www.jusletter.ch

Andreas Glarner / Stephan D. Meyer

Smart Contracts in Escrow-Verhältnissen

Die Entwicklung von Blockchain-Technologie und Smart-Contract-Applikationen macht es erstmals möglich, Softwaresysteme zu bauen, welche das dezentrale Halten und Transferieren von Vermögenswerten ohne Intermediäre erlauben. Die Autoren zeigen in diesem Beitrag anhand verschiedener Fallgruppen auf, wie Smart Contracts im Rahmen von Escrow-Verhältnissen genutzt werden können und welche rechtlichen Fragen sich dabei stellen.

Beitragsarten: Beiträge
Rechtsgebiete: Informatik und Recht

Zitiervorschlag: Andreas Glarner / Stephan D. Meyer, Smart Contracts in Escrow-Verhältnissen, in: Jusletter 4. Dezember 2017

ISSN 1424-7410, https://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

I. Einleitung

[Rz 1] Mit der Einführung der Bitcoin-Blockchain wurde erstmals ein Register geschaffen, auf welchem Dateneinträge durch kryptographische Verbindung von Datenblöcken konzeptionell unveränderbar und dezentral gespeichert werden können. Zahlungen können damit ohne Intermediär direkt zwischen den Nutzern (*peer-to-peer)* ausgeführt werden. Jede Transaktion wird unabänderlich auf der Blockchain vermerkt. Entwickler der Schweizer Blockchain-Stiftung «Ethereum» haben die Grundidee der Bitcoin-Blockchain weiterentwickelt und mit der sog. Ethereum-Blockchain ein Protokoll ausgearbeitet, das es erlaubt, auf einer Blockchain nicht nur Werte zu speichern, sondern auch komplexere dezentrale und automatisiert ablaufende Anwendungen, die sich auf diese Werte beziehen. Solche Applikationen sind unter dem Begriff «Smart Contracts» und «DApps» bekannt geworden.

[Rz 2] Die Idee von Smart Contracts ist keineswegs neu. Bereits im Jahr 1994 verfasste der amerikanische Computerwissenschafter und Kryptograph Nick Szabo einen Artikel über Verträge, bei denen ein Computerprotokoll die vordefinierten Bedingungen selbstständig ausführen könne. Das einfachste Beispiel für einen Smart Contract war laut Szabo ein Warenautomat, der beim Einwurf einer Geldmünze automatisiert ein Produkt ausgibt.[1] In einer komplexeren Ausgestaltung sollte ein Smart Contract autonom Zahlungsbedingungen, Pfandrechte und sogar die Vertragsdurchsetzung sicherstellen. Damit würden Abweichungen vom Vertrag verhindert und vertrauensbildende Intermediäre überflüssig gemacht.

[Rz 3] Die Idee von Szabo blieb über viele Jahre Vision und deren Umsetzung wurde kaum vorangetrieben. Erst durch die Entwicklung der Blockchain-Technologie wurde es möglich, Smart Contracts weiterzuentwickeln und umzusetzen. Ein blockchain-basiertes Computerprotokoll ist in der Lage, selbständig, d.h. ohne natürliche oder juristische Person im Hintergrund, digitale Vermögenswerte wie beispielsweise Ether Tokens zu halten und gemäss im Voraus programmierten und nicht einseitig abänderbaren Bedingungen wieder freizugeben.[2] Nebst vielen Aspekten ist das Revolutionäre an der neuen Technologie somit insbesondere, dass a) Software selber Vermögenswerte halten und b) nach vordefinierten Regeln und ohne Einflussmöglichkeit von Personen darüber verfügen kann.

[Rz 4] Wollten bis anhin zwei Parteien einen Vermögenswert für eine gewisse Zeit binden, mussten sie die Dienstleistung eines Dritten, zumeist eines Finanzintermediärs, in Anspruch nehmen. In der Praxis haben sich für viele Konstellationen sogenannte Escrow Agreements durchgesetzt. Die Möglichkeit, den Escrow-Agenten als Intermediär durch einen Smart Contract zu ersetzen, führt einerseits zu Effizienzgewinnen und reduzierten Kosten, andererseits aber auch zu diversen rechtlichen Fragestellungen. Auch in Zukunft lassen sich kaum alle Konstellationen rein smartcontract-basiert und ohne Intermediär umsetzen. So wird es gemäss Ansicht der Autoren weiterhin Konstellationen geben, in welchen es einen klassischen Escrow-Agenten benötigt, oder zumindest einen Daten Service Provider, der Daten in den Smart Contract einspeist, aufgrund derer der Smart Contract seine Funktionen ausführt.

[Rz 5] Erste Anwendungen von Smart Contracts zur Sicherung von Hauptgeschäften werden in der Praxis bereits genutzt, so wurde beispielsweise im September 2017 eine Immobilientransaktion in der Ukraine und Grossbritannien bereits komplett über einen Smart Contract mit Escrow-Funktion abgewickelt.[3] Nachdem alle Voraussetzungen erfüllt waren, löste der involvierte Notar die Transaktion über den Smart Contract aus.[4] Ebenfalls gibt es schon diverse Anwendungstests im Bereich Trade Finance, in welchen der Smart Contract die Funktion der Banken übernehmen soll.

---

1 Nick Szabo, Formalizing and Securing Relationships on Public Networks, 1997, https://archive.is/i65kY selection-17.1-17.59 (Alle Websites zuletzt besucht am 31. Oktober 2017).

2 Stephan D. Meyer/Benedikt Schuppli, «Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht, recht 03/2017, 207 f.

3 Peter Grant, An Entire Real Estate Deal Takes Place Online, Using Cryptocurrency Technology, Wall Street Journal Online vom 26. September 2017, https://www.wsj.com/articles/an-entire-real-estate-deal-takes-place-online-using-cryptocurrency-technology-1506462545.

4 Vgl. betreffend den genauen Ablauf bspw. Natalia Karayaneva, How A Smart Contract replaced An Escrow Company in a $60k deal, https://hackernoon.com/how-a-smart-contract-replaced-an-escrow-company-in-a-60k-deal-551ff7839044.

