Information und Recht 85

Cryptocoin-Schulden

Haftung und Risikoverteilung bei der Verschaffung von Bitcoins und Alt-Coins

Bearbeitet von
Paulina Jo Pesch

1. Auflage 2017. Buch. XXVI, 228 S. Kartoniert
ISBN 978 3 406 71053 7
Format (B x L): 14,1 x 22,4 cm

Recht > Handelsrecht, Wirtschaftsrecht > Telekommunikationsrecht, Postrecht, IT-Recht > IT-Recht, Internetrecht, Informationsrecht

Zu Inhalts- und Sachverzeichnis

schnell und portofrei erhältlich bei

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

beck-shop.de
DIE FACHBUCHHANDLUNG

den Vertragsgegenstand zu verschaffen.[558] Da sowohl der Käufer oder Tauscher, als auch der Erbringer eines Entgelts zur vollständigen, dauerhaften Übertragung des Vertragsgegenstands (hier: Cryptocoins) verpflichtet sind, kann die Herbeiführung des Erfolgs nur angenommen werden, wenn der Gläubiger den Leistungsgegenstand endgültig behalten darf.[559]

Die Übertragung von Cryptocoins ist dann endgültig erfolgt, wenn ihr Empfänger die Kontrolle über die Cryptocoins ausüben und sie insbesondere weiter transferieren kann und der Leistende sich jeder Zugriffsmöglichkeit entäußert hat. In Cryptocoin-Netzwerken hat derjenige die faktische Kontrolle über Cryptocoins, dessen Adresse und damit öffentlichem Schlüssel die Cryptocoins zugeordnet sind und der in der Lage ist, mit seinem zugehörigen privaten Schlüssel eigene Transaktionen über die Cryptocoins abzusenden. Der Cryptocoin-Schuldner hat also die Situation herbeizuführen, dass die geschuldeten Cryptocoins durch die Blockchain einer Adresse des Gläubigers zugeordnet sind. Diese Lage kann grundsätzlich auf zwei Wegen herbeigeführt werden. Erstens kann der Schuldner eine Transaktion über den entsprechenden Cryptocoin-Betrag von einer eigenen Adresse an eine Adresse des Gläubigers veranlassen. Zweitens kann der Schuldner dem Gläubiger den Schlüssel zu einer Adresse verschaffen, der der geschuldete Betrag zugewiesen ist. Für die letztgenannte Übertragungsmöglichkeit spricht zwar, dass diese (1.) nicht als Transaktion aus der Blockchain ersichtlich und damit als datenschutzfreundlich[560] zu bewerten ist und (2.) nicht den Unsicherheiten der Verarbeitung der Transaktion im dezentralen Netzwerk unterliegt. In die Überlegungen ist jedoch mit einzubeziehen, dass der Gläubiger sich bei Verschaffung der Zugangsdaten nie sicher sein kann, dass der Schuldner nicht ebenfalls weiterhin im Besitz der privaten Schlüssel ist, sodass die endgültige Verschaffung der Cryptocoins an den Gläubiger an der fortbestehenden Zugriffsmöglichkeit des Schuldners scheitern würde. Der Gläubiger müsste daher eine Transaktion an eine ausschließlich von ihm kontrollierte Adresse veranlassen, um sich die geleisteten Cryptocoins praktisch zu sichern. Mangels entgegenstehender Vereinbarungen kann der Schuldner daher nicht berechtigterweise darauf vertrauen, dass er seine Schuld durch die Verschaffung der Zugangsdaten zu einer eigenen Adresse tilgen kann. Häufig wird die Verschaffung von Cryptocoins gerade durch das Anstoßen einer Transaktion sogar konkludent dadurch vereinbart sein,

[558] Für den Kauf *Saenger*, in: Schulze, BGB, Vor §§ 433 ff., Rn. 1.

[559] *BGH*, Urt. v. 27.6.2008 – V ZR 83/07, MDR 1996, 1112 = WM 2008, 1703, 1705 = ZIP 1996, 418 f.; *BGH*, Beschl. v. 23.1.1996, – XI ZR 75/95, MDR 1996, 1112 = NJW 1996, 1207 = WM 1996, 438 f. (beide zur Geldschuld).

