zitierte Literatur verwiesen.

1.2 Die Bedeutung der Private Keys

Der Zugriff auf und die Verfügungsmacht über Kryptowährungen wie BTC erfolgt ausschliesslich mittels eines kryptographischen Schlüsselpaars; eines öffentlichen Schlüssels (*Public Key*, PUK) und eines privaten Schlüssels (*Private Key*, PIK). Dieses Schlüsselpaar wird von den Nutzern üblicherweise auf einem *Wallet* (zu Deutsch: Brieftasche) abgespeichert. Hierbei handelt es sich um eine Software, welche den Zugriff auf die eigenen BTC erleichtert, indem es die verwendeten Schlüssel verwaltet und zudem den aktuellen Stand der kontrollierten Währungseinheiten angibt. Bei mit dem Internet verknüpften Wallets spricht man auch von *Hot Wallets*. Demgegenüber ist es aber auch möglich, die eigenen kryptographischen Schlüssel *offline*, beispielsweise auf Papier niedergeschrieben, aufzubewahren. Bei dieser Methode spricht man von *Paper Wallets* (oder auch *Cold Storage*).

Will man eine Transaktion in BTC durchführen, so verwendet man seinen eigenen privaten Schlüssel sowie eine aus dem öffentlichen Schlüssel des Empfängers abgeleitete Zieladresse und signiert damit den BTC derart, dass wiederum nur der Empfänger mit seinem privaten Schlüssel die nächste Transaktion gültig signieren kann.¹³ Bei einer BTC-Transaktion findet daher keine bilaterale Übergabe von Daten oder digitalen «Münzen» statt, sondern es wird lediglich eine neuen Signatur an eine bestehende Kette aus digitalen Signaturen auf der Blockchain angehängt. Zur Erhöhung der Sicherheit kann man zudem den Zugriff auf BTC so ausgestalten, dass mehrere voneinander abhängige Schlüssel zur gültigen Signatur einer Transaktion erforderlich sind. Man spricht dann von *MultiSig-Adressen*. So ist es möglich, dass beispielsweise zwei von drei Schlüsseln oder fünf von sieben Schlüsseln benötigt werden.

Für die weiteren Ausführungen ist zwischen Situationen zu unterscheiden, bei denen ein Nutzer selbst Zugriff auf den mit den BTC verbundenen privaten Schlüssel hat und solchen, bei denen die Mitwirkung eines Dienstleisters erforderlich ist. Bei den letzteren Fällen hat ein Nutzer regelmässig nur Zugriff auf ein digitales Konto, welches von dem Dienstleister verwaltet wird. Entweder es besteht dann ein schuldrechtlicher Anspruch des Nutzers auf Auslieferung seines privaten Schlüssels, der den direkten Zugriff auf die geschuldete Anzahl BTC erlaubt, oder aber der Nutzer hat einen schuldrechtlichen Anspruch auf Überweisung einer entsprechenden Anzahl BTC an eine nur von ihm kontrollierte Adresse.

2. Typologie der Blockchain-Gabelungen

Die wissenschaftliche Beschreibung von Blockchain *Forks*, einem technisch komplexen Teilthema des Blockchain-Universums, ist eine noch junge Disziplin. Die entsprechende Nomenklatur steht folglich erst am Anfang und ist grösstenteils uneinheitlich.¹⁴ Im Folgenden unternehmen wir zum besseren Verständnis des Phänomens den Versuch einer Typisierung von Blockchain-Gabelungen. Wir unterscheiden für diesen Aufsatz drei Formen von Blockchain-Gabelungen in offenen Blockchainsystemen: (1) vorübergehende, unbeabsichtigte Blockchain-Gabelung im Normalbetrieb, (2) beabsichtigte Protokoll-Gabelung zur Schaffung eines neuen Blockchainsystems und (3) beabsichtigte Gabelung eines bestehenden Blockchainsystems.

Die nachfolgende Kategorisierung ist zwangsläufig technisch vereinfacht und folglich auch unvollständig. Zudem stellen wir nicht nur auf technisch-objektive Kriterien, sondern auch auf subjektive Kriterien wie die hinter einer Blockchain-Gabelung stehende Absicht der Nutzergemeinschaft ab. Ziel der folgenden Ausführungen ist es denn auch nicht, das Thema der Blockchain-Gabelungen vollständig aufzuarbeiten, sondern ein Grundverständnis dafür zu schaffen, welche rechtlichen Folgen mit solchen Gabelungen einhergehen können.

2.1 Vorübergehende, unbeabsichtigte Blockchain-Gabelung im Normalbetrieb

Von einer Gabelung einer Blockchain spricht man u.a. dann, wenn zwei oder mehr parallele Stränge derselben Blockchain, d.h. derselben Transaktionsdatenbank, im Netzwerk der verbundenen Computer generiert werden, die nach dem zugrundeliegenden Blockchain-Protokoll

¹⁰ Vgl. FinfraG Kommentar-Hess/Kalbermatter/Weiss-Voigt, Art. 81, Rz. 86.

¹¹ Eine eindrückliche geographische Übersicht über alle zu einem gegebenen Zeitpunkt mit dem Netzwerk verbundenen Computer findet sich unter <https://bitnodes.21.co/> (Abruf 27.10.2017).

¹² Meisser (FN 2), 82 ff.

¹³ Antonopoulos (FN 6), 61 ff. und 111 ff.; Meyer/Schuppli (FN 2), 205.

¹⁴ Vgl. Mohit Mamoria, Your ultimate guide to the upcoming fork that's splitting the Bitcoin community, https://thenextweb.com/contributors/2017/07/24/ultimate-guide-upcoming-fork-thats-splitting-bitcoin-community/#.tnw_dG2xE9HC (Abruf 27.10.2017); Dean S. Walsh, What is a Fork?, <http://cryptorials.io/glossary/fork/> (Abruf 27.10.2017).

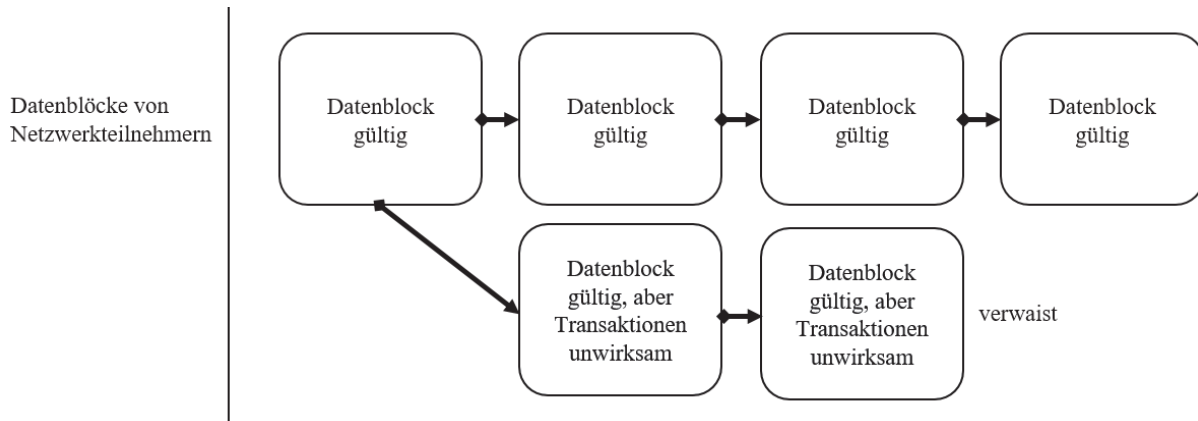


Abbildung 1: Vorübergehende, unbeabsichtigte Blockchain-Gabelung im Normalbetrieb.

jeweils als gültige und damit grundsätzlich fortsetzungsfähige Version der Blockchain in Frage kommen.

Solche Gabelungen sind bei der BTC-Blockchain kein seltenes Ereignis und können bereits dann entstehen, wenn nicht alle Netzwerkteilnehmer des weltweiten Netzwerkes miteinander verbunden sind oder wenn zwei Netzwerkteilnehmer zeitgleich einen neuen gültigen Block anfügen, in dem aber jeweils unterschiedliche Transaktionen enthalten sind.¹⁵ Sie sind gewissermaßen eine natürliche Folge der verwendeten Mechanismen offener Blockchainsysteme.¹⁶

Wie jedes andere Blockchain-Netzwerk enthält auch das BTC-Protokoll bestimmte Regeln, wie mit Gabelungen im Normalbetrieb umgegangen wird, um möglichst schnell wieder alle Netzwerkteilnehmer auf einen einheitlichen Stand zu bringen. So werden zunächst alle ungültigen Blöcke, z.B. infolge eines Übertragungsfehlers im Netzwerk, vom empfangenden Netzwerkteilnehmer verworfen. Bestehen dann immer noch mehrere Versionen der Blockchain, wird die längste Kette von Datenblöcken fortgesetzt. Gibt es mehrere gleich lange Versionen, so setzt sich diejenige durch, die vom Netzwerkteilnehmer als erste wahrgenommen worden ist.¹⁷ Die dabei vom Netzwerk verworfene Version der Blockchain wird im Folgenden von den Netzwerkteilnehmern ignoriert. Die Transaktionen, die darin enthalten waren und nun erneut der Verarbeitung harren, gelangen zurück in den Transaktionspool und werden in der Folge in neuen Datenblöcken verarbeitet. Für die Nutzer, deren Transaktionen auf der verworfenen Version der Blockchain enthalten waren, ergibt sich folglich im Normalfall bloss eine Verarbeitungsverzögerung. Dieser Vorgang

wird zuweilen auch als Blockchain-Reorganisation bezeichnet und lässt sich grafisch wie in Abbildung 1 darstellen.

Gabelungen der Blockchain können jedoch auch die Folge von Programmfehlern im Blockchain-Protokoll sein. Die Folgen solcher Gabelungen können schwerwiegend sein. Bei der BTC-Blockchain trat ein solcher Fall z.B. im Jahr 2013 auf, als eine Inkompatibilität zwischen einer neu veröffentlichten und einer alten Version des BTC-Protokolls zu einer rund sechsständigen unbeabsichtigten Gabelung der BTC-Blockchain führte.¹⁸ Deren Beseitigung erforderte damals eine koordinierte Aktion innerhalb der BTC-Nutzergemeinschaft, durch welche wieder auf die ältere Version des BTC-Protokolls gewechselt wurde. Der wirtschaftliche Schaden betrug, beim damaligen BTC-Preis von rund USD 45, in etwa USD 35'000.¹⁹ Heute wäre der Schaden eines vergleichbaren Vorfalls aufgrund der aktuellen BTC-Preise ungleich höher.

2.2 Beabsichtigte Protokoll-Gabelung zur Schaffung eines neuen Blockchainsystems

Ebenfalls von *Fork* wird gesprochen, wenn das einer Blockchain zugrundeliegende Protokoll kopiert, modifiziert und wieder in Betrieb genommen wird mit dem Ziel, eine neue, eigenständige Blockchain zu erschaffen. Dies ist alleine mit dem BTC-Protokoll seit seiner Entstehung unzählige Male geschehen, wobei viele der so geschaffenen alternativen Blockchains und ihre dazugehörigen virtuellen Währungen (auch *Altcoins* genannt) nur kurz existieren, z.B. weil sie nie eine genügend grosse Gemeinschaft überzeugen können oder bloss

¹⁵ CHRISTIAN DECKER/ROGER WATTENHOFER, Information propagation in the Bitcoin network, 13th IEEE International Conference on Peer-to-Peer Computing 2013, 1 ff., 6.