[Rz 6] Der vorliegende Beitrag gibt in einem *ersten Teil* (II.) einen Überblick über die Grundlagen von Escrow Agreements im Schweizer Recht und deren konkrete Anwendungsbereiche. In einem *zweiten Teil* (III.) werden in Kürze die Grundlagen der Blockchain-Technologie und Smart Contracts dargelegt. Ebenso werden drei Fallgruppen gebildet, wie Smart Contracts in Escrow-Konstellationen eingesetzt werden können. Im *dritten bis fünften Teil* (IV. – VI.) werden diese drei Fallgruppen vertieft erörtert. Abgeschlossen wird der Beitrag in einem *sechsten Teil* (VII.) mit einem Gesamtüberblick und im *siebten Teil* (Vlll.) mit einem Fazit.

II. Grundzüge von Escrow Agreements im schweizerischen Recht

1. Zweck und Arten von Escrow Agreements

[Rz 7] Der Begriff «escrow» leitet sich aus dem normannisch-französischen Wort «escrit» und dem lateinischen «scriptum» ab.[5] Entstanden ist das Rechtsinstitut im angelsächsischen Raum und wird dort wie folgt umschrieben: «a legal document or property delivered by a promisor to a third party to be held by the third party [...] until the occurrence of a condition, at which time the third party is to hand over the document or property to the promisee».[6] In der schweizerischen Literatur wird das Escrow Agreement definiert als «Hinterlegung einer beliebigen Sache – im Interesse zweier Parteien – bei einem Dritten, bis die zuvor festgelegten Bedingungen eintreten, und die Sache an eine der beiden Parteien zurückgegeben oder auch an einen Vierten weitergegeben werden kann».[7] Entscheidend ist der Entzug und Übertrag der Verfügungsgewalt an jener Sache.[8]

[Rz 8] Der Zweck eines Escrow Agreements besteht in der Sicherung der Forderung eines Gläubigers sowie des Vollzugs eines Hauptgeschäftes[9]. Daneben können noch andere Ziele mit dem Escrow Agreement verfolgt werden. So beinhaltet beispielsweise ein Source Code Escrow oftmals auch eine Prüfung des Codes durch den Escrow-Agenten.[10] Das Escrow Agreement ist als Innominatvertrag zu qualifizieren.[11] Abgegrenzt wird es anhand seines Sicherungszwecks insbesondere vom Hinterlegungsvertrag nach Art. 472 des Obligationenrechts (OR; SR 220), der eine Aufbewahrung im Interesse des Hinterlegers beabsichtigt. Im Folgenden wird der Begriff «Hinterlegung» daher ohne direkten Bezug zu Art. 472 ff. OR verwendet.

[Rz 9] Wird der Sicherungszweck nicht durch die Übergabe einer beweglichen Sache, sondern mittels Zession einer Forderung verfolgt, so ist nicht von einem Escrow Agreement, sondern von einer (Sicherungs-)Abtretung auszugehen.[12]

---

5 Stefan Eisenhut, Escrow-Verhältnisse, Das Escrow Agreement und ähnliche Sicherungsgeschäfte, in: Spiro et al., Basler Studien zur Rechtswissenschaft, Band 95, Basel 2009, 7.

6 Black's Law Dictionary, 8. Edition, 2004, escrow; so zitiert in: Eisenhut (Fn 5), 7.

7 Stefan Gerster, Das Escrow Agreement als obligationenrechtlicher Vertrag, in: Forstmoser et al., Zürcher Studien zum Privatrecht, Band 87, Zürich 1991, 3.

8 Eisenhut (Fn 5), 13.

9 In der Literatur teilweise auch als Grundgeschäft bezeichnet, wobei dieser Begriff für Verwirrung sorgen kann, da darunter teilweise auch das Verpflichtungs- als Gegenstück zum Verfügungsgeschäft verstanden werden kann; vgl. Eisenhut (Fn 5), 13.

10 Eisenhut (Fn 5), 24.

11 Eisenhut (Fn 5), 93.

12 Eisenhut (Fn 5), 48 ff.

[Rz 10] In der Praxis werden Escrow Agreements vorwiegend in folgenden Konstellationen abgeschlossen:

- Ein *Vollzugs*-Escrow bezweckt die Sicherung des Erfüllungsobjekts in einem synallagmatischen Hauptgeschäft, wobei dem Escrow-Agenten eine Ablieferungsfunktion zukommt.[13]
- Beim *Gewährleistungs*-Escrow wird ein vereinbarter Teil einer Kaufpreissumme vom Käufer an einen Escrow-Agenten übertragen. Wird der Betrag auf ein Bankkonto einbezahlt, so führt die Einzahlung zu einem *depositum irregulare* und die Bank wird gemäss Art. 481 Abs. 2 OR Alleineigentümerin des Vermögenswerts.[14] Zwischen Käufer und Verkäufer besteht eine Solidargläubigerschaft gegenüber dem Escrow-Agenten. Der Käufer hat üblicherweise dann einen Anspruch, wenn er rechtzeitig einen Gewährleistungsanspruch erhoben hat und dieser durch den Verkäufer oder das Gericht anerkannt wurde. Auf der anderen Seite besteht seitens des Verkäufers eine Forderung, wenn die Gewährleistungsfristen unbenutzt abgelaufen sind und keine Gewährleistungsansprüche mehr hängig sind.
- Bei einem *Sicherungs*-Escrow wird ein Sicherungsobjekt hinterlegt, welches aber, im Gegensatz zum Vollzugs-Escrow, nicht gleichzeitig Erfüllungsobjekt des Hauptgeschäftes ist.[15] Dem Escrow Agreement kommt daher keine Abwicklungsfunktion zu. Beispielsweise kann dadurch die Erfüllung einer potentiellen Schadenersatzforderung sichergestellt werden.
- Beim *Aktien*-Escrow werden Wertpapiere hinterlegt, beispielsweise zur Sicherung einer Call-Option. Im Gegensatz zur Situation bei Gewährleistungs-Escrows führt die Hinterlegung von Wertpapieren in einem Depot ohne anderslautende Vereinbarung nicht zu einem Übergang des Eigentums. Der Escrow-Agent ist Besitzer, nicht aber Eigentümer der hinterlegten Sache.[16]
- Der *Source-Code*-Escrow beinhaltet üblicherweise die Hinterlegung von auf einem Datenträger abgespeichertem Sourcecode (Quelltext) durch einen lizenzierenden Anbieter von Software.[17] Die Hinterlegung des Sourcecodes ermöglicht es einem Lizenznehmer, sich unter gewissen Umständen, üblicherweise als *ultima ratio*, Zugang zu den Daten zu verschaffen. So bleibt er in der Lage, beispielsweise Änderungen vorzunehmen oder Fehler zu beheben.