[560] Vgl. *Lerch*, ZBB 2015, 190, 199.

beck-shop.de
DIE FACHBUCHHANDLUNG

dass schon bei der Anbahnung der Einigung über die Cryptocoin-Verschaffung eine Adresse des Gläubigers angezeigt oder genannt oder Angaben zum Ablauf der Cryptocoin-„Bezahlung" gemacht worden sind.

Die Erfüllung von Cryptocoin-Schulden erfordert daher im Normalfall die Vornahme einer Transaktion: Konkret hat der Schuldner eine mit seinem passenden privaten Schlüssel signierte Transaktion über den geschuldeten Betrag von Cryptocoins – von einer Adresse, der mindestens dieser Betrag zugeordnet ist, an die Adresse des Gläubigers – an das Netzwerk zu kommunizieren. Die Bestätigung der Transaktion durch Aufnahme in einen Block der längsten Kette der Blockchain erfolgt dann ohne sein weiteres Zutun. Es besteht zwar auch die Möglichkeit, dass der Schuldner die Transaktion nicht selbst an das Netzwerk kommuniziert, sondern sie an den Gläubiger übermittelt, der daraufhin das Absenden der Transaktion an das Netzwerk selbst übernimmt. Ohne Anhaltspunkte dafür, dass die Parteien dies vereinbart haben, kann aber nicht angenommen werden, dass der Schuldner die Transaktion selbst nicht anzustoßen hat. Aus dem Leistungsversprechen folgt, dass der Schuldner den Leistungserfolg herbeizuführen hat. Das Bewirken des Leistungserfolgs fällt in seinen Risikobereich.[561] Aus der Möglichkeit der Mitwirkung des Gläubigers folgt aber nicht, dass dieser generell darauf verwiesen werden kann, an der Herbeiführung des Leistungserfolgs, die zum Pflichtenkreis des Schuldners zählt, mitzuwirken.

Dies ließe sich nur auf eine Pflicht des Gläubigers zur Mitwirkung stützen. Eine solche Mitwirkungspflicht zur Erleichterung der Leistungserbringung für den Schuldner kann unter Berücksichtigung der beiderseitigen Interessen zwar anzunehmen sein, etwa wenn dem Schuldner ansonsten Schaden droht oder ihm das Bewirken des Leistungserfolgs selbst nicht möglich ist, wenn dem Gläubiger hierdurch keine Nachteile und kein erheblicher Aufwand entstehen.[562] Wenn Schuldner und Gläubiger gleichermaßen zum Absenden der Transaktion in der Lage sind, gebieten die Interessen des Schuldners es jedenfalls nicht, dass der Gläubiger die Transaktion selbst absendet. Wenn der Schuldner aber zur Absendung der Transaktion an den Gläubiger in der Lage ist, ist er in der Regel auch zur Absendung an das Netzwerk in der Lage. Es kann aber zwischen den Parteien vereinbart werden, dass der Schuldner die Transaktion an den Gläubiger zu übermitteln hat und

[561] *Bachmann*, in: MüKo BGB, § 241, Rn. 80; *Olzen*, in: Staudinger, § 241, Rn. 211; *Sutschet*, in: BeckOK BGB, § 241, Rn. 65.

[562] *Bachmann*, in: MüKo BGB, § 241, Rn. 80; Olzen, in: Staudinger, § 241, Rn. 212; *Sutschet*, in: BeckOK BGB, § 241, Rn. 65.

beck-shop.de
DIE FACHBUCHHANDLUNG

dieser ihre Bestätigung selbst veranlasst. Dies kann sich aus den Umständen des Vertragsschlusses ergeben. Insbesondere bei der Nutzung mobiler Cryptocoin-„Zahlungsdienste" ist es nicht unüblich, dass der Schuldner die Transaktion an den Gläubiger übermittelt, sodass er bei Präsenzgeschäften nicht auf eine Internetverbindung angewiesen ist.[563] Auch kann sich der Gläubiger nach Vertragsschluss konkludent mit dieser Vorgehensweise einverstanden erklären, wenn der Schuldner die Transaktion daraufhin direkt an den Gläubiger übermittelt und dieser die Transaktion daraufhin selbst absendet. Abseits solcher Umstände gehört das Absenden der Transaktion an das Netzwerk aber zur vom Schuldner vorzunehmenden Leistungshandlung.