¹⁶ AMY CASTOR, A Short Guide to Bitcoin Forks, <https://www.coindesk.com/short-guide-bitcoin-forks-explained/> (Abruf 27.10.2017).

¹⁷ MEISSER (FN 2), 84.

¹⁸ VITALIK BUTERIN, Bitcoin Network Shaken by Blockchain Fork, <https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/> (Abruf 27.10.2017).

¹⁹ BUTERIN (FN 18).

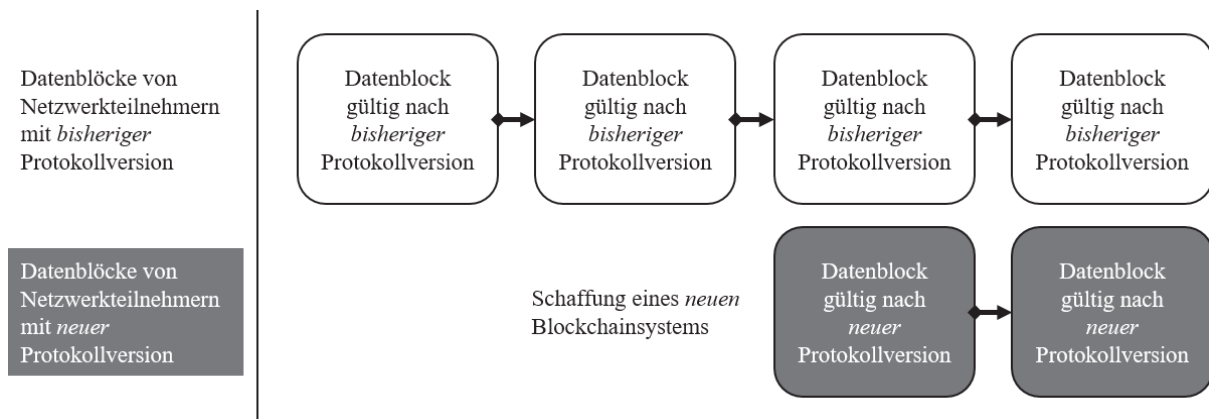


Abbildung 2: Schaffung eines neuen Blockchainsystems.

technische Spielereien darstellen.²⁰ In diesen Fällen wird zuweilen auch von einem *Codebase* oder *Software Fork* gesprochen.²¹

So entstanden sind allerdings auch valable Alternativen zu BTC, die eine eigene Nutzergemeinschaft versammelt haben. Eines der prominenteren Beispiele für eine solche BTC-Gabelung ist die Kryptowährung *Litecoin*.²² Hintergrund vieler dieser Blockchain-Protokoll-Gabelungen sind unterschiedliche Vorstellungen innerhalb der Nutzergemeinschaft (z.B. zwischen Entwickler und Minern) über die Weiterentwicklung des jeweiligen Blockchain-Protokolls. Es ist eine der Eigenarten offener Blockchainsysteme, dass jedermann zu jeder Zeit eine eigene neue Blockchain aus der Taufe heben kann.

In der Regel wird bei solchen Protokoll-Gabelungen eine neue *leere* Blockchain erschaffen, die mit Transaktionsstand null beginnt, d.h. die Kette von Datenblöcken ist zu Beginn nur sehr kurz und wird erst durch den laufenden Betrieb der neuen Blockchain erweitert. Dies bedeutet auch, dass jeder Nutzer, der auf der neuen Blockchain Transaktionen durchführen will, zuerst zu entsprechenden Währungseinheiten kommen muss (z.B. durch Mining, Kauf oder Erbringung von Dienstleistungen). Oder mit anderen Worten: Ein Nutzer, der auf der BTC-Blockchain eine gewisse Anzahl BTC kontrollierte, hat auf der Litecoin-Blockchain nicht automatisch die Verfügungsmacht über eine entsprechende Anzahl Litecoins, obwohl es sich bei Litecoin technisch um eine Gabelung des BTC-Protokolls handelt. Grafisch lässt sich der Fall der Protokoll-Spaltung wie in Abbildung 2 darstellen.

2.3 Beabsichtigte Gabelung eines bestehenden Blockchainsystems

Zur dritten Kategorie der *Forks* gehören nach unserem Dafürhalten all diejenigen, zumindest vorübergehenden Gabelungen eines bestehenden Blockchainsystems auf der Ebene der Transaktionsdatenbank, die von einer genügenden Anzahl Netzwerkteilnehmer eines Blockchainsystems *absichtlich* durch eine Veränderung der technischen Regeln des zugrundeliegenden Blockchain-Protokolls herbeigeführt werden.²³ Das Resultat entspricht mithin einer Gabelung der Blockchain in zwei Versionen durch Verwendung einer neuen Version des zugrundeliegenden Blockchain-Protokolls. In diese Kategorie fallen auch Veränderungen des Blockchain-Protokolls, die von der Mehrheit der Netzwerkteilnehmer begrüßt werden – d.h. auch unbestrittene Fehlerbehebungen oder Verbesserungen des Blockchain-Protokolls werden regelmässig in dieser Form umgesetzt. Diese dritte Kategorie lässt sich wiederum unterteilen in *Soft-Forks* (zu Deutsch: weiche Gabelung) und *Hard-Forks* (zu Deutsch: harte Gabelung) der Blockchain.²⁴

Eine der wichtigsten Eigenschaften einer weichen Gabelung liegt darin, dass die Netzwerkteilnehmer der bisherigen Version des Blockchain-Protokolls auch weiterhin (passive) Netzwerkteilnehmer sein können. Denn die bisherige Version des Blockchain-Protokolls akzeptiert die von der neuen Protokollversion generierten Datenblöcke weiterhin als gültig. Umgekehrt lehnt die neue Version des Blockchain-Protokolls die nach den Regeln der bisherigen Protokollversion erstellten Datenblöcke als ungültig ab. Die Gültigkeitsregeln sind mit anderen Worten in der neuen Version *strenger*. Hat die für die jeweilige Blockchain relevante Mehrheit der Netzwerk-

²⁰ Eine, zwischenzeitlich nicht mehr aktualisierte, graphische Übersicht der Gabelungen sowie Informationen zu deren Eigenschaften findet sich unter <http://mapofcoins.com/bitcoin#> (Abruf 27.10.2017).

²¹ WALSH (FN 14).

²² Vgl. <https://litecoin.com/> (Abruf 27.10.2017).

²³ Vgl. MAMORIA (FN 14).

²⁴ Vgl. zum Ganzen: ANDREAS M. ANTONOPOULOS, *Forkology: A Study of Forks for Newbies* 6. Juni 2017, <https://www.youtube.com/watch?v=rpeceXY1QBM> (Abruf 27.10.2017).

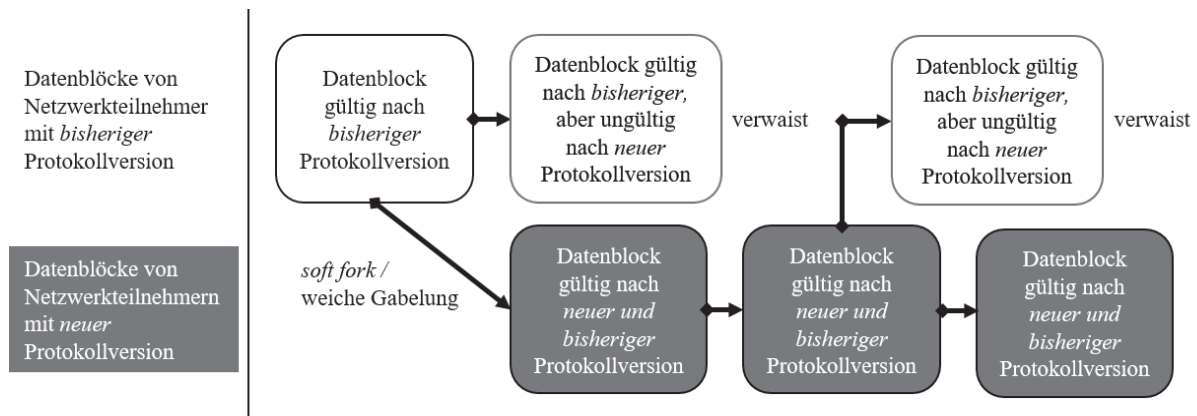


Abbildung 3: soft fork / weiche Gabelung.

teilnehmer²⁵ auf die neue Version gewechselt, so werden sie in absehbarer Zeit auch die längere Blockchain generieren, die sowohl nach der bisherigen als auch nach der neuen Protokollversion, und somit für alle Netzwerkteilnehmer, gültig ist. Die neue Version des Blockchain-Protokolls setzt sich *ohne dauerhafte Spaltung* der Transaktionsdatenbank im Netzwerk durch. Grafisch lässt sich der Fall der weichen Gabelung wie in Abbildung 3 darstellen.²⁶

Demgegenüber führt eine harte Gabelung dazu, dass die mit der neuen Version des Blockchain-Protokolls generierten Datenblöcke von den Netzwerkteilnehmern nach der bisherigen Protokollversion als ungültig zurückgewiesen und folglich nur vom neuen Teil des Netzwerks als gültig anerkannt werden. Die Gültigkeitsregeln sind mit anderen Worten in der neuen Protokollversion *weniger streng*. Folglich werden durch eine harte Gabelung zwei Versionen der Blockchain, einmal nach der neuen und einmal nach der bisherigen Protokollversion, von den zwei Gruppen von Netzwerkteilnehmern fortgesetzt. Wechseln sämtliche Netzwerkteilnehmer im Laufe der Zeit zu einer der beiden Protokollversionen, so wird nur eine Blockchain fortgesetzt. Grafisch lässt sich der Fall der harten Gabelung wie in Abbildung 4 darstellen.²⁷

Weiche Gabelungen sind folglich vorwärts kompatibel, während harte Gabelungen nur rückwärts kompatibel sind. Bei einer harten Gabelung entstehen somit immer zwei konkurrierende Versionen der bisherigen Blockchain, die sich eine Transaktionshistorie teilen. Bei einer weichen Gabelung hingegen konvergieren alle Netzwerkteilnehmer auf derselben Blockchain.²⁸ Wichtig ist,

dass es bei beiden Erscheinungsformen einer Gabelung *allein die Netzwerkteilnehmer* sind, die entscheiden, welche Version des Blockchain-Protokolls sie in Zukunft einsetzen. Den Betreibern der Netzwerkknoten steht es frei, entweder die alte Protokollversion weiter zu verwenden, oder ein Update auf die neue Software durchzuführen. Dies steht im Gegensatz zum bekannten Push-Modell der normalen Softwareupdates, bei dem regelmässig der Hersteller entscheiden kann, ob der Nutzer eine neue Version verwenden muss. Damit sind es auch ausschliesslich die Nutzer, die *durch ihr Verhalten* über die Durchführung von weichen und harten Blockchain-Gabelungen entscheiden.²⁹

3. Die Geburtsstunde von Bitcoin Cash

Die für diesen Aufsatz ausschlaggebende harte Gabelung ereignete sich am 1. August 2017 um 18:24 Uhr, indem der erste Datenblock mit Transaktionen generiert wurde, der nur unter der BCC-Version des Blockchain-Protokolls gültig war. Diese neue Version wird von dem sich abspaltenden Teil der Nutzergemeinschaft unter der Bezeichnung *Bitcoin Cash* als Konkurrenz zu BTC positioniert und soll ebenso wie das BTC-Protokoll auch in der Zukunft weiterentwickelt werden. Damit bestehen neu zwei Kryptowährungen, die zwar eine gemeinsame Transaktionshistorie teilen, in der Zukunft jedoch nicht kompatibel sind und sich je eigenständig weiterentwickeln werden. Ob eine in diesem Konkurrenzkampf obsiegt oder ob beide nebeneinander weiterbestehen, ist zurzeit nicht absehbar.