2. Involvierte Parteien

[Rz 11] Escrow-Verträge können entweder als Zwei- oder Drei-Parteien-Verhältnisse ausgestaltet werden. Bei einem Zwei-Parteien-Verhältnis schliessen eine Partei und der Escrow-Agent einen (echten) Vertrag zugunsten eines Dritten ab. Der Escrow-Agent wird den hinterlegten Vermögenswert an einen begünstigten Dritten weiterleiten.[18]

[Rz 12] Beim Drei-Parteien-Escrow wird eine Vereinbarung zwischen zwei Parteien eines Hauptgeschäfts und einem Escrow-Agenten abgeschlossen. In dieser Konstellation wird der Vermögens-

13 Eisenhut (Fn 5), 53.

14 Ueli Huber, Der Escrow in der Zwangsvollstreckung, SZW 6/2005, 286.

15 Eisenhut (Fn 5), 54.

16 Huber (Fn 14), 290.

17 Gerster (Fn 7), 25 ff.

18 Gerster (Fn 7), 7.

wert von einer Partei an den Escrow-Agenten übergeben, der ihn bei Eintritt der Bedingungen entweder an die andere Partei weiterleitet oder dem Hinterleger zurückgibt.[19]

III. Ethereum-Blockchain und Smart Contracts

1. Von der Bitcoin- zur Ethereum-Blockchain

[Rz 13] Eine Blockchain ist ein dezentrales Register (*distributed ledger*) mit konzeptionell unveränderbaren[20] Einträgen, auf dem Daten auf einer Kette an kryptographisch miteinander verbundenen Blöcken (*blockchain*) festgehalten werden. Bei Bitcoin werden auf diesem Register Transaktionsdaten gespeichert. Wie einleitend beschrieben, hat die Schweizer Stiftung «Ethereum» seit dem Jahr 2013 Lösungen entwickelt, um auf einer Blockchain nicht nur Werte, sondern auch komplexere dezentrale Software-Applikationen (DApps) zu speichern. Hierfür wurde die Ethereum-Blockchain als Plattform für Smart Contracts entwickelt. Diese ist komplett eigenständig und somit unabhängig von der Bitcoin-Blockchain, jedoch ist das technische Grundkonzept, wie beispielsweise die kryptographische Ausgestaltung oder das Mining, vergleichbar.[21] Zudem hat die Ethereum-Blockchain mit dem Ether (ETH) auch einen eigenen Token. Ether kann für das Erstellen und Nutzen von Applikationen, welche auf dem Ethereum-Protokoll basieren, verwendet werden. Unabhängig hiervon wird Ether auch als Zahlungs- und Investitionsobjekt gebraucht und ist mit einer Marktkapitalisierung von über CHF 43 Milliarden nach Bitcoin die verbreitetste sog. Kryptowährung.[22]

[Rz 14] Für weiterführende Informationen betreffend die Grundlagen der Blockchain-Technologie oder die Funktionsweise der Bitcoin- und Ethereum-Blockchain wird an dieser Stelle auf die vorhandene Literatur verwiesen.[23]

2. Smart Contracts als Halter von Vermögenswerten

[Rz 15] Wie einleitend dargelegt, wurde der Begriff «Smart Contracts» im Jahr 1994 durch den amerikanischen Computerwissenschafter und Kryptograph Nick Szabo eingeführt.[24] Szabo beschrieb damit Computerprotokolle, die einen Vertrag gemäss vordefinierten Bedingungen selbstständig umsetzen können. Im Protokoll könnten beispielsweise die Zahlungsbedingungen, Pfandrechte und sogar die Vertragsdurchsetzung geregelt werden.

---

19 Gerster (Fn 7), 6.

20 Die Unveränderbarkeit gilt nicht absolut, so können insbesondere Änderungen vorgenommen werden, wenn Miner mit der Mehrheit der Rechenleistung eine Änderung des Protokollcodes vornehmen wollen, wodurch gewisse Einträge nicht mehr als gültig erachtet werden.

21 Auch wenn nun geplant ist, den Konsensmechanismus von «Proof of Work» zu «Proof of Stake» zu ändern; vgl. für weiterführende Informationen: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.

22 https://coinmarketcap.com/.

23 Bspw. Luzius Meisser, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015; Mirjam Eggen, Chain of Contracts, AJP 2017, 3 ff.; Meyer/Schuppli (Fn 2), 204 ff.