Aufgrund der Eigenheit von Cryptocoin-Netzwerken, dass Transaktionen durch weitere Bestätigungen iterativ abgesichert werden,[564] ist aber zweifelhaft, ab welchem genauen Zeitpunkt der Leistungserfolg eintritt und damit die Pflicht des Schuldners zur Verschaffung von Cryptocoins als erfüllt anzusehen ist. Das hängt davon ab, wie die Vereinbarung einer Cryptocoin-Verschaffungspflicht auszulegen ist.

Auch wenn der Empfänger von Cryptocoins ab Aufnahme einer ihn begünstigenden Transaktion in die Blockchain erst einmal gültige Transaktionen über die empfangenen Cryptocoins absenden kann, führt die iterative Absicherung von Cryptocoin-Transaktionen mit zunehmendem Bestätigungsgrad und insbesondere ihre anfängliche Angreifbarkeit[565] dazu, dass Cryptocoins ihrem Empfänger auch nach der Bestätigung der Transaktion wieder entzogen werden können. Bei Annahme der Erfüllung durch erstmalige Aufnahme in die Blockchain könnte der Gläubiger auch in solchen Fällen wegen der Rechtsfolge des § 362 Abs. 1 BGB die Primärleistung nicht mehr fordern, sondern wäre auf Schadensersatzansprüche verwiesen. Die endgültige Zuordnung der Cryptocoins zum Gläubiger träte aber tatsächlich erst infolge der erfolgten Aufnahme der Transaktion in einen alternativen, in der längsten Kette befindlichen Block ein. Mit der Aufnahme der Transaktion in die Blockchain ist noch keineswegs sichergestellt, dass die Cryptocoins der Adresse des Empfängers endgültig zugeordnet bleiben, dieser sie also endgültig behalten kann. Mit jeder weiteren Bestätigung der Transaktion durch Anhängen weiterer Blöcke steigt die für die Errechnung eines alternativen, längeren Asts nötige Rechenleistung exponentiell, sodass die Wahrscheinlichkeit, dass die Transaktion rückwirkend beseitigt wird, entsprechend sinkt.

---

[563] *Hajdarbegovic*, ‚Bitcoin Box' Can Process Payments With No Web Connection, abrufbar unter http://www.coindesk.com/bitcoin-box-can-process-payments-web-connection/ (letzter Abruf: 2.1.2017).

[564] Zum technischen Hintergrund Kap. 2, A. V., insb. 1.

[565] Zu den Angriffsszenarien Kap. 2, A. V.

beck-shop.de
DIE FACHBUCHHANDLUNG

Vor diesem Hintergrund stellt sich die Frage, ab welchem Zeitpunkt davon ausgegangen werden kann, dass der Gläubiger die empfangenen Cryptocoins endgültig behalten kann. Es genügt in Abhängigkeit von der Gesamtrechenleistung eines Cryptocoin-Netzwerks einerseits für die sichere Bestätigung der Transaktion nicht unbedingt, dass diese im letzten Block der Blockchain enthalten ist. Andererseits darf man im Interesse des Leistenden die Zahl der nötigen Folgeblöcke nicht überstrapazieren. Vor diesem Hintergrund bereitet das Festsetzen eines Zeitpunkts, ab dem eine Transaktion als ausreichend bestätigt und damit die Schuld als erfüllt betrachtet werden kann, einige Schwierigkeiten.