²⁵ Für das BTC-Protokoll ist dies die Mehrheit der Rechenleistung im Netzwerk.

²⁶ Angelehnt an: Developer Guide Bitcoin, <https://bitcoin.org/en/developer-guide> (Abruf 27.10.2017), Consensus Rule Changes.

²⁷ Angelehnt an: Developer Guide Bitcoin (FN 27), Consensus Rule Changes.

²⁸ ANTONOPOULOS (FN 24) illustriert dies anschaulich am Beispiel eines vormals vegetarischen Restaurants, bei dem die Köche (die

Entwickler) einmal entscheiden, zu veganer Küche zu wechseln (weiche Gabelung), und einmal, von nun an mit Fleisch zu kochen (harte Gabelung). Im ersten Fall können die Kunden (die Netzwerkteilnehmer), die vegetarisch essen (auf der alten Protokollversion sind), das Restaurant weiterhin besuchen. Im zweiten Fall hingegen werden sämtliche Vegetarier als Kunden des Restaurants ausgeschlossen.

²⁹ WALSH (FN 14).

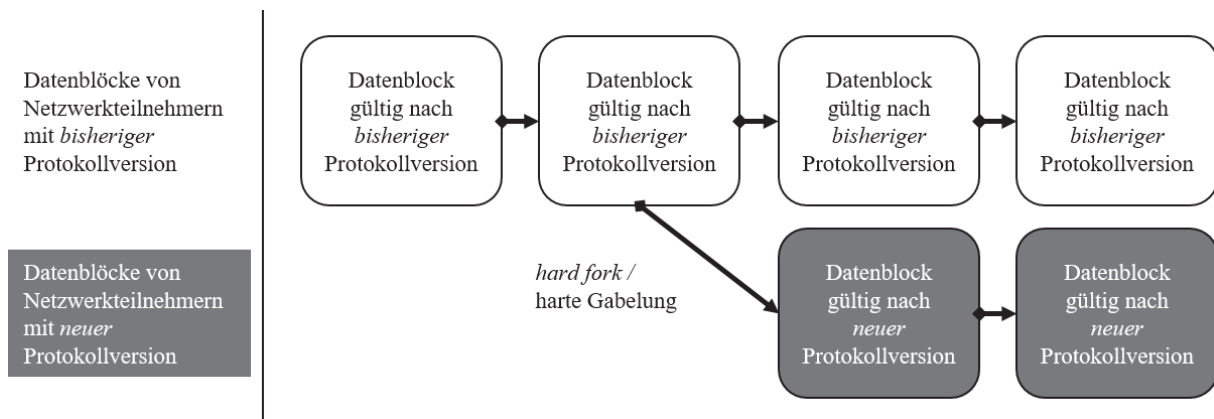


Abbildung 4: hard fork / harte Gabelung.

Anfänglicher Hauptunterschied zwischen BTC und BCC ist die Grösse der Datenblöcke, die bei BTC 1 MB beträgt und bei BCC 8 MB. Zudem besteht eine Reihe weiterer technischer Unterschiede. Auch wenn der Unterschied gering wirken mag, steckt dahinter eine jahrelange und zuweilen mit harten Bandagen geführte Diskussion innerhalb der BTC-Gemeinschaft. Zusammengefasst liegen die Gründe für diese Auseinandersetzung in einem tiefgreifenden Dissens zwischen einzelnen Gruppierungen innerhalb der BTC-Gemeinschaft darüber, wie BTC weiterentwickelt werden soll.³⁰

Bei dieser harten Gabelung kontrolliert der einzelne Nutzer, der vor der Gabelung eine bestimmte Anzahl BTC kontrollierte, nach der Gabelung eine identische Anzahl an BCC auf der BCC-Blockchain (oben II.2.3), und zwar zusätzlich zu den BTC, die er auch weiterhin kontrolliert. Die tatsächliche Verfügungsmacht über BTC und BCC übt der Nutzer mittels seiner Private Keys aus (oben II.1.2). Diese zusätzlichen Währungseinheiten sind eine Folge davon, dass die divergierenden Gabelungen (BTC bzw. BCC) eine gemeinsame Transaktionshistorie teilen. Der Wert dieser beiden nun unabhängig voneinander existierenden virtuellen Währungen wird wiederum ausschliesslich durch den Markt bestimmt.

III. Die auftragsrechtliche Ablieferungspflicht

1. Das Auftragsverhältnis im Allgemeinen

Beim Auftrag nach schweizerischem Obligationenrecht handelt es sich um einen Arbeitsleistungsvertrag i.w.S. bei dem der Beauftragte gewisse Dienstleistungen zu erbringen hat im Hinblick auf ein bestimmtes Resultat. Dabei führt der Beauftragte ein fremdes Geschäft und hat die fremden Interessen zu wahren. Ein Erfolg ist regelmässig nicht geschuldet.³¹ Der Auftrag ist das «Sammelbecken» des schweizerischen Vertragsrechts, indem er subsidiär Anwendung findet, wenn kein Sonderrecht auszumachen ist.³² Besondere Wesensmerkmale des Auftrags sind die Treuepflicht, ein besonderes Vertrauensverhältnis sowie oft ein besonderer Persönlichkeitsbezug. Der Beauftragte handelt auf Rechnung und auf Gefahr des Auftraggebers.³³ Der Auftrag kommt damit für viele Leistungen in Frage (z.B. Tathandlungen, Rechtshandlungen, Treuhand, etc.) und ist insbesondere im Bereich der Finanzdienstleistungen ein häufig anzutreffender Vertragstypus.³⁴

2. Die Rechenschaftspflicht nach Art. 400 OR

Unter dem Randtitel «Rechenschaftsablegung» regelt Art. 400 OR drei Teilaspekte der auftragsrechtlichen Vertragsbeziehung: die Rechenschaftspflicht i.e.S., die im Folgenden besonders interessierende Ablieferungspflicht (auch als Herausgabepflicht bezeichnet) sowie die Verpflichtung zur Verzinsung der herauszugebenden

³⁰ Für ausführlichere Informationen zu den Argumenten auf beiden Seiten vgl.: WILL JANENSCH, Understanding The Bitcoin Block Size Debate: Decentralized Governance and the Challenge of Scaling, <https://medium.com/@WJanensch/understanding-the-bitcoin-block-size-debate-decentralized-governance-and-the-challenge-of-scaling-98912d465dd7> (Abruf 27.10.2017); ROB BLASETTI, What You Need To Know About The Bitcoin Scaling Debate, <https://decentralize.today/what-you-need-to-know-about-the-bitcoin-scaling-debate-48b9734d062e> (Abruf 27.10.2017).

³¹ BSK OR I-WEBER, Art. 394 N 1 f.

³² BSK OR I-WEBER, Art. 394 N 22.

³³ BSK OR I-WEBER, Art. 394 N 3.

³⁴ BSK OR I-WEBER, Art. 394 N 7 f.

Gelder.³⁵ Der Gesetzestext von Art. 400 OR lautet wie folgt:

- ¹ Der Beauftragte ist schuldig, auf Verlangen jederzeit über seine Geschäftsführung Rechenschaft abzulegen und alles, was ihm infolge derselben aus irgendeinem Grunde zugekommen ist, zu erstatten.
- ² Gelder, mit deren Ablieferung er sich im Rückstande befindet, hat er zu verzinsen.

Nach der bundesgerichtlichen Rechtsprechung ist die Rechenschaftspflicht zwingende Folge der Fremdgeschäftsführung im Auftragsverhältnis und zugleich Voraussetzung und Grundlage der Ablieferungspflicht.³⁶ Bei der Rechenschaftspflicht i.e.S. lassen sich die Komponenten Informationspflicht und Abrechnungspflicht unterscheiden. Die Informationspflicht beinhaltet insbesondere eine Pflicht zur aktiven und unaufgeforderten Benachrichtigung sowie eine Pflicht, dem Auftraggeber alle erforderlichen Auskünfte zu erteilen.³⁷ Der Beauftragte hat zum Beleg seiner fremdnützigen und haushälterischen Ausführung des Auftrags eine Abrechnung zu erstellen und dazu alle erforderlichen Belege und Akten aufzubewahren.³⁸ Auf die Informationspflicht als eigenständige Rechtspflicht wird nicht näher eingegangen.

3. Die Ablieferungspflicht im Besonderen

3.1 Gegenstand der Ablieferungspflicht

Die Ablieferungspflicht ergibt sich aus dem zweiten Satzteil von Art. 400 Abs. 1 OR, wonach der Beauftragte «alles, was ihm infolge [der Geschäftsführung] aus irgendeinem Grunde zugekommen ist, zu erstatten» hat. Die so umschriebene Ablieferungspflicht ist eine Folge der Fremdgeschäftsführung des Auftragsverhältnisses und bedeutet Sachleistung mit Erfolgshaftung.³⁹ Die *Erstattung* ist als Begriff nach der h.L. zu eng, da die auftragsrechtliche Ablieferungspflicht nicht nur das betrifft, was vom Auftraggeber erhalten wurde, sondern vielmehr umfassend zu verstehen ist.⁴⁰

Nach dem Bundesgericht ist die Ablieferungspflicht «ein zentrales Element der Fremdgeschäftsführung des Auftrags», «lässt sich als Konkretisierung der Treuepflicht nach Art. 392 Abs. 2 OR verstehen» und beugt insbesondere der Gefahr vor, dass der Beauftragte aufgrund der Zuwendungen durch Dritte die Interessen des Auftraggebers nicht ausreichend berücksichtigt.⁴¹ Aus der Treuepflicht wird zuweilen auch der Anspruch des Auftraggebers abgeleitet, den «erzielten Nettotonutzen tat-

sächlich zugewendet» zu erhalten.⁴² Die Ablieferungspflicht bildet dabei das Gegenstück zur Schadloshaltung des Beauftragten durch den Auftraggeber. Was der Beauftragte erworben oder erhalten hat, darf nicht bei ihm zurückbleiben, und zugleich muss er für das, «was er nicht erwerben konnte, [...] den Schaden nicht an sich selbst tragen».⁴³ Je nachdem, welcher Typus Vermögenswert ablieferungspflichtig ist, hat der Beauftragte alles Erforderliche zu unternehmen, um diesen dem Auftraggeber abzuliefern. Das bedeutet, dass er z.B. an Sachen Eigentum einzuräumen und Forderungen zu zedieren hat.⁴⁴