24 Nick Szabo, Smart Contracts, 1994, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[Rz 16] Der Begriff Smart Contract ist jedoch in zweierlei Hinsicht irreführend. So stellt der Smart Contract nicht *per se* einen Vertrag im rechtlichen Sinne dar, sondern einen Softwareapplikationstyp. Ebenso steht das Wort «smart» auch nicht für «intelligent». Vielmehr wird der Begriff – wie in der Elektronikindustrie üblich – für Anwendungen verwendet, die in der Lage sind, autonom mit anderen Applikationen zu interagieren, d.h. sich mit diesen zu verbinden und Daten auszutauschen.[25] Ein Smart Contract führt nur das aus, was der Ersteller programmiert hat, dies aber zuverlässig.[26]

[Rz 17] In technischen Beschreibungen wird ein Smart Contract definiert als «*a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain*».[27] Die juristische Literatur unterteilt den Begriff Smart Contracts in «Smart Contract Code» und «Smart Legal Contracts». Der erste Begriff «Smart Contract Code» soll dabei die operationelle Ausführung eines Software-Agenten, m.a.W. eines Computerprogramms, beschreiben, das bis zu einem gewissen Teil zu einem autonomen und eigenständigen Verhalten in der Lage ist.[28] Auf der anderen Seite beschreibt «Smart Legal Contract» die Art und Weise, wie ein «juristischer» Vertrag in Code dargestellt und durch Software ausgeführt werden kann.[29] In diesem Teilbereich bestehen diverse Forschungsprojekte, beispielsweise der Ricardian Contract oder Legalese, die Vertragsinhalte in code-basierte Sprachen transferieren.[30]

[Rz 18] Im Rahmen des vorliegenden Beitrages wird der Begriff «Smart Contract» als eine Sammlung von Softwarefunktionen verstanden, die sich, gestützt auf die Blockchain-Architektur, beim Eintritt gewisser Bedingungen selbst ausführen können und die aufgrund der dezentralen und kryptographischen Ausgestaltung der Blockchain konzeptionell selbstdurchsetzend und manipulationssicher sind.[31] Erstmals wurde damit die Möglichkeit geschaffen, die sichere Bindung und Weiterleitung von Vermögenswerten ohne Intermediär und «klassischen Escrow-Agenten» umzusetzen.

3. Verhältnis zwischen Vertrag und Smart Contract

[Rz 19] Vom Begriff «Smart Contract» darf demnach nicht zwingend auf einen Vertrag im Rechtssinne geschlossen werden. Je nach Art der Interaktion kann aber durchaus ein Vertragsverhältnis vorliegen:

a. Direkte Interaktion einer Partei mit einem Smart Contract

[Rz 20] Es ist möglich, als einzelne Partei mit einem Smart Contract zu interagieren, ohne dass eine Gegenpartei in Form einer natürlichen oder juristischen Person existiert. Die rechtliche Qua-

25 Meyer/Schuppli (Fn 2), 208.

26 Meyer/Schuppli (Fn 2), 208.

27 Ethereum Homestead Guide, https://github.com/ethereum/homestead-guide/blob/master/source/contracts-and-transactions/contracts.rst.

28 Christopher D. Clack/Vikram A. Bakshi/Lee Braine, Smart Contract Templates: foundations, design landscape and research directions, London 2016, https://arxiv.org/pdf/1608.00771.pdf, 2.

29 Clack/Bakshi/Braine (Fn 28), 2; Meyer/Schuppli (Fn 2) 207 f.

30 Clack/Bakshi/Braine (Fn 28), 2 f.

31 Meyer/Schuppli (Fn 2), 208.

lifikation von Transaktionen mit einer Software als Gegenpartei ist heute noch nicht geklärt und nicht Gegenstand des vorliegenden Beitrages. Die heute vorherrschende Meinung geht indes davon aus, dass mangels Rechtssubjektivität des Smart Contracts, d.h. der Softwareapplikation, kein Rechtsverhältnis eingegangen wird (siehe IV.2. unten).

b. Abwicklung von Zweiparteien-Beziehungen

[Rz 21] Daneben ist es aber auch zweien Parteien möglich, gemeinsam einen Smart Contract zu nutzen. In dieser Konstellation besteht regelmässig ein Vertragsverhältnis zwischen diesen Parteien, wobei der Smart Contract als Ausführungsinstrument des Vertrages genutzt wird. Der Smart Contract ist Bestandteil der Vertragsbeziehung, welche aber regelmässig Rechte und Pflichten beinhaltet, welche nicht im Smart Contract spezifiziert sind, sondern sich aus allgemeinen Rechtsgrundsätzen oder (evtl. auch impliziten) Zusatzvereinbarungen ergeben. Inwieweit der Inhalt des Smart Contracts auch den Inhalt des Vertrags im rechtlichen Sinne darstellt, muss im Einzelfall beurteilt werden. Gemäss Art. 1 OR i.V.m. Art. 11 OR ist ein Vertrag eine Willenserklärung, die grundsätzlich an keine Form gebunden ist. Es ist demnach denkbar, dass das Erstellen und Weiterleiten von Smart Contract Code als Offerte zum Vertragsabschluss zu qualifizieren ist, sofern der Code alle wesentlichen Vertragspunkte beinhaltet. Ebenso ist es aber möglich, dass die übereinstimmende Willenserklärung mündlich erfolgt oder schriftlich auf Papier festgehalten wird.

c. Abwicklung von Mehrparteien-Beziehungen

[Rz 22] Die Nutzung von Smart Contracts ist nicht auf Zwei-Parteien-Verhältnisse beschränkt. Smart Contracts können auch als eigentliche «Smart Contract Systems» (SCS) von mehreren Parteien genutzt werden. Die Möglichkeiten reichen bis zur Erstellung komplexer dezentraler autonomer Organisationen (DAOs). Bei einer solchen DAO wird ein Netzwerk diverser interagierender Smart Contracts geschaffen, sodass verschiedene Personen dezentral gemeinsame Projekte strukturieren und abwickeln können.[32] Beim bisher bekanntesten Anwendungsfall einer DAO («The DAO» genannt) wurden im Mai 2016 über USD 150 Millionen an Kapital gesammelt.[33] «The DAO» hat dann gestützt auf Abstimmungen der Investoren automatisiert finanzielle Mittel Projekten zugewiesen und die Gewinne wiederum auf die Investoren verteilt. Aufgrund eines Fehlers im Code konnte eine unbekannte Person im Juni 2016 jedoch einen substanziellen Teil der Gelder der DAO entziehen, wodurch jenes Projekt sein Ende fand, und die Ethereum-Blockchain in Ethereum und Ethereum Classic gespalten wurde.[34]

---

32 Meyer/Schuppli (Fn 2), 208.

33 Andreas Flütsch, Schweiz bringt weltgrösstes Crowdfunding hervor, Tages-Anzeiger Online vom 20. Mai 2016, https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/schweiz-bringt-weltgroesstes-crowdfunding-hervor/story/27265162. Zur rechtlichen Einordnung des Falls vgl. auch Eleonor Gyr, Dezentrale Autonome Organisation DAO, in: Jusletter 4. Dezember 2017.