Denkbar ist die Bestimmung des Erfüllungszeitpunkts durch eine wirksame Vereinbarung der Parteien, eine Transaktion welchen Bestätigungsgrads der Schuldner schuldet.[566] Gerade weil Cryptocoin-Transaktionen durch jede weitere Bestätigung iterativ abgesichert werden, finden sich dementsprechend in den Nutzungsbestimmungen einiger Bitcoin-Intermediäre explizite Regelungen oder sonstige Aussagen zur Anzahl der notwendigen Bestätigungen.[567]

a) Erfüllungszeitpunkt mangels Parteivereinbarung

Gerade bei Verträgen, an denen kein Intermediär beteiligt ist, wird es aber an ein einer ausdrücklichen Parteivereinbarung häufig fehlen. Zu fragen ist, was der genaue Inhalt des Versprechens, Cryptocoins zu verschaffen, ist und was der Gläubiger demnach zu erhalten erwarten darf, wann also eine Transaktion objektiv als ausreichend abgesichert anzusehen ist. Einerseits darf die Zahl der für den Eintritt des Leistungserfolgs nötigen Bestätigungen im Interesse des Schuldners nicht übermäßig hoch sein. Denn der Gläubiger kann die Einrede des § 320 BGB erheben und damit seine Leistung verweigern, bis der Leistungserfolg eingetreten ist.[568] Je höher man also die Zahl der nötigen Bestätigungen ansetzt, desto länger ist der Schuldner dem Leistungsverweigerungsrecht des Gläubigers ausgesetzt. Andererseits kann die Erfüllung, die spätestens zum Gefahrübergang führt, nicht schon dann zu Lasten

[566] Zur Wirksamkeit von Erfüllungszeitpunkt-Vereinbarungen Kap. 6, C. I.

[567] Sechsfach bestätigte Bitcoin-Transaktionen fordern Klausel 8.1 der BitPay-AGB, abrufbar unter https://bitpay.com/about/terms#fees-and-settlement (letzter Abruf: 2.1.2017); Punkt 3 der BitKonan-FAQ, abrufbar unter https://bitkonan.com/info (letzter Abruf: 2.1.2017); Klausel 3.3.1. der BitCasino-AGB, abrufbar unter https://bitcasino.io/terms (letzter Abruf: 2.1.2017).

[568] *BGH*, Urt. v. 19.5.2006 – V ZR 40/05, NJW 2006, 2773, 2775 = WM 2006, 1913, 1915; *Emmerich*, in: MüKo BGB, § 320, Rn. 36b; *Westermann*, in: Erman BGB, § 320, Rn. 18.

beck-shop.de
DIE FACHBUCHHANDLUNG

des Gläubigers angenommen werden, wenn dieser noch der ernsthaften Gefahr des Verlusts der Cryptocoins ausgesetzt ist.

In der Praxis hat sich insbesondere bei Bitcoins eine bestimmte Handhabung des Problems durchgesetzt, die für die Frage nach dem Zeitpunkt der Erfüllung ergiebig sein könnte. Das Bitcoin-Wiki führt aus, zum Schutz gegen Double-Spending solle eine Transaktion nicht als bestätigt angesehen werden, bevor eine gewisse Anzahl („a certain number of blocks") sie bestätigt.[569] Die Referenzimplementierung zeigt eine Transaktion nach sechs Bestätigungen, das heißt der ersten Bestätigung durch Aufnahme in die Blockchain plus fünf Folgeblöcken, als vollständig bestätigt an.[570] Dementsprechend findet sich in der Wikipedia die Aussage, die Bestätigung einer Transaktion im Bitcoin-Netzwerk gelte „nach sechs aufeinanderfolgenden Bestätigungen als hinreichend verbindlich bestätigt".[571] Auch die angeführten Nutzungsbestimmungen von Intermediären bestimmen, dass eine Transaktion bei sechsfacher Bestätigung als erfolgt anzusehen ist.[572] Die Anzahl von sechs Blöcken ist technisch nicht zwingend, sondern beruht auf einer Analyse der Wahrscheinlichkeit eines erfolgreichen Angriffs durch einen Angreifer, der 10 % der Gesamtrechenleistung des Bitcoin-Netzwerks aufbringt.[573] Tatsächlich ist schon bei wenigeren Bestätigungen sehr unwahrscheinlich, dass eine Transaktion noch aus der längsten Kette der Blockchain verdrängt wird.