Der Beauftragte hat grundsätzlich alles abzuliefern, was er vom Auftraggeber zur Ausführung erhalten, in Erfüllung des Auftrags geschaffen oder im Rahmen der Ausführung des Auftrags erlangt hat.⁴⁵ Dazu gehören grundsätzlich alle Vermögenswerte wie Wertpapiere, Bucheffekten, Geld, obligatorische Rechte sowie Gegenstände aller Art wie Pläne, Dokumente etc.⁴⁶, aber auch Gegenstände ohne ersichtlichen Wert.⁴⁷ Die Ausnahme bilden rein interne Dokumente, für die regelmässig keine oder eine eingeschränkte Ablieferungspflicht besteht.⁴⁸

3.2 Begrenzung der Ablieferungspflicht durch «inneren Zusammenhang»

Je nach Art des Auftrags ziehen Lehre und Rechtsprechung die Grenze für die Ablieferungspflicht unterschiedlich.⁴⁹ Anschaulich illustrieren lässt sich dies am Typus der Vermögensverwaltungsverträge. Denn besonders intensiv geführt wird die Diskussion um die Grenzen der Ablieferungspflicht bei den sogenannten Retrozessionen, die bei Vermögensverwaltungsverträgen und ähnlichen Auftragsverhältnissen, wie der Anlageberatung, anfallen. Unter Retrozessionen versteht man u.a. die Weitergabe der durch die Bank für ihre Tätigkeit von Dritten erhaltenen Kommissionen an den Vermögensverwalter gestützt auf eine mit diesem getroffene Abmachung.⁵⁰ Bei Vermögensverwaltung und ähnlichen Dienstleistungen liegen dabei Dreipersonenverhältnisse vor, in denen der Beauftragte als Intermediär handelt (z.B. Auftraggeber – Vermögensverwalter – Bank oder Auftraggeber – Bank – Fondsanbieter).⁵¹

³⁵ BSK OR I-WEBER, Art. 400 N 1 f.; BK-FELLMANN, OR 400 N 7 ff.

³⁶ BGE 110 II 181 E. 2.

³⁷ BSK OR I-WEBER, Art. 400 N 2 ff. und N 12; BK-FELLMANN, OR 400 N 19 ff.

³⁸ BSK OR I-WEBER, Art. 400 N 7 f.; BK-FELLMANN, OR 400 N 23.

³⁹ BSK OR I-WEBER, Art. 400 N 10 f.; BK-FELLMANN, OR 400 N 125.

⁴⁰ Vgl. statt vieler m.w.H. BK-FELLMANN, OR 400 N 10.

⁴¹ BGE 138 III 755 E. 5.3.

⁴² BK-GAUTSCHI, Art. 400 N 3b.

⁴³ BK-GAUTSCHI, Art. 400 N 6a.

⁴⁴ BSK OR I-WEBER, Art. 400 N 11; BK-FELLMANN, OR 400 N 120 f.

⁴⁵ WAYGOOD-WEINER (FN 4), 90.

⁴⁶ BK-FELLMANN, OR 400 N 11, 116, 130; vgl. im speziellen für Bucheffekten BGE 137 III 393 E. 5.3.1.

⁴⁷ BK-FELLMANN, OR 400 N 122.

⁴⁸ BSK OR I-WEBER, Art. 400 N 11.

⁴⁹ Vgl. dazu jeweils m.w.H. VITO ROBERTO, Die auftragsrechtliche Herausgabepflicht des «Erlangten», ZSR 2009, 15 ff.; BSK OR I-WEBER, Art. 400, N 12 ff.

⁵⁰ Vgl. ROLF KUHN, Retrozessionszahlungen an externe Vermögensverwalter – eine Standortbestimmung, AJP 2006, 1051 ff., 1053.

⁵¹ Vgl. ROBERTO (FN 49), 18 f.; KUHN (FN 50), 1051.

Das Bundesgericht entschied die Kontroverse um die Ablieferungspflicht von Retrozessionen bei den Vermögensverwaltungsaufträgen in BGE 132 III 460 grundsätzlich zugunsten der Auftraggeber und bejahte eine Ablieferungspflicht. Der Fall betraf einen Vermögensverwalter einer Stiftung, der Provisionen und Finder's Fees, die er von Banken für seine Anlagetätigkeit auf Rechnung der Stiftung erhalten hatte, einbehielt. Es ging somit um Vermögenswerte, die der Beauftragte von Dritten erhalten hatte. Das Bundesgericht stellte dabei u.a. fest, dass die Ablieferungspflicht des Beauftragten auch «indirekte Vorteile, die dem Beauftragten infolge der Auftragsausführung von Dritten zukommen», beschlage, und führte weiter aus, dass «der Beauftragte [...] durch den Auftrag weder gewinnen noch verlieren [soll]», sondern «alle Vermögenswerte, welche in einem inneren Zusammenhang mit dem erteilten Auftrag stehen, herausgeben müsse. Nur das, was er «lediglich bei Gelegenheit der Auftragsausführung, ohne inneren Zusammenhang mit dem ihm erteilten Auftrag, von Dritten erhält», dürfe der Auftragnehmer behalten.⁵² Bemerkenswerterweise wird das Thema Interessenkonfliktpotenzial, welches in der Rechtsprechung (siehe sogleich unten) und in der Lehre sehr viel Beachtung fand, in diesem ersten Leiturteil nur im Zusammenhang mit dem gültigen Verzicht erwähnt.⁵³ Als Voraussetzung für die Ablieferungspflicht bzw. als Anknüpfungspunkt für den inneren Zusammenhang erwähnt es das Bundesgericht noch nicht.

Seitdem hat sich das Bundesgericht in mehreren Entscheidungen mit der Ablieferungspflicht befasst.⁵⁴ Es stellte dabei u.a. fest, dass eine Umschreibung all derjenigen Fälle, bei denen ein innerer Zusammenhang bei Zuwendungen eines Dritten besteht, nicht möglich sei.⁵⁵ Als Massstab für das Vorliegen eines inneren Zusammenhangs bei Zuwendungen eines Dritten wendet das Bundesgericht zwei Grundsätze an, die, soweit ersichtlich, nebeneinander bestehen.⁵⁶

Der erste Grundsatz ist die angestrebte Vorbeugung von Interessenkonflikten zur Sicherung der Fremdnützigkeit des Auftrags, wobei nicht erforderlich ist, dass der Beauftragte tatsächlich pflichtwidrig handelt bzw. der Auftraggeber einen konkreten Nachteil erleidet.⁵⁷ Bei der Retrozessionsthematik steht dieses Kriterium im Vordergrund, da dabei stets Zuwendungen von Dritten

an den Auftragnehmer im Fokus stehen, bei denen regelmässig Interessenskonfliktpotential besteht.

Der zweite Grundsatz ist, dass der Beauftragte, abgesehen von einem allfälligen Honorar, durch den Auftrag «weder gewinnen noch verlieren soll»⁵⁸ bzw. «durch den Auftrag keinen Vermögensvorteil erlangen soll»⁵⁹. Mit anderen Worten handelt es sich um den Grundsatz der Nichtbereicherung des Beauftragten.⁶⁰

Die bundesgerichtliche Feststellung, dass eine umfassende Beschreibung der Konstellationen mit innerem Zusammenhang nicht möglich ist, beschlägt u.E. nicht nur die Fälle, in denen eine Zuwendung von Dritten erfolgt, sondern die beiden deckungsgleichen Formeln des *inneren Zusammenhangs* bzw. *infolge des Auftrags* schlechthin.⁶¹ Auch wenn ein Vermögenswert nicht von Dritten zugewendet wird und folglich überhaupt kein Interessenkonfliktpotential vorliegen kann, unterscheidet das Bundesgericht zwischen infolge des Auftrags und bei Gelegenheit des Auftrags erlangten Vorteilen.⁶² Während sich das Bundesgericht bei Fällen mit vorhandenem Interessenkonfliktpotential geradezu für eine automatische Bejahung des inneren Zusammenhangs auszusprechen scheint,⁶³ ist die Abgrenzung dort diffiziler, wo in Ermangelung eines solchen Potentials nur der Grundsatz der Nichtbereicherung zur Beurteilung des inneren Zusammenhangs beigezogen werden kann. Dann muss in jedem Einzelfall diskutiert werden, ob der fragliche Vermögenswert in Erfüllung des Auftrags angefallen ist oder nicht. Diese Beurteilung gilt es im Folgenden auch für die harte Gabelung der BTC-Blockchain vorzunehmen.

3.3 Dispositive Natur der Ablieferungspflicht

Erwähnenswert ist noch, dass das Bundesgericht die grundsätzlich dispositive Natur der Ablieferungspflicht bejaht hat, wobei jedoch eine «vollständige und wahrheitsgetreue» Information des Auftraggebers über die zu erwartenden Retrozessionen sowie eine klare Verzichtsbekundung vorausgesetzt wurden.⁶⁴ Was diese Formel konkret bedeutet, stellte das Bundesgericht erst in BGE 137 III 393 klar. Ohnehin hat sich das Bundesgericht seit dem Leiturteil BGE 132 III 460 hauptsächlich mit den Verzichtsanforderungen beschäftigt und nur am Rande mit dem inneren Zusammenhang als Grenze der Ablie-

⁵² BGE 132 III 460 E. 4.1.

⁵³ BGE 132 III 460 E. 4.2.

⁵⁴ Die wichtigsten sind BGE 137 III 393, BGE 138 III 137 sowie BGE 138 III 755. Zuletzt bestätigt wurde die Rechtsprechung in BGE 4A_508/2016 E. 5.1.1. ff. Ausgeklammert wird vorliegend der Entscheid BGE 6B_223/2010 vom 13. November 2011, da das Bundesgericht selbst in BGE 138 III 755 E. 5.2 feststellte, dieser habe sich nicht näher mit der Ablieferungspflicht befasst und es handle sich nicht um einen Grundsatzentscheid.

⁵⁵ BGE 138 III 755 E. 5.3.

⁵⁶ Vgl. WAYGOOD-WEINER (FN 4), 97.

⁵⁷ BGE 138 III 755 E. 5.3; vgl. WAYGOOD-WEINER (FN 4), 100 f.

⁵⁸ BGE 137 III 393 E. 5.3.1; BGE 138 III 755 E. 4.2 und 5.3.

⁵⁹ BGE 138 III 137 E. 5.3.3.

⁶⁰ WAYGOOD-WEINER (FN 4), 97, 103 ff.

⁶¹ Vgl. ROBERTO (FN 49), 20.

⁶² BGE 138 III 755 E. 4.2.

⁶³ BGE 138 III 755 E. 5.3, in enger Anlehnung an BK-FELLMANN, OR 400 N 128: «Bei Zuwendungen Dritter ist ein innerer Zusammenhang schon dann zu bejahen, wenn die Gefahr besteht, der Beauftragte könnte sich dadurch veranlasst sehen, die Interessen des Auftraggebers nicht ausreichend zu berücksichtigen.»

⁶⁴ BGE 132 III 460 E. 4.2.

ferungspflicht.⁶⁵ Auf die Verzichtfrage wird vorliegend nicht näher eingegangen.⁶⁶

IV. Fallgruppen

Mit der zunehmenden Verbreitung von BTC und weiterer Kryptowährungen buhlt eine zunehmende Anzahl Dienstleister in diesem Wirtschaftszweig um Kundenschaft. Eine der neu entstehenden Branchen umfasst vielfältige Dienstleistungen rund um das Sichern, Halten und Verwalten von BTC. Eine andere ist auf das Handeln virtueller Währungen fokussiert.