34 Bei diesem als Hard-Fork bezeichneten Ereignis wurde die Entwendung der Mittel von einer Mehrheit der Miner mittels einer Protokolländerung rückgängig gemacht. Die ursprüngliche Protokollversion wurde von einer Minderheit der Miner als «Ethereum Classic» weitergeführt.

4. Einsatzmöglichkeiten als Escrow und Bildung von Fallgruppen

[Rz 23] Die Vorteile der Nutzung eines Smart Contracts sind vielseitig. Insbesondere erlauben Smart Contracts grundsätzlich den Verzicht auf Intermediäre, was sowohl die Effizienz erhöht als auch die Kosten senkt. Zudem wird durch die Automatisierung der Vertragsexekution gerade in globalen Transaktionsstrukturen eine erhöhte Erfüllungssicherheit erzielt. Diesen (und weiteren) Vorteilen stehen indes auch Nachteile operativer und rechtlicher Natur gegenüber. So besteht eine starke Abhängigkeit von der verwendeten technischen Infrastruktur. Weiter ist es schwierig, zuverlässige Input-Daten in die Softwarestruktur einzubringen. Smart Contracts können zudem einzig Tokens als Vermögenswerte halten. Diese sind heute noch nicht flächendeckend verbreitet und nach wie vor einer hohen Volatilität ausgesetzt. Darüber hinaus steht die binäre Logik von Softwarefunktionen in einem Spannungsfeld mit der Komplexität und Unvorhersehbarkeit der realen Welt, womit auch über Smart-Contract-Systeme abgewickelte Vertragsbeziehungen für Streiterledigungsmechanismen offen sein müssen.

[Rz 24] Es gibt verschiedene Möglichkeiten, einen Smart Contract im Rahmen eines Escrow-Verhältnisses zu nutzen. Allen ist gemeinsam, dass während einer gewissen Zeit die finanziellen Mittel (im Falle der Ethereum Blockchain die Ether Tokens) durch einen Smart Contract gebunden werden sollen. Ebenfalls wird in allen Fällen beim Eintritt vordefinierter Ereignisse, analog zu den bisherigen Escrow-Dienstleistungen, eine Transaktion ausgelöst. Unterschiedlich sind die Varianten jedoch in der Art und Weise, wie der Smart Contract von diesem transaktionsauslösenden Ereignis Kenntnis erhält.

[Rz 25] Smart Contracts können nicht nur als *Ersatz* von Escrow-Agenten eingesetzt werden, sondern auch als *Instrument zur Abwicklung* eines klassischen Escrow-Geschäfts. In diesem Fall ist zwar nach wie vor eine natürliche oder juristische Person als «klassischer» Escrow-Agent vorhanden, jedoch nur mit denjenigen faktischen Verfügungsmöglichkeiten, die im Smart Contract vorgesehen sind. Dies führt zu einer Reduzierung des Gegenparteienrisikos zwischen dem Hinterleger des Vermögenswerts und dem Escrow-Agenten.

[Rz 26] Im vorliegenden Beitrag wird zwischen drei Fallgruppen unterschieden, bei denen der Smart Contract entweder in einem Escrow-Geschäft oder mit einer escrow-ähnlichen Funktion eingesetzt wird. Die erste Fallgruppe bezieht sich auf Smart Contracts, die für die Parteien des Hauptgeschäfts als autonome Escrow-Agenten ohne involvierte Drittpartei fungieren (nachfolgend IV.). Die zweite Fallgruppe (nachfolgend V.) bezieht sich auf Konstellationen, in denen eine Drittpartei vorhanden ist, diese aber lediglich Daten zur Verfügung stellt, welche in den Smart Contract eingespeist werden und nach vorgegebenen Bedingungen die Transaktion auslösen können. Die dritte Fallgruppe beinhaltet schliesslich Situationen, in denen eine Drittpartei, beispielsweise eine natürliche oder juristische Person, mittels eines manuellen Inputs die Transaktion eines Smart Contracts auslöst (nachfolgend VI.). Die dritte Fallgruppe kommt den klassischen Escrow-Verhältnissen am nächsten.

[Rz 27] Die Fallgruppen wurden bewusst weit abgesteckt, sodass Situationen eingeschlossen sind, die zwar nach der oben erwähnten Definition, sei es mangels Gegenpartei oder mangels Hinterlegung eines Vermögenswerts, kein Escrow Agreement beinhalten, in denen die Parteien durch den Einsatz eines Smart Contracts aber vergleichbare Sicherungszwecke verfolgen. Da sich die Möglichkeiten der Blockchain-Technologie rasch weiterentwickeln und neben Ethereum zunehmend auch andere Infrastrukturen für Smart Contracts entstehen, haben die beschriebenen Fall-

gruppen keinen abschliessenden Anspruch. Sie dienen dem Leser vielmehr als Übersicht über mögliche Ausgestaltungen.