In der Praxis, etwa von Händlern, die entscheiden, wann sie Waren verschicken, die mit Bitcoins „bezahlt" werden, wird eine Transaktion aufgrund einer Risikoabwägung als bereits ausreichend oder noch nicht hinreichend bestätigt betrachtet. Dementsprechend werden die Anforderungen an die Bestätigung häufig in Beziehung zum Transaktionsumfang gesetzt.[574] Die Beantwortung der abstrakten rechtlichen Frage nach dem Bewirken des Leistungserfolgs bei Bitcoin-Leistungen muss allerdings den Wert der Leistung außer Betracht lassen. Ansonsten wäre der Zeitpunkt der Leistung eines bestimmten Betrags von Bitcoins von deren Wert abhängig. Während es in der Praxis darum geht, das Risiko eines Leistungsausfalls zu beurteilen und die eigene Leistung über eine auf dieser Grundlage vernünftige Zeitspanne zurückzubehalten, geht es bei der Untersuchung des Erfüllungszeitpunkts darum, zu bestimmen,

[569] Bitcoin-Wiki, Confirmation, abrufbar unter https://en.bitcoin.it/wiki/Confirmation (letzter Abruf: 2.1.2017).
[570] Bitcoin-Wiki, Confirmation, abrufbar unter https://en.bitcoin.it/wiki/Confirmation (letzter Abruf: 2.1.2017).
[571] Http://de.wikipedia.org/wiki/Bitcoin (letzter Abruf: 2.1.2017).
[572] Fn. 567.
[573] *Rosenfeld*, S. 7.
[574] Https://bitcoin.org/de/glossar#bestaetigung (letzter Abruf: 2.1.2017).

beck-shop.de
DIE FACHBUCHHANDLUNG

ab wann Cryptocoins endgültig von einer an die andere Person als übertragen anzusehen sind.

Trotzdem liegt den Überlegungen der Marktteilnehmer eine rechtlich relevante Erwägung zugrunde. Ihrem Verhalten entspräche es, die Obergrenze der immer wieder angeführten ein bis sechs Blöcke, also das Hinzufügen des fünften Blocks, der auf den die Transaktion enthaltenden Block folgt, als Erfüllungszeitpunkt anzusetzen. Wenn sich die Verkehrsteilnehmer offenbar vorbehalten, im äußersten Fall bis zu diesem Zeitpunkt zu warten, bevor sie eine Transaktion als sicher bestätigt betrachten, handelt es sich hier um den Zeitpunkt, an dem nach der Verkehrsauffassung kein Recht zur Leistungsverweigerung aus § 320 Abs. 1 Satz 1 BGB – das freilich auch vorher nicht geltend gemacht werden muss – mehr besteht. Wer ohne Zusatz erklärt, Bitcoins verschaffen zu wollen, dessen Gegenüber darf erwarten, eine sechsfach bestätigte Transaktion über die Cryptocoins an die eigene, genannte Adresse zu erhalten. Denn im Bitcoin-Verkehr – sowohl bei den an der dezentralen Konsensbildung beteiligten Minern als auch unter den sonstigen Nutzern – wird davon ausgegangen, man dürfe als Gläubiger einer Bitcoin-Transaktion die eigene Leistung bis zu diesem Zeitpunkt zurückhalten. Zwar ist unabhängig vom Erfüllungszeitpunkt der Bitcoin-Gläubiger gemäß § 271 Abs. 1 BGB sofort zu der von ihm zu erbringenden Leistung – präziser: der Vornahme der Leistungshandlung[575] – verpflichtet. Aber ihm stünde bis zum Zeitpunkt der Erfüllung der ihm gebührenden Leistung die Einrede aus § 320 BGB zu. Die Annahme der erfüllungsgeeigneten Bestätigung ab sechs Blöcken würde den Schuldner auch angesichts der üblichen Bestätigungsdauer nicht nennenswert belasten. Zwar wird die Transaktion bei insgesamt hohem Transaktionsaufkommen nicht unbedingt in die ersten nach ihrem Absenden gefundenen Blöcke aufgenommen werden, legt man jedoch die Aufnahme in den drittnächsten Block zugrunde,[576] ergibt sich eine sechsfache Bestätigung der Transaktion nach bereits rund anderthalb Stunden.