Es ist für einen BTC-Nutzer möglich, die Private Keys in digitaler Form auf eigenen Computern, USB-Sticks, Smartphones etc. oder aber in physischer Form auf Papier aufbewahren (siehe oben II.1.2), ohne dass diese jemals in den Herrschaftsbereich eines Dienstleisters geraten. Diese Form der Private-Key-Verwaltung dürfte zurzeit (noch) die häufigste Erscheinungsform sein, da viele BTC-Nutzer einen relativ hohen technischen Wissensstand aufweisen. Bei dieser Selbstverwaltung liegt mangels involvierten Dienstleisters überhaupt kein Vertragsverhältnis vor. Eine Ablieferungspflicht kann folglich ebenso wenig vorliegen. Es obliegt alleine dem BTC Nutzer, den Zugriff zu seinen BCC sicherzustellen und diese nach der harten Gabelung mittels seines BTC Private Keys unter seine Kontrolle zu bringen. Dieser Vorgang wird meist als *coin-split* bezeichnet. Begeht der BTC-Nutzer bei diesem keinen technischen Fehler, erhält er die faktische Verfügungsmacht über die gleiche Anzahl BCC, die er auch als BTC kontrolliert.

Relevant ist die Frage nach der Ablieferungspflicht folglich nur, wenn der Nutzer *keinen* direkten Zugriff auf seine BTC Private Keys und/oder seine BTC hat. Zur besseren Veranschaulichung unterscheiden wir hierzu drei Fallgruppen. Dies bringt zwangsläufig eine Vereinfachung der vielfältigen Dienstleistungsmodelle und zugrundeliegenden technischen Systeme mit sich. In der Praxis wird man um die genaue Analyse der tatsächlichen und rechtlichen Umstände des Einzelfalls nicht herumkommen. Wir gehen davon aus, dass das Auftragsrecht im Vordergrund der entsprechenden Vertragsverhältnisse steht und insb. Art. 400 OR anwendbar ist.

1. Fremdverwaltung der Bitcoin Private Keys

Unsere erste Fallgruppe bilden diejenigen BTC-Nutzer, die ihre BTC Private Keys durch einen Dienstleister fremdverwalten lassen (sog. Wallet- bzw. Custody-Pro-

vider). In erster Linie verfolgt solche Fremdverwaltung den Zweck, den Zugang und die Nutzbarkeit der eigenen BTC zu verbessern (z.B. mittels Zurverfügungstellung einer durch die BTC gedeckten Kreditkarte durch den Beauftragten).⁶⁷ Für solche Fremdverwaltungsdienstleistungen gibt es viele unterschiedliche Erscheinungsformen, die sich bezüglich der technischen Verfügungsmacht des Dienstleisters über die Private Keys bzw. der BTC sowie der Komplexität der angebotenen Dienstleistungen unterscheiden. Vor dem Hintergrund der Ablieferungspflicht im Besonderen kann man u.E. jedoch zwei Gruppen bilden: Einerseits diejenigen Private Key Verwalter, die die alleinige Verfügungsmacht über die Private Keys und damit über die BTC des Kunden haben, und andererseits die Private Key Verwalter, die ausschliesslich gemeinsam mit dem Kunden über die Private Keys verfügen können (z.B. mittels MultiSig, siehe oben II.1.2). Qualifiziert man die BTC Private Keys nicht als Sache, so finden die Bestimmungen zum Hinterlegungsvertrag nach Art. 472 OR keine Anwendung.⁶⁸

2. Auftrag zur Beschaffung von Bitcoin

Unsere zweite Fallgruppe bilden diejenigen Auftraggeber, die *vor* der harten BTC-Gabelung die Beschaffung von BTC in Auftrag gegeben haben und bei welchen der Beauftragte die BTC *vor* der harten BTC-Gabelung auf der BTC-Blockchain in eigenem Namen, aber auf Rechnung des Auftraggebers beschafft hat, die BTC jedoch erst *nach* der harten BTC-Gabelung dem Auftraggeber ausliefert.⁶⁹ In einer solchen Konstellation lautet der Auftrag (nur) auf BTC, jedoch hat der Beauftragte in der Zeit zwischen harter Gabelung und Auslieferung auch Zugriff auf die BCC. Es liegt folglich in seiner Hand, ob er dem Auftraggeber nur die BTC oder die BTC zusammen mit den BCC ausliefert. Hier liegt ein Kommissionsgeschäft nach Art. 425 OR nahe. Qualifiziert man BTC jedoch nicht als Sache oder als Devise⁷⁰, so finden die Bestimmungen zum Kommissionsgeschäft, die Kraft Art. 425 Abs. 2 OR ohnehin auf Auftragsrecht verweisen, höchstens analoge Anwendung.⁷¹

⁶⁵ WAYGOOD-WEINER (FN 4), 91.

⁶⁶ KUHN (FN 50), 1053; vgl. zudem die Auflistung der vielfältigen Lehrmeinungen in BGE 137 III 393 E. 2.2.

⁶⁷ BARBARA GRAHAM-SIEGENTHALER/ANDREAS FURRER, The Position of Blockchain Technology and Bitcoin in Swiss Law, Jusletter 8. Mai 2017, Rz. 80.

⁶⁸ Bejaht man hingegen eine Sachqualifikation und damit die Anwendung des Hinterlegungsrechts, so könnte es sich bei den anfallenden BCC um einen Zuwachs im Sinne von Art. 475 Abs. 1 OR handeln, welcher vom Hinterleger herausgefordert werden kann; vgl. BSK OR I-KOLLER, 475 N 3.

⁶⁹ Die umgekehrte Konstellation einer Verkaufskommission lautend auf BTC wirft diese Frage u.E. nicht auf, da der Verkaufserlös stets in Schweizer Franken vorliegen wird und nie BCC anfallen. Der allenfalls schwankende Verkaufspreis von BTC infolge der harten Gabelung ändert daran grundsätzlich nichts.

⁷⁰ Vgl. insb. zur Anwendbarkeit auf Devisengeschäfte BGer 4C.152/2002 E. 2.1 f. vom 22 Juli 2002 sowie BGer 4C.89/2005 E. 3.2.2.3 vom 13. Juli 2005

⁷¹ Vgl. BSK OR I-LENZ/VON PLANTA, Art. 425 N 2.

3. Kontoführung lautend auf Bitcoin

Unsere dritte Fallgruppe bilden all diejenigen Auftraggeber, die statt der eigenen oder delegierten Verfügungsmacht über ihre BTC Private Keys (Selbst- bzw. Fremdverwaltung) bei einem Dienstleister ein auf BTC lautendes Konto und damit einen vertraglichen Anspruch auf Lieferung von BTC besitzen. Für die Zwecke der weiteren Ausführungen gehen wir davon aus, dass dabei auf Wunsch des Kunden vonseiten des Beauftragten stets eine *tatsächliche* Lieferpflicht für die BTC besteht. Finanzdienstleister, die solche BTC-Konten anbieten, sind typischerweise Handelsplattformen (auch *exchanges* genannt), Broker und zunehmend auch Banken.

V. Auftragsrechtliche Ablieferungspflicht beim Bitcoin-Hardfork

1. Unterschied zur Retrozessionsthematik

In jeder der drei Fallgruppen geht es im Kern um die Frage, ob die Beauftragten die im Rahmen ihrer Dienstleistungserbringung anfallenden BCC den Auftraggebern abliefern müssen oder ob der Beauftragte sich mit gutem Recht auf den Standpunkt stellen kann, dass diese ihm selbst zustehen. Oder anders ausgedrückt: Besteht für die bei der harten BTC-Gabelung anfallenden BCC eine Ablieferungspflicht aus Art. 400 OR? Die folgenden Ausführungen beziehen sich dabei auf Konstellationen, in denen ausschliesslich dispositives Recht betreffend die Ablieferungspflicht zur Anwendung kommt.

Bevor nachfolgend die von der Rechtsprechung zur Ablieferungspflicht entwickelten Kriterien angewendet werden, muss ein Unterschied zwischen der harten BTC-Gabelung und der Retrozessionsthematik hervorgehoben werden: Da es sich bei der BTC-Blockchain wie erwähnt um ein intermediärloses System handelt (siehe oben II.1.1), sind die dem Beauftragten zufallenden BCC gerade keine Zuwendungen eines Dritten, sondern eine natürlicherweise auftretende technische Folge der harten Gabelung. Dies im Gegensatz zu den vielfältigen vermögenswerten Vorteilen, die der Retrozessionsrechtsprechung zugrunde liegen, welche stets von Dritten stammen.

2. Bitcoin Cash als Vermögenswert

Die Tatsache, dass digitale Daten einen wirtschaftlichen Wert haben können und auch in vielfältiger Form das Objekt von Kauf-, Lizenz- und weiteren Verträgen sind, dürfte heute unbestritten sein.⁷² Folglich ist un-

zweifelhaft, dass es sich bei BCC um einen grundsätzlich ablieferungsfähigen Vermögenswert im Sinne des Auftragsrechts handelt, zumal die Ablieferungspflicht selbst Gegenstände ohne erkennbaren Wert beschlagen kann.⁷³ Ähnliches dürfte jedenfalls für alle Tokens von Blockchainsystemen gelten, die handelbar sind und einen Marktpreis besitzen. Die Frage, ob es sich bei BTC gar um Sachen im Sinne von Art. 641 Abs. 1 ZGB handelt, kann daher für die nachfolgenden Ausführungen offenbleiben.⁷⁴

Zusätzlich fragt sich, wann der neue Vermögenswert in der Form der BCC als erlangt gelten soll. Nach unserem Dafürhalten sollten die BCC ab jenem Zeitpunkt als erlangt gelten, ab dem es dem Beauftragte mittels seines Private Keys technisch möglich ist, über die BCC zu verfügen. Dies kann je nach den technischen Gegebenheiten einer harten Gabelung einige Zeit dauern, wenn z.B. erst eine stabile Lösung für den *coin-split* in die vom Beauftragten verwendete Softwarelösung integriert werden muss oder aber gar die Überlebensfähigkeit der harten Gabelung selbst infolge der Mehrheiten im Netzwerk noch nicht geklärt ist. Alternativ sollte es mit Zustimmung des Auftraggebers stets möglich sein, dass der Beauftragte direkt den BTC Private Key übergibt, ohne dass er über die neuen BCC je verfügt hat und damit den *coin-split* allein dem Auftraggeber überlässt.

3. Blockchain-Gabelung als indirekter Vorteil

Bei den dem Beauftragten zukommenden Vorteilen unterscheidet das Bundesgericht zwischen direkten und indirekten Vorteilen. Die direkten Vorteile sind diejenigen, die dem Beauftragten vom Auftraggeber zur Erfüllung des Auftrags zur Verfügung gestellt werden. Indirekte Vorteile sind all diejenigen, die dem Beauftragten infolge oder bei Gelegenheit der Auftragsausführung zukommen.⁷⁵ Die direkten Vorteile unterliegen in jedem Fall der Ablieferungspflicht, während die indirekten Vorteile nur dann der Ablieferungspflicht unterliegen, wenn sie dem Beauftragten nicht bloss bei Gelegenheit der Auftragsausführung zugekommen sind.

Für die zweite und dritte Fallgruppe ist eindeutig, dass es sich bei den anfallenden BCC um einen indirekten Vor-

⁷³ BK-FELLMANN, OR 400 N 122.