IV. Fallgruppe 1: Smart Contract mit Escrow-Funktion

1. Beschreibung der Fallgruppe

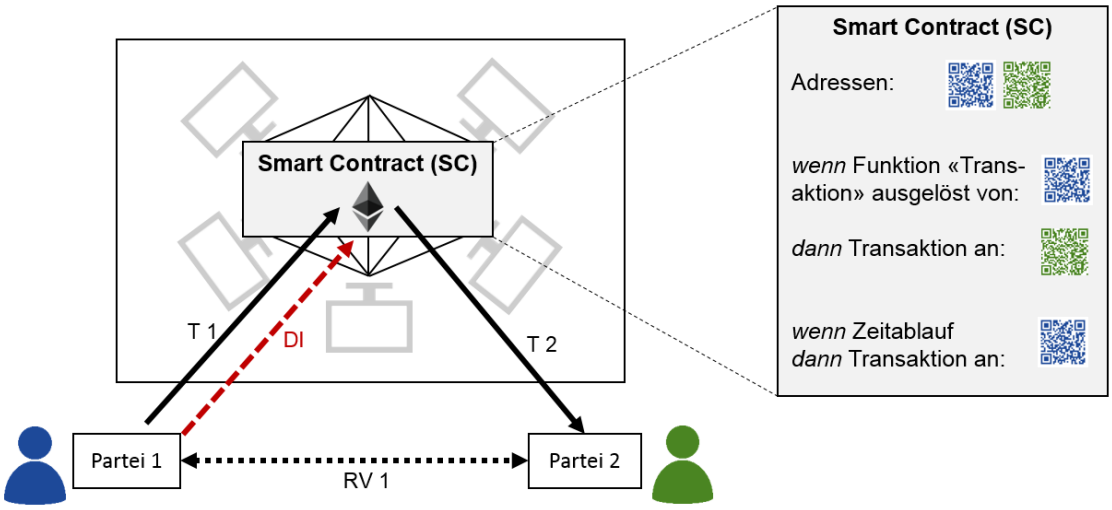
[Rz 28] Die erste Fallgruppe beinhaltet Konstellationen, bei denen eine oder zwei Parteien einen Smart Contract zur Bindung von Vermögenswerten nutzen, ohne dass eine natürliche oder juristische Person als Drittpartei involviert ist.[35] Es ist neben den zwei Parteien des Hauptgeschäfts kein Intermediär vorhanden, mit welchem ein Vertragsverhältnis eingegangen wird. Somit besteht, mangels Rechtssubjektivität des Smart Contracts, auch kein Escrow Agreement. In der Praxis kann ein Smart Contract in dieser Hinsicht wie folgt genutzt werden:

- Eine oder zwei Parteien definieren das zahlungsauslösende Ereignis so, dass der Smart Contract dieses autonom und ohne Bezug von Daten ausserhalb der Blockchain verarbeiten kann. Somit muss das Ereignis (i) ohne Notwendigkeit von Ermessen und (ii) aufgrund von sich auf der Blockchain befindlichen Daten bestimmbar sein. Ein einfaches Beispiel ist ein Smart Contract mit einem einprogrammierten «Timer». Sobald eine gewisse Zeit abgelaufen ist,[36] löst der Smart Contract ohne weitere Inputs die Zahlung an den im Voraus definierten Empfänger aus.
- Ebenfalls kann der Smart Contract so ausgestaltet werden, dass eine Partei des Hauptgeschäfts die Transaktion selbst auslösen kann. Bei dieser Variante müssen jedoch einige Vorkehrungen getroffen werden, damit der Sicherungszweck des Smart Contracts nicht unterlaufen wird (siehe 3. unten).

[Rz 29] Die Fallgruppe lässt sich am Beispiel eines durch die Hauptpartei auslösbaren Smart Contracts wie folgt visualisieren:

35 Die Teilnehmer des Blockchain-Netzwerkes (Miner) werden vorliegend nicht als Drittparteien bezeichnet.

36 In der Praxis wird stattdessen auch auf das Erstellen eines zukünftigen Blocks mit einer bestimmten Nummer abgestellt, da sich dies in technischer Hinsicht einfacher umsetzen lässt.



Legende (in chronologischer Reihenfolge):

RV 1: Rechtsverhältnis (Hauptgeschäft) zwischen Partei 1 und 2

T 1: Speichern des SC (mit Adressen von Partei 1 und 2)
gleichzeitig oder später
Transaktion Partei 1 an SC (Ether werden durch SC gebunden)

DI: Dateninput an SC (Auslösen Funktion «Transaktion» durch Partei 1)
danach
T 2: Transaktion SC an Partei 2

Grafik 1: Smart Contract als autonomer Escrow-Agent

2. Rechtssubjektivität eines Smart Contracts?

[Rz 30] Wie dargelegt, existiert bei der vorliegenden Ausgestaltung kein Intermediär als Vertragspartei. Die in Escrow gelegten Vermögenswerte werden dezentral durch eine Softwareapplikation, den Smart Contract, kontrolliert.

[Rz 31] Basierend auf dem heutigen Stand der Diskussion ist davon auszugehen, dass Softwareapplikationen keine Rechtssubjektivität zugesprochen werden kann. Entsprechend besteht bei dieser Fallgruppe mangels Rechtssubjektivität des Smart Contracts auch kein Escrow Agreement. Ein 3-Parteien-Escrow-Verhältnis wird zu einem Rechtsgeschäft zwischen zwei Parteien; der Zwei-Parteien-Escrow-Vertrag zugunsten eines Dritten wird eine einseitige Handlung ohne Vertragsverhältnis. Ob auch in Zukunft die Rechtssubjektivität stets auf natürliche oder juristische Personen beschränkt sein wird oder ob eines Tages eine «elektronische Person» geschaffen wird, bleibt abzuwarten. Die noch vorwiegend philosophische Frage wird aktuell vermehrt im Zusammenhang mit Robotern und künstlicher Intelligenz erörtert.[37]

37 Vgl. bspw. Martin Schnetter, Robotik und ihre Regulierung: Tendenzen in Technik, Recht und Ethik, Berlin 2016, 38.

3. E-Commerce als Anwendungsbeispiel

[Rz 32] Denkbar ist die Nutzung eines Smart Contracts zur Sicherung eines Hauptgeschäfts beispielsweise bei einer Online-Auktion. Wenn ein Käufer im Internet eine Sammlung an Gesetzeskommentaren erwirbt, kann er einen Smart Contract erstellen und den Kaufpreis in Ether vom Smart Contract binden lassen. Sobald die Bücher beim Käufer angekommen sind, wird der Betrag an den Verkäufer transferiert. Für das Auslösen der Transaktion sind zwei Varianten denkbar:

- Einerseits könnte der Käufer den Smart Contract so erstellen, dass er selbst mittels seines privaten Schlüssels die Zahlung nach Erhalt der Bücher auslösen kann, wie dies bei der obigen Visualisierung dargestellt wurde (siehe Grafik 1 oben). Diese Variante ist aber für den Verkäufer offensichtlich nicht vorteilhaft, da er von der Transaktion des Käufers abhängig ist. Der Mehrwert im Vergleich zu einer nachträglichen Überweisung des Kaufpreises wäre gering.
- Andererseits, dies ist die sinnvollere Variante, könnte der Käufer beim Erstellen des Smart Contracts den Hash[38] einer beliebigen, nur ihm bekannten Nummer auf dem Smart Contract abspeichern. Sobald die Bücher physisch übergeben worden sind, wird auch die geheime Nummer an den Verkäufer ausgehändigt, der damit die Transaktion des Kaufpreises an sich auslösen kann.[39] Der Vorteil dieser Variante ist, dass der Austausch zwischen Nummer und Büchern Zug-um-Zug erfolgen kann. Der Verkäufer kann den Spediteur so instruieren, dass er die Bücher nur übergibt, wenn er vom Käufer die korrekte Nummer erhält. Zudem löst das Eingeben der geheimen Nummer automatisch die Zahlung aus, und zwar ausschliesslich an die Adresse des Verkäufers. Somit ist diese Methode auch einfacher und sicherer, als wenn Bargeld an den Spediteur übergeben würde.

[Rz 33] Um sicherzustellen, dass der Spediteur tatsächlich die korrekte Nummer übernimmt, könnte in einer weiter optimierten Version auch der Spediteur in den Smart Contract eingebunden werden. Dieser würde ebenfalls nur dann seine Entschädigung erhalten, wenn er die korrekte geheime Nummer in den Smart Contract eingibt.

[Rz 34] Unabhängig von den beiden Varianten ist in jedem Fall ein Zeitlimit einzuprogrammieren, so dass, falls die Gesetzeskommentare gar nie verschickt würden, der Kaufpreis nicht unbeschränkt vom Smart Contract gebunden bliebe.

---

38 Beim Hash handelt es sich um einen kryptographischen Algorithmus, der einen Datensatz beliebiger Länge in einen solchen bestimmter Länge umwandelt. Die Umwandlung erfolgt in diese Richtung schnell und unkompliziert. Umgekehrt ist das Umwandeln eines Hashs in die ursprüngliche Nummer bei ausreichender Verschlüsselung jedoch nicht mehr möglich. Somit ist sichergestellt, dass der Smart Contract beim Input der korrekten Nummer die Transaktion auslöst, aber keine Drittperson anhand des (öffentlich einsehbaren) Hash-Werts diese Nummer ausfindig machen kann; vgl. Meyer/Schuppli (Fn 2), 206.

39 Siehe das beschriebene Beispiel (inklusive Code) unter https://dappsforbeginners.wordpress.com/tutorials/two-party-contracts/.

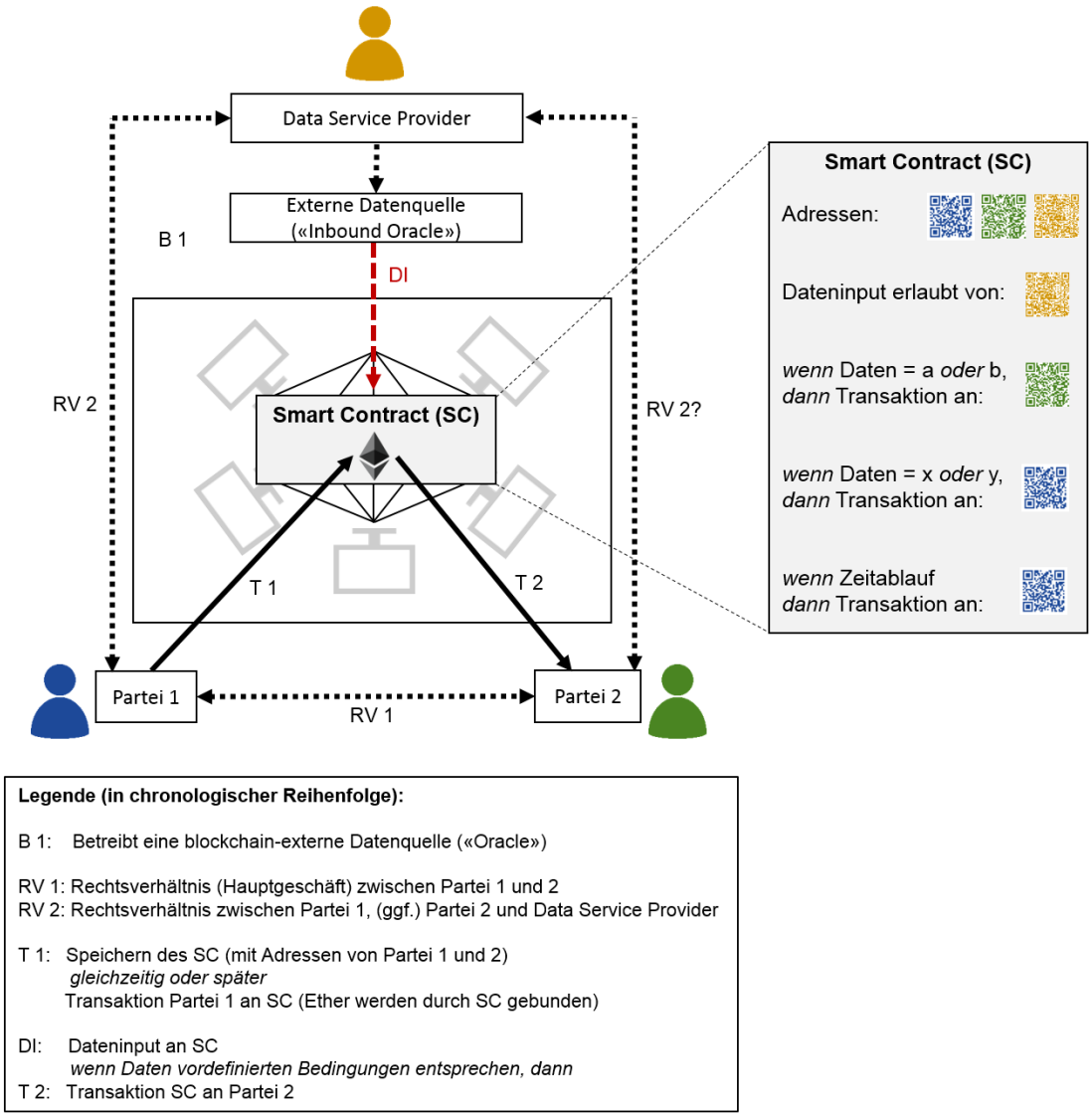
V. Fallgruppe 2: Drittpartei als Daten-Orakel