Die praktische Handhabung des Bestätigungserfordernisses bei Bitcoin-Transaktionen lässt sich für die abstrakte rechtliche Bestimmung des Erfüllungszeitpunkts bei Cryptocoin-Verschaffungspflichten fruchtbar machen. Fordert die Rechtsprechung für ein Eintreten des Leistungserfolgs bei Verschaffung eines Gegenstandes ein endgültiges Behaltenkönnen und haben die Parteien nicht vereinbart, welcher Grad der

[575] *Bittner*, in: Staudinger, § 271, Rn. 1; *Krüger*, in: MüKo BGB, § 271, Rn. 1.

[576] Die durchschnittliche Bestätigungsdauer von Bitcoin-Transaktionen mit Transaktionsgebühr veranschaulicht Blockchain.info, Median Transaction Time (With Fee Only), abrufbar unter https://blockchain.info/charts/median-confirmation-time (letzter Abruf: 2.1.2017).

beck-shop.de
DIE FACHBUCHHANDLUNG

Bestätigung geschuldet ist, ist zu fragen, wann eine nicht näher bestimmte Transaktion objektiv hinreichend abgesichert ist. Die Handhabung bei Bitcoin kann dabei gewissermaßen als Vorbild für die Handhabung bei Alt-Coins gesehen werden: Wem die Verschaffung von Cryptocoins versprochen wird, der darf erwarten, eine Transaktion zu erhalten, die einen Grad an Bestätigung aufweist, bei dem der maßgebliche Verkehrskreis von einer ausreichenden Bestätigung ausgeht. Nicht einfach übertragen lässt sich der Wert von sechs Blöcken, da bei weniger genutzten Cryptocoins die Gesamtrechenleistung und damit die von einem Angreifer aufzubringende Rechenleistung wesentlich niedriger sind. Auch andere Faktoren, wie die Anpassung der Schwierigkeit bei Proof-of-Work-Systemen[577] und die durchschnittliche Zeitspanne bis zum Auffinden eines weiteren Blocks (je kleiner, desto leichter kurzfristig korrumpierbar), sind maßgeblich.

b) Handhabung der Entziehung der Cryptocoins nach Eintritt der Erfüllung aufgrund von Forks

Obwohl der hier für den Normalfall von Bitcoin-Schulden angesetzte Bestätigungsgrad sehr hoch liegt, besteht die – wenn auch unwahrscheinliche – Möglichkeit, dass eine Transaktion doch noch aus der längsten Kette der Blockchain verdrängt wird. Denn technisch ist eine Cryptocoin-Transaktion nie endgültig abgesichert. So hat es etwa bei Bitcoin im März 2013 dadurch, dass einige Miner eine andere Version des Bitcoin-Protokolls ausgeführt haben, einen Fork gegeben, der 32 verwaiste Blöcke zur Folge hatte.[578] Etwas Ähnliches ist im Juli 2015 passiert, als Miner, die zusammen 50 % der Rechenleistung des Netzwerks vereinigten, einen nach einer Aktualisierung des Protokolls ungültigen Block fehlerhaft als gültig erkannt und an diesen eine Kette von immerhin sechs Blöcken angehängt haben.[579] Und auch im extrem unwahrscheinlichen und nach dem Stand der Technik aufwändigen Fall einer Mehrheits-Attacke[580] durch Anhängen von mindestens sieben alternativen, die Gläubiger-begünstigende Transaktion nicht enthaltenden Blöcken könnte die Transaktion noch aus der längsten Kette der Blockchain beseitigt und so die Cryptocoins dem Gläubiger – zumindest zwischenzeitlich – entzogen werden. Infolge der Entziehung vom Gläubiger können folgende Situationen eintreten: Wenn die Transaktion in

[577] Zum Proof-of-Work bei Bitcoin Kap. 2, A. III. 3.

[578] Siehe die Diskussion unter http://bitcoin.stackexchange.com/questions/8334/what-block-numbers-hashes-were-discarded-by-the-march-2013-blockchain-fork (letzter Abruf: 2.1.2017). Zum technischen Hintergrund von Forks Kap. 2, A. III. 4.