⁷⁴ Vgl. dazu ausführlich m.w.H. GRAHAM-SIEGENTHALER/FURRER (FN 67), 11 ff.; potentiell irreführend ist hingegen die vor kurzem erfolgte Sacheinlagegründung der Blockchain & Cryptocurrency Services Zug AG (SHAB Nr. 188 vom 25.09.2017, Meldung-Nr. 3777579) in der das Handelsregisteramt Zug eine Sacheinlage von 19 BTC «in unbeschwertem Eigentum» zum Gegenwert von 66'500 Schweizer Franken akzeptierte. Angesichts der Praxis zur Sacheinlage, wonach eine solche z.B. auch in der Form von werthaltigen Forderungen oder Immaterialgüterrechten erfolgen kann, darf dies nicht als Bestätigung der Sachqualifikation von BTC gelesen werden.

⁷⁵ BGE 132 III 460 E. 4.1. sowie BGE 138 III 755 E. 4.2.

⁷² GRAHAM-SIEGENTHALER/FURRER (FN 67), 16 ff.

teil handelt, da diese dem Beauftragten nicht vom Auftraggeber zur Verfügung gestellt werden, sondern, wie beschrieben, dem Beauftragten als technisches Ergebnis der harten Gabelung zukommen (siehe oben II.2 und II.3).

Für die erste Fallgruppe ist es anspruchsvoller zu beantworten, ob es sich bei den BCC um einen direkten oder indirekten Vorteil handelt. Denn vorderhand wird der Private Key durch den Auftraggeber dem Beauftragten zur Verfügung gestellt, unter Umständen mit dem Ziel, von den dadurch ermöglichten Dienstleistungen des Beauftragten profitieren zu können. Man könnte daraus ableiten, dass es sich bei den anfallenden BCC um einen direkten Vorteil handelt, da der zur Verfügung über die (bisherigen) BTC und die (neuen) BCC ermächtigende Private Key gerade vom Auftraggeber kommt. Eine solche Schlussfolgerung wäre jedoch unzutreffend. Denn der Private Key des Auftraggebers erlaubt die Verfügung über den «Saldo» aller vorangegangenen BTC-Transaktionen. Vereinfacht ausgedrückt handelt es sich bei diesem Saldo um eine Kette von Signaturen, deren Endpunkt das Ausmass der Verfügungsmacht beschreibt. Selbst wenn nun der identische Private Key auf der neuen BCC-Blockchain ebenfalls Verfügungen ermöglicht, so ist die BCC-Blockchain mit den dazugehörigen Verfügungsmöglichkeiten nichtsdestotrotz komplett neu entstanden. Der Beauftragte hat die neue Verfügungsmöglichkeit über BCC folglich gerade nicht vom Auftraggeber als direkten Vorteil erhalten, sondern sie ist ebenfalls eine rein technische Folge der harten Gabelung und damit ein indirekter Vorteil.

4. Innerer Zusammenhang

Das abschliessende Kriterium im bundesgerichtlichen Prüfungsschema zur Ablieferungspflicht ist die Frage nach einem inneren Zusammenhang zwischen dem Auftragsverhältnis und dem indirekten, dem Beauftragten zugekommenen Vorteil. Die nachfolgenden Ausführungen dazu und die damit verbundene Auseinandersetzung mit dem jeweiligen Zweck der einzelnen Auftragsverhältnisse erlauben es folglich auch, die Ablieferungspflicht im Einzelfall zu bejahen oder zu verneinen.

4.1 Abgrenzung gemäss Lehre und Rechtsprechung

Das Bundesgericht orientiert sich in der Retrozessionsrechtsprechung bei der Frage nach der Ablieferungspflicht indirekter Zuwendungen durch Dritte in erster Linie am Interessenkonfliktpotential der entsprechenden Zuwendung. Mangels Gegenpartei, deren Interessen anstelle derjenigen des Beauftragten in den Vordergrund treten könnten, kann die Retrozessionsrechtsprechung nicht unmittelbar auf die harte BTC-Gabelung angewendet werden. Ob der Beauftragte dem Auftraggeber Zu-

gang zu den bei der harten BTC-Gabelung anfallenden BCC gewährt, ist nicht Ergebnis der Interessenwahrung zugunsten des Auftraggebers oder aber eines Dritten. Denn der Beauftragte wird, vorbehaltlich besonderer Umstände, in der Regel keinen Einfluss darauf haben, ob eine harte Gabelung stattfindet oder nicht. Folglich besteht auch kein Potential für einen Interessenskonflikt beim Beauftragten.

Eine solche aufwandlose Vermehrung eines Gutes findet in der analogen Welt kaum Entsprechung. Der harten BTC-Gabelung wohl am nächsten kommen der Erhalt von Gratisaktien oder das Anfallen von natürlichen Früchten.⁷⁶ Bei Ersterem handelt es sich jedoch wiederum um eine Zuwendung von Dritten, bei Letzterem ergibt sich die Eigentumsposition unmittelbar aus Art. 643 ZGB. Bei der harten BTC-Gabelung handelt es sich folglich um ein neuartiges Phänomen. Die Tatsache, dass die BCC keine Zuwendung durch Dritte sind und in der analogen Welt keine genaue Entsprechung finden, steht einer Ablieferungspflicht jedoch nicht entgegen, wenn die Anknüpfungskriterien erfüllt sind.

Ohne Interessenkonfliktpotential als Anknüpfungspunkt besteht nach der bundesgerichtlichen Rechtsprechung ein innerer Zusammenhang dort, wo ein Vermögenswert *infolge* und nicht nur *bei Gelegenheit* des Auftrags vom Beauftragten erhalten wurde. Der Begriff des inneren Zusammenhangs wird m.a.W. negativ abgegrenzt gegenüber den Gelegenheitsvorteilen. Diese Abgrenzung ist, wie die Lehre dargelegt hat, in der Praxis anspruchsvoll.⁷⁷ Da auch bei Gelegenheit erhaltene Vermögenswerte in einem natürlichen und adäquaten Kausalzusammenhang zum Auftrag stehen können, kann dies als alleiniges Abgrenzungskriterium nicht ausschlaggebend sein. Das Bundesgericht selbst hat, soweit ersichtlich, abgesehen vom Kriterium des Interessenkonfliktpotentials, kaum verallgemeinerungsfähige Kriterien für diese Abgrenzung herausgearbeitet. Es verweist jeweils allgemein auf den Grundsatz der Nichtbereicherung und scheint zugleich auf den Zweck des jeweiligen Auftragsverhältnisses im Einzelfall abzustellen.⁷⁸

In der schweizerischen Lehre schlägt VITO ROBERTO vor, zur Begründung des inneren Zusammenhangs anhand der Grundlage für die Zuwendungen zu differenzieren. Anknüpfungspunkt für die Bejahung des inneren Zusammenhangs wäre demnach der Zusammenhang zwischen der Person des Beauftragten und dem erlangten Vorteil. Nur solche Vorteile, die der Auftraggeber auch

⁷⁶ Bejaht man bei Kryptowährungen wie BTC und BCC die Sachqualifikation im Sinne von Art. 641 Abs. 1 ZGB, dann könnte es sich bei den BCC um solche natürlichen Früchte der BTC-Blockchain i.S.v. Art. 643 ZGB handeln.

⁷⁷ Vgl. jeweils m.w.H. ROBERTO (FN 49), 25 ff. sowie WAYGOOD-WEINER (FN 4), 90 ff.

⁷⁸ Vgl. BGE 137 III 393 E. 5.3.1 und E 5.3.3.

erlangt hätte, wenn er das Geschäft selbst besorgt hätte, wären demnach abzuliefern.⁷⁹

Für die vergleichbare Thematik im deutschen Recht vertritt CHRISTIANE WENDEHORST, es sei zunächst von einer umfassenden Pflicht zur Ablieferung aller *adäquat kausal* durch die Auftragsausführung erlangten Vorteile auszugehen. In einem zweiten Schritt sollen solche Vorteile ausgeschlossen werden, die der Auftraggeber «*schon naturgemäss nicht hätte erzielen können*», da sie «*ein objektiv eigenes Geschäft*» des Beauftragten darstellen.⁸⁰

Ebenfalls vertreten wird die Dienstleistungstheorie, nach welcher Vorteile *nicht* herausgegeben werden müssen, wenn sie eine spezifische, eigenständige Dienstleistung des Beauftragten darstellen, Äquivalenz zwischen Entschädigung und Leistung besteht und keine negativen Auswirkungen eines Interessenkonflikts auf den Kunden zu befürchten sind.⁸¹

Nachfolgend gehen wir zuerst auf die natürliche und adäquate Kausalität ein und untersuchen sodann den typisierten Vertragszweck der einzelnen Fallgruppen, um zu eruieren, ob die BCC dem Beauftragten infolge oder lediglich bei Gelegenheit des Auftragsverhältnisses zugekommen sind. Dabei wenden wir auch die von der Lehre entwickelten Abgrenzungskriterien an.

4.2 Natürliche und adäquate Kausalität zwischen Auftragsausführung und Vermögenswert

Unzweifelhaft ist, dass jeweils ein natürlich kausaler Zusammenhang besteht zwischen den neuen BCC und dem Halten und Verwalten von BTC-Private Keys bzw. den vom Beauftragten zu beschaffenden BTC bzw. den zur Deckung von Kundenkonten gehaltenen BTC. Denkt man den jeweiligen Auftrag weg, so würden mangels Verfügungsmacht über BTC zum Zeitpunkt der harten Gabelung auch keine BCC im Verfügungsbereich des Beauftragten anfallen.

Die jeweilige Ausführung des Auftrags zum Zeitpunkt der harten Gabelung ist zudem für alle drei Fallgruppen auch adäquat kausal für die Verfügungsmacht über die neu geschaffenen BCC.⁸² Denn die Ursache für die Entstehung des neu geschaffenen Vermögenswerts liegt in der *emergenten* Entscheidung einer Teilmenge der Gemeinschaft der BTC-Nutzer, das BTC-Protokoll zu adaptieren und die neue BCC-Protokollversion auf einer eigenen Blockchain-Gabelung fortzuschreiben (siehe oben II.2.3). Nach dem gewöhnlichen Lauf der Dinge und nach der allgemeinen Lebenserfahrung ist die

Auftragsausführung in allen drei Fallgruppen geeignet, einem Beauftragten, der zum Zeitpunkt einer solchen Entscheidung für den Auftraggeber BTC Private Keys kontrolliert, die Verfügungsmacht über die neuen BCC zu verschaffen. Dem Beauftragten fällt dadurch ein Vermögenswert zu und er wird über die allenfalls vereinbarte Entschädigung hinaus bereichert, weil er zum richtigen Zeitpunkt die BTC Private Keys kontrolliert.

Der natürliche und adäquate Kausalzusammenhang alleine genügt jedoch noch nicht, um einen inneren Zusammenhang zu bejahen, sondern es muss zudem der jeweilige Zweck der den Fallgruppen zugrundeliegenden Auftragsverhältnisse betrachtet werden, um zu entscheiden, ob die BCC infolge oder bloss bei Gelegenheit des Auftrags angefallen sind.

4.3 Zweck des Vertrages bei Fremdverwaltung von Bitcoin Private Keys

Bei der ersten Fallgruppe steht als Zweck regelmässig die sichere Aufbewahrung der BTC Private Keys, allenfalls verbunden mit der Verbesserung von deren Nutzbarkeit, im Vordergrund. Folglich hat der Auftraggeber eine berechtigte Erwartung, dass allfällige, bei der Aufbewahrung ohne Zutun des Beauftragten anfallende, Vermögenswerte ebenfalls für ihn sicher aufbewahrt und auf Verlangen herausgegeben werden.

Nichts anderes ergibt sich auch bei Anwendung der skizzierten Theorien aus der Lehre, denn hätte der Auftraggeber die Verwaltung selbst besorgt, so wären ihm die BCC ohne Weiteres zugekommen. Es handelt sich somit klarerweise nicht um einen Vorteil, den nur der Beauftragte hätte erlangen können, noch ist der Erhalt der BCC das Ergebnis einer spezifischen, eigenständigen Leistung des Beauftragten.

Wenn BTC Private Keys durch einen Beauftragten verwaltet werden, besteht somit die auftragsrechtliche Pflicht, bei einer harten Gabelung neu erlangte Tokens an den Auftraggeber abzuliefern. Sofern die BTC Private Keys vom Beauftragten noch nicht zur Erlangung der neu geschaffenen BCC benutzt wurden, wird der Beauftragte dieser Ablieferungspflicht mit der blossen Rückgabe derselben erfüllen können. Der Auftraggeber kann dann selbst über beide virtuellen Währungen verfügen. Diejenigen Beauftragten, die nur gemeinsam mit dem Kunden über die BTC und BCC verfügen können, trifft keine eigentliche Ablieferungspflicht. Sie müssen aber am Erlangen des Zugriffs auf die BCC durch die Benutzung oder das Zurverfügungstellen ihres Multi-Sig Private Keys mitwirken.

4.4 Zweck des Vertrages bei Auftrag zur Beschaffung von Bitcoin

Bei der zweiten Fallgruppe lässt sich der Vertragszweck umschreiben als Auftrag zur Beschaffung der Verfü-

⁷⁹ ROBERTO (FN 49), 36 f.

⁸⁰ CHRISTIANE WENDEHORST, Anspruch und Ausgleich, Theorie einer Vorteils- und Nachteilsausgleichung im Schuldrecht, Habil. München 1998, Tübingen 1999, 429.

⁸¹ Vgl. ausführlich dazu WAYGOOD-WEINER (FN 4), 105.

⁸² Vgl. ausführlich zum Begriff der adäquaten Kausalität m.w.H. BGE 123 III 110 E. 2.

gungsmacht über BTC auf Rechnung des Auftraggebers. Erfüllt wird der Vertrag entweder dadurch, dass zugunsten einer Adresse des Auftraggebers eine Transaktion ausgelöst wird, oder indem die entsprechenden Private Keys übergeben werden.

Wie bereits dargelegt, ist die Verfügungsmacht über die BCC die natürlich und adäquat kausale Folge der Verfügungsmacht über die BTC. Die neu geschaffenen BCC sind dem Beauftragten zugekommen, während er die BTC auf Rechnung und auf Risiko des Kunden gehalten hat, d.h. während er Verfügungsmacht über die dem Beauftragten zustehenden BTC hatte. Das Beschaffen, kurzzeitige Halten und Weiterleiten der BTC an den Auftraggeber ist hier die vertragliche Hauptleistungspflicht des Beauftragten. Der Auftraggeber trägt, analog zum Kommissionsgeschäft nach Art. 425 OR, sowohl das Erfüllungs-, als auch das Risiko für Schäden und den Untergang der BTC.⁸³ Da es sich bei der harten Gabelung um die Verwirklichung eines vom Beauftragten nicht beeinflussten Risikos handelt, ist es folgerichtig, von einem inneren Zusammenhang auszugehen, weshalb die Verfügungsmacht über die BCC ebenfalls dem Auftraggeber zukommt.⁸⁴ Die neu geschaffenen BCC kommen dem Beauftragten zudem auch nicht aufgrund von in seiner Person liegenden Gründen zu. Auch in diesem Fall ist somit eine Ablieferungspflicht zu bejahen.

In einer solchen Konstellation kann sich zudem, unabhängig von der Ablieferungspflicht, die Frage stellen, ob dem Beauftragten eine Vertragsverletzung anzulasten ist, wenn er die BTC bewusst erst *nach* einem Hardfork ohne die damit verknüpften BCC erworben hat, weil der BTC-Preis durch den Hardfork gefallen ist. Dies ist in erster Linie eine Frage der Auslegung des Vertrages im Einzelfall, insbesondere mit Bezug auf den vereinbarten Zeitpunkt der Beschaffungshandlung durch den Beauftragten. Es ist anzuraten, hierzu eine eindeutige Regelung in entsprechende Verträge aufzunehmen.

4.5 Zweck des Vertrages bei Kontoführung lautend auf Bitcoin

Die dritte Fallgruppe bietet das komplexeste Anschauungsmaterial für die Frage der Ablieferungspflicht. Der Zweck des Vertrages lässt sich folgendermassen umschreiben: Dem Auftraggeber wird die Möglichkeit eingeräumt, beim Beauftragten ein auf BTC lautendes Konto zu führen und dabei jederzeit vom Beauftragten zu verlangen, dass dieser ihm innert einer gewissen, wohl meist vertraglich vereinbarten, Frist die Verfügungsmacht über eine dem Kontostand entsprechende Anzahl BTC verschafft. Der Auftraggeber hat mit anderen Wor-

ten nur auf Verlangen einen vertraglichen Anspruch auf Erhalt von BTC vom Beauftragten.

Bei dieser Ausgangslage ist entscheidend, ob der kontoführende Beauftragte die BTC-Forderungen seiner Kunden durch selbst und auf eigene Rechnung gehaltene BTC deckt. Eine entsprechende Pflicht des Beauftragten müsste u.E. vertraglich vereinbart sein. Ansonsten dürfte er frei sein, das Risiko einzugehen, sich erst auf Verlangen des Auftraggebers zum Marktpreis mit BTC einzudecken.⁸⁵ Ist eine vollständige BTC-Deckung der durch den Beauftragten geführten Konten gegeben, so kommen dem Beauftragten durch die harte Gabelung eine den BTC-Ansprüchen seiner Auftraggeber entsprechende Anzahl BCC zu. Hält der Beauftragte die BTC in der Absicht, die Deckung der von ihm geführten BTC-Konten sicherzustellen, so ist der innere Zusammenhang zum Kontoführungsauftrag zu bejahen, denn der Beauftragte hält die BTC gerade zur Erfüllung des Vertragszweckes. Folglich besteht eine Ablieferungspflicht für die BCC. Zudem fallen die BCC auch hier nicht infolge einer spezifischen, eigenständigen Leistung des Beauftragten bzw. infolge von in seiner Person liegenden Gründen an. Hält der Beauftragte zum Zweck der Eigeninvestition und nicht zur Deckung der Kundenforderungen BTC und fallen durch eine harte Gabelung BCC an, so ist eine Ablieferungspflicht hingegen abzulehnen, da der innere Zusammenhang fehlt.

Ist vom Beauftragten nur eine teilweise BTC-Deckung hergestellt, so stellt sich die Frage, ob die Ablieferungspflicht ebenfalls nur anteilmässig besteht. Klar ist, dass dem Beauftragten nur dann die volle Anzahl BCC tatsächlich *zugekommen* sind, wenn er zum Zeitpunkt der harten Gabelung eine Anzahl BTC hält, die den ausstehenden Forderungen sämtlicher BTC-Konten seiner Auftraggeber entspricht. Hat er hingegen zu diesem Zeitpunkt Verfügungsmacht über weniger BTC, als Forderungen von Kunden bestehen, so kommen ihm auch entsprechend weniger BCC zu. Hält der Beauftragte zumindest einen Teil der BTC gedeckt, so ist eine anteilmässige Ablieferungspflicht mit der gleichen Begründung wie oben zu bejahen. Sie ist jedoch richtigerweise auf den jeweiligen Deckungsgrad zu beschränken, denn der Auftraggeber soll aus der Ablieferungspflicht auch nicht mehr leisten müssen, als ihm selbst zugekommen ist. Eine *überschiessende* Ablieferungspflicht, nach welcher der Dienstleister mehr BCC abliefern müsste, als ihm selbst zugekommen sind, ist abzulehnen. Vorbehalten bleiben Fälle, in denen der Beauftragte durch die Teildeckung gegen eine andere vertragliche Pflicht verstösst.

⁸³ Vgl. BSK OR I-LENZ/VON PLANTA, Art. 425 N 4.

⁸⁴ Vgl. die vergleichbare Argumentation bei einer Verkaufskommission in BGE 138 III 137 E 5.3.2 ff.

⁸⁵ Was angesichts der Volatilität der virtuellen Währungen als riskantes Unterfangen erscheint, vgl. <https://www.buybitcoinworldwide.com/de/volatilitatsindex/> (Abruf 27.10.2017).

Verneint man eine überschüssige Ablieferungspflicht, stellt sich die Frage, ob den kontoführenden Beauftragten, ohne ausdrückliche vertragliche Abrede, eine Pflicht trifft, rechtzeitig vor einem BTC-Hardfork eine vollständige BTC-Deckung herzustellen. Klar erscheint, dass ein solche Volldeckung immer im besten wirtschaftlichen Interesse des Kunden liegt, da er dann, unabhängig von der Kursentwicklung der beiden Kryptowährungen, sowohl über die bisherigen als auch über die neuen Währungseinheiten verfügt. Eine solche Pflicht zur Herstellung der Volldeckung ergibt sich klarerweise nicht aus der auftragsrechtlichen Ablieferungspflicht. Entscheidend ist folglich der tatsächliche übereinstimmende Wille der Parteien im Einzelfall, oder, sofern nicht eruierbar, der mutmassliche, objektivierte Parteiwille.⁸⁶

Ein Anhaltspunkt kann dabei die Berufsausübung sein.⁸⁷ Eine solche ist im schnelllebigen Bereich der Kryptowährungsdienstleistungen erst in Entstehung begriffen und es ist u.E. verfrüht, Schlussfolgerungen zur Üblichkeit einer Volldeckung zu ziehen. Eine flächendeckende Volldeckungspflicht scheint jedenfalls in der Konsequenz zu weitgehend zu sein, wenn man bedenkt, dass nicht jede harte Gabelung weit im Voraus absehbar und planbar ist, die Überlebenswahrscheinlichkeit von neu entstehenden Kryptowährungen oft in den ersten Wochen und Monaten unklar sein kann. Zudem können die sich aus einer solchen Volldeckungspflicht ergebenden finanziellen Belastungen für den Beauftragten erheblich sein, wenn sehr kurzfristig eine grosse Zahl an Kryptowährungseinheiten in zuweilen illiquiden Märkten beschafft werden muss. Insbesondere mit der Entstehung neuer Dienstleistungen, wie z.B. der Vergabe von Krediten lautend auf BTC, erhöht sich die Wahrscheinlichkeit, dass nicht mehr sämtliche BTC-Guthaben durch eine entsprechende Menge BTC gedeckt sein werden. Auch hier ist folglich dringend anzuraten, die technische und ökonomische Realität der jeweiligen Kryptowährungsdienstleistung vertraglich präzise abzubilden und den Auftraggeber insbesondere auf allfällige Deckungseinschränkungen hinzuweisen. Zudem sollte der Auftraggeber darauf bestehen, dass Volldeckung besteht, ansonsten er im Falle einer harten Gabelung das Risiko eingeht, dass keine, oder nur eine im Umfang reduzierte, Ablieferungspflicht besteht.