[579] Some Miners are Generating Invalid Blocks, abrufbar unter https://bitcoin.org/en/alert/2015-07-04-spv-mining#list-of-forks (letzter Abruf: 2.1.2017).

[580] Zu Mehrheits-Attacken Kap. 2, A. V. 2. b).

beck-shop.de
DIE FACHBUCHHANDLUNG

einer alternativen, schlussendlich längeren Kette der Blockchain verarbeitet wird, sind die Cryptocoins letztlich – mit Verzögerung – dem Gläubiger zugeordnet. Wenn die Transaktion überhaupt nicht verarbeitet wird, können die Cryptocoins entweder dem Schuldner zugeordnet bleiben. Oder sie sind Gegenstand einer anderweitigen, mit dem privaten Schlüssel des Schuldners signierten Transaktion geworden und der Adresse eines Dritten oder einer anderen Adresse des Schuldners zugeordnet. Schließlich kann der Fork schon die Transaktion an den Schuldner betreffen, die ihrerseits entweder in der längsten Kette der Blockchain ebenfalls enthalten ist oder entfällt, sodass die Cryptocoins wieder dem ursprünglichen Sender zugeordnet sind.

Es stellt sich die Frage, was in den genannten Fällen gelten soll. Vorrangig wäre eine von den Parteien ausdrücklich getroffene Regelung, die jedoch insbesondere wegen der sehr niedrigen Wahrscheinlichkeit und dementsprechend geringen Häufigkeit von Forks, die zur Verwaisung langer Äste führen, in der Regel fehlen wird. Möglicherweise ist das Problem aber im Wege ergänzender Vertragsauslegung zu lösen; erst nachrangig[581] wäre über einen Anspruch auf Vertragsanpassung oder ein Rücktrittsrecht nach § 313 BGB zu nachzudenken.

Eine ergänzende Vertragsauslegung kommt nur zur Schließung planwidriger Regelungslücken in Betracht.[582] Wenn die Parteien keine Regelung dazu treffen, was bei Verwaisung des Asts der Blockchain, durch den Erfüllung eingetreten ist, gelten soll, würde nach allgemeinen Regeln der Gläubiger nach Erfüllung das Verlustrisiko tragen. Demnach würden die Eigenheiten des von beiden Parteien gewählten Cryptocoin-Systems dazu führen, dass im unwahrscheinlichen Falle eines Forks der Gläubiger die empfangenen Cryptocoins nicht endgültig behalten könnte, obwohl er seine Leistung an den Schuldner ordnungsgemäß erbracht hat. Dass das nicht den Anforderungen an die Vertragsgerechtigkeit genügt, ergibt sich nicht etwa aus einem allgemeinen Prinzip ausgleichender Gerechtigkeit,[583] sondern aus dem von den Parteien geschlossenen Austauschvertrag selbst. Die allgemeinen Regeln passen insofern nicht auf Cryptocoin-Transaktionen, als die Bestimmung des Erfüllungszeitpunkts wegen der iterativen Absicherung von Cryptocoin-Transaktionen auf einer Abwägung der Interessen von Schuldner und Gläubiger auf Grundlage der Verlustwahrscheinlichkeit unter Einbeziehung von Praktikabilitätserwägungen beruht. Vor diesem Hintergrund

[581] *Martens*, in: BeckOGK BGB, § 313, Rn. 171 ff.; *Pfeiffer*, in: jurisPK BGB, § 313, Rn. 47; *Westermann*, in: Erman BGB, § 313, Rn. 18; *Medicus*, BR, Rn. 154.

[582] *BGH*, Urt. v. 3.12.2014 – VIII ZR 370/13, NJW 2015, 1167, 1168; *BGH*, Urt. v. 21.9.1994 – XII ZR 77/93, NJW 1994, 3287; *Busche*, in: MüKo BGB, § 157, Rn. 38; *Wendtland*, in: BeckOK BGB, § 157, Rn. 40.

[583] Dazu Kap. 5, A.