VI. Ergebnis

1. Kryptowährungen als technische Herausforderung des Rechts

Noch sind offene, pseudonyme und intermediärlose Kryptowährungen wie BTC auf der Grundlage offener Blockchainsysteme ein sehr junges Phänomen. Die zum Teil sehr unterschiedlichen Lehrmeinungen zur rechtlichen und ökonomischen Verortung zeigen jedoch, dass es sich dabei um eine erhebliche Herausforderung – und punktuellen Überforderung – des Rechts handelt.⁸⁸ Eine der vielen Eigenheiten der Blockchain-Technologie ist die mögliche Vervielfältigung des auf dem Blockchainsystem repräsentierten digitalen Vermögenswerts durch eine harte Gabelung als Ergebnis eines dezentralen Konsensprozesses der Nutzergemeinschaft.

Zur angemessenen rechtlichen Auseinandersetzung mit dem Thema ist ein grundlegendes Verständnis von deren Funktionsweise unerlässlich, wobei dafür nicht zwingend erforderlich ist, das jeweilige Blockchainsystem auf der Ebene des Programmcodes zu durchdringen. Dieser Aufsatz versteht sich als Beitrag zur Verbesserung des so verstandenen funktionalen Verständnisses, indem er einige grundlegenden Eigenschaften der BTC-Blockchain umreist, einige Grundsätze zu Private Keys beschreibt und schliesslich drei verschiedene Erscheinungsformen von Gabelungen beim BTC-Blockchainsystem erläutert.

2. Grenzen der bundesgerichtlichen Rechtsprechung zur Ablieferungspflicht

Die bundesgerichtliche Rechtsprechung zum Thema der Ablieferungspflicht behandelt mehrheitlich Konstellationen, in denen Beauftragten im Rahmen ihrer Tätigkeit von Dritten vermögenswerte Vorteile zukommen und dadurch mögliche Interessenkonflikte geschaffen werden. Die hier untersuchte Konstellation der harten BTC-Gabelung unterscheidet sich davon grundlegend, indem die Vermögensvorteile weder von Dritten kommen noch einen Interessenskonflikt beim Beauftragten verursachen können. Aus diesem Grund ist es erforderlich, den vom Bundesgericht zur Begründung der Ablieferungspflicht herangezogenen inneren Zusammenhang zwischen Auftragsverhältnis und erlangtem Vorteil näher zu untersuchen, um für die harte BTC-Gabelung zu aussagekräftigen Ergebnissen zu gelangen.

Die hierin vorgenommene Untersuchung hat für die drei umrissenen Fallgruppen gezeigt, dass für die durch die harte BTC-Gabelung anfallenden BCC der innere Zusammenhang, mit einigen Spezifitäten bei der dritten Fallgruppe, grundsätzlich zu bejahen ist. Die BCC un-

⁸⁶ BSK OR I-WIEGAND, Art. 18 N 76 ff.

⁸⁷ Vgl. BGE 132 III 460 E. 4.3.

⁸⁸ Vgl. GRAHAM-SIEGENTHALER/FURRER (FN 67), Rz. 9.

terliegen folglich in allen drei Fallgruppen als indirekt erlangte Vermögenswerte mit innerem Zusammenhang zum Auftrag grundsätzlich der Ablieferungspflicht.

Das bei Retrozessionen zuweilen vorgebrachte Argument, die anfallenden Vermögenswerte seien pauschal die angemessene Entschädigung für den Aufwand, der dem Beauftragten aus dem Auftragsverhältnis erwachsen sei, verfängt bei der harten Gabelung von BTC und BCC nicht. Wer sich als Beauftragter für die Verwaltung von BTC Private Keys anbietet, BTC beschafft oder Konten für Kunden lautend auf BTC führt, muss grundsätzlich mit Hardforks rechnen. Erwachsen dem Beauftragten tatsächliche, beweisbare Kosten aus dem *coin-split* zwischen BTC und BCC und enthält der Vertrag keine andere Regelung, so muss es dem Beauftragten allerdings zugestanden werden, solche konkret belegbaren Kosten auf den Auftraggeber zu überwälzen. Denn es darf nicht vergessen gehen, dass die Ablieferungspflicht das Gegenstück zur Schadloshaltung des Beauftragten durch den Auftraggeber ist. Bejaht man erstere für den BTC-Hardfork, kommt man nicht umhin, auch letztere zu bejahen.

Der Vollständigkeit halber muss noch erwähnt werden, dass dem Beauftragten im Falle einer harten Gabelung angemessene Zeit zugestanden werden muss, bis er die Übertragung der BCC vorgenommen bzw. den Zugriff auf die BCC ermöglicht haben muss. Was angemessen ist, hängt dabei vom Einzelfall und der technischen Komplexität der harten Gabelung ab. Für den BTC-Hardfork erscheint angesichts der langen Vorlaufzeit der harten Gabelung eine Zeitspanne von vier bis acht Wochen angemessen.

Schliesslich erlauben die hierin erläuterten Schlussfolgerungen zu den drei Fallgruppen auch eine Annäherung an den Gehalt des inneren Zusammenhangs bei Konstellationen ohne Interessenskonfliktpotential im Allgemeinen. Erstens dürfte zur Begründung des inneren Zusammenhangs entscheidend sein, ob der vom Beauftragten erlangte Vorteil als eine natürliche und adäquat kausale Folge der Auftragsausführung erscheint. Ist dies zu bejahen, müssen im Sinne einer negativen Abgrenzung diejenigen Fälle ausgeschieden werden, bei denen der erlangte Vorteil nicht vom Vertragszweck abgedeckt ist. Dies ist insbesondere dann der Fall, wenn der Vorteil das Ergebnis einer unabhängigen geschäftlichen Leistung des Beauftragten ist oder aufgrund von ausschliesslich in der Person des Beauftragten liegenden Gründen erlangt wurde. Ist der erlangte Vorteil vom Vertragszweck nicht abgedeckt, ist von einem Gelegenheitsvorteil auszugehen und eine Ablieferungspflicht zu verneinen.

3. Schluss

Auch wenn im Bereich der Kryptowährungen und anderen Blockchain-Tokens noch viele rechtliche Fragen zu klären sind, bietet das schweizerische Auftragsrecht

eine flexible Grundlage für verschiedene Dienstleistungen rund um Blockchainsysteme. Wie sich gezeigt hat, sind selbst bei ausserordentlichen Ereignissen wie dem BTC-Hardfork bei richtiger Auslegung sachgerechte Lösungen möglich. In der Praxis dürfte regelmässig vorfrageweise zu klären sein, ob überhaupt Schweizer Recht zur Anwendung kommt. Denn die entsprechenden Dienstleister haben, trotz der vielfältigen Aktivitäten in der Schweiz auf der Grundlage von Blockchain-Technologie, nicht selten Sitz im Ausland, woraus sich vielfältige und teils anspruchsvolle kollisionsrechtliche Fragen ergeben können.⁸⁹

Die hier präsentierten Ergebnisse zur Ablieferungspflicht für den BTC-/BCC-Hardfork sind wohl nicht unmittelbar anwendbar auf alle Arten harter Gabelungen eines Blockchainsystems. Denn harte Gabelungen sind, genauso wie Blockchainsysteme überhaupt, fast beliebig komplex und können sich erheblich unterscheiden. Die formulierten Grundsätze dürften jedoch immerhin überall dort anwendbar sein, wo ein Auftragsverhältnis vorliegt, der Beauftragte die faktische Kontrolle über Private Keys ausübt und aus einer harten Gabelung zwei neue, jeweils werthaltige Blockchains hervorgehen, auf denen mittels derselben Private Keys über Blockchain-Tokens verfügt werden kann.

Soweit öffentlich bekannt, haben die meisten in- und ausländischen Dienstleister beim BTC-Hardfork die neu geschaffenen BCC an ihre Kunden und Auftraggeber abgeliefert oder dies zumindest in Aussicht gestellt. Wallet Provider wie das Unternehmen Coinbase, die BCC ursprünglich nicht in ihr System implementieren wollten, mussten sich harscher Kritik stellen.⁹⁰ Coinbase hat nun angekündigt, auf eine Unterstützung von BCC ab Januar 2018 hinzuarbeiten, «assuming no additional risks emerge during that time».⁹¹ Einige haben sich auch auf den Standpunkt gestellt, ihre Lösung erlaube es den Auftraggebern, selbstständig, auf die BCC zuzugreifen. Ob diese Fälle der Ablieferung die Folge rechtlicher Einschätzungen der Dienstleister waren oder aber bloss Kulanz, wird sich in Zukunft weisen. Denn sicher ist, dass mit der zunehmenden Anzahl Kryptowährungen auch die Anzahl harter Gabelungen zunehmen wird. So diskutierten Teile der (verbliebenen) Nutzergemeinschaft bei

⁸⁹ So enthalten z.B. die AGB von kraken.com, eine der grösseren Börsen für virtuelle Währungen, die von Payward Inc. betrieben wird, eine Schiedsgerichtsklausel sowie eine Rechtswahl zugunsten von kalifornischem Recht, soweit nicht amerikanisches Bundesrecht anwendbar ist. Vgl. Kraken TOS, <https://www.kraken.com/legal/tos> (Abruf 27.10.2017).

⁹⁰ BECKY PETERSON, Tons of Coinbase users fled the platform after it rejected bitcoin cash — now the \$1 billion startup is in the center of a raging storm, <http://www.businessinsider.com/coinbase-investors-think-rejecting-bitcoin-cash-hard-fork-make-platform-stronger-2017-8> (Abruf 27.10.2017).

⁹¹ DAVID FARMER, Update on Bitcoin Cash, <https://blog.coinbase.com/update-on-bitcoin-cash-8a67a7e8dbdf> (Abruf 27.10.2017).

BTC erst kürzlich wieder über zwei neuerliche harte Gabelungen der virtuellen Währung.⁹²

Unabhängig von der Beurteilung der Ablieferungspflicht im Einzelfall ist als Erkenntnis aus diesem Aufsatz ebenso wichtig, dass sich aus dem Aufstieg der Kryptowährungen vielfältige neue und spannende rechtliche Fragestellungen ergeben. Diese Fragestellungen bedeuten auch, dass erheblicher rechtlicher Klärungs- und damit auch vertraglicher Regelungsbedarf besteht, sobald Dienstleistungen im Bereich der Kryptowährungen angeboten werden. So werden vertragliche Regelungen zum Umgang mit harten Gabelungen, Denial-of-Service-Angriffen oder ähnlichen Blockchain-Grossereignissen zukünftig zwingend erforderlich sein, will sich ein Dienstleister nicht erheblichen rechtlichen Risiken aussetzen. Über kurz oder lang werden sich folglich auch die Gerichte mit diesen Themen beschäftigen müssen.

⁹² <http://www.trustnodes.com/2017/09/27/bitcoin-industry-block-stream-developers-go-head-head-november-hardfork> (Abruf 27.10.2017); Bitcoin (BTC) Hardfork November 2017: Worauf muss ich bei dem Segwit2x-Update achten? <https://www.bitcoinmag.de/bitcoin/bitcoin-segwit2x-november-2017-hardfork/a-110> (Abruf 27.10.2017).