1. Beschreibung der Fallgruppe

[Rz 35] Die zweite Fallgruppe beinhaltet Konstellationen, in welchen blockchain-externe Daten die Grundlage für das transaktionsauslösende Ereignis darstellen. Zumeist noch zentral[40] vorhandene Daten werden mittels eines sogenannten «Inbound Oracle» in den Smart Contract eingespeist. Im Gegensatz zu einem klassischen Escrow-Agenten nimmt die Drittpartei aber weder direkten Einfluss auf das Auslösen der Transaktion, noch verfügt sie über eine direkte Zugriffsmöglichkeit auf die im Smart Contract gebundenen Werte. Die Parteien des Hauptgeschäfts definieren die für die Transaktion relevanten Bedingungen direkt im Smart Contract. Der Input der vordefinierten Daten wird zum zahlungsauslösenden Ereignis.

[Rz 36] Die Fallgruppe lässt sich wie folgt darstellen:

40 Jedoch gibt es bereits mehrere Projekte mit dem Ziel, auch dezentrale *Oracles* zu erstellen, beispielsweise das LINK Network (https://link.smartcontract.com/) oder auch die Aeternity Plattform (https://www.aeternity.com/).



Grafik 2: Drittpartei als Bereitstellerin von transaktionsauslösenden Daten

2. Orakel als Schnittstelle zwischen Blockchain und externen Daten

[Rz 37] Die Schnittstellen zwischen Daten inner- und ausserhalb der Blockchain sind von grosser Bedeutung. Im Gegensatz zu einem klassischen Webserver ist ein Smart Contract nicht in der Lage, selbst auf Daten ausserhalb der Blockchain zuzugreifen. Diese müssen von einem sog. «Inbound Oracle» in die Blockchain eingespeist werden. Während alle Daten auf der Blockchain konzeptionell unveränderbar und unmanipulierbar sind, haben externe Daten (resp. die Datenquellen) diese Eigenschaften nicht. Es gibt folgende Varianten, wie man dennoch eine gewisse Integrität der Daten und Authentizität des Datenursprungs sicherstellen kann:

- Als «Inbound Oracle» wird eine besonders vertrauenswürdige (beispielsweise staatliche) Institution ausgesucht.
- Anstatt eines «Inbound Oracle» werden Dateninputs von mehreren Quellen akzeptiert und der Smart Contract löst die datenabhängige Handlung nur dann aus, wenn eine genügende

Anzahl gleicher Antworten eingegangen ist. Diese Methode hat jedoch den Nachteil, dass sie sowohl hohe Transaktionsgebühren[41] verursacht, als auch längere Zeit benötigt, bis die genügende Anzahl an Rückmeldungen eingegangen ist.

- Neben den eigentlichen Daten wird ein Authentizitätsnachweis beigelegt, der belegen soll, dass die in den Smart Contract eingefügten Daten den Originaldaten entsprechen. Dieses Konzept wird beispielsweise von Oraclize verwendet, einem grösseren Anbieter von Blockchain-Orakel-Dienstleistungen.[42]

3. Qualifikation des Vertragsverhältnisses

[Rz 38] Es stellt sich die Frage, ob ein Data Service Provider als Escrow-Agent klassifiziert werden könnte, da er zwar indirekt, aber massgeblich die Auslösung der Transaktion bewirkt. Dies ist u.E. zu verneinen. Der Data Service Provider liefert die von den Parteien bezeichneten Daten und speist diese in den Smart Contract ein. Die Verarbeitung dieser Input-Daten folgt gemäss den im Smart-Contract-Algorithmus implementierten, vordefinierten Funktionen und Bedingungen und führt je nach Dateninhalt zu einem bestimmten Output des Smart Contracts.

[Rz 39] Der Data Service Provider hat somit keine Verfügungsgewalt über die im Smart Contract gehaltenen Vermögenswerte. Auch wenn der Data Service Provider mittels manipulierter Daten gezielt eine Reaktion des Smart Contracts bewirken könnte, handelt es sich beim Vertragsverhältnis zwischen den Parteien des Hauptgeschäfts und der Drittpartei mangels Hinterlegung bzw. Übertragung der Verfügungsmacht nicht um ein Escrow Agreement. Vielmehr ist in diesen Konstellationen, sofern Schweizer Recht anwendbar ist, von einem gewöhnlichen Auftragsverhältnis i.S.v. Art. 398 OR oder allenfalls von einem Werkvertrag i.S.v. Art. 363 OR auszugehen. Denkbar sind aber auch Fälle, in denen das Orakel dezentral betrieben wird, so dass es an einer Gegenpartei und somit einem Vertragsverhältnis fehlen kann.

4. Logistik als Anwendungsbeispiel

[Rz 40] Ein Smart Contract mit einem Daten-Orakel erscheint sinnvoll, wenn das transaktionsauslösende Ereignis keinen, oder zumindest kaum, Ermessensspielraum beinhaltet und sich die relevanten Informationen in binären Code übertragen lassen. Das Konzept lässt sich zudem besonders gut mit der mechanischen Praxis der «strict compliance», wie sie bei Escrow Verhältnissen nach amerikanischem Recht üblich ist, vereinbaren.[43] Eine Wertung des «übereinstimmenden wirklichen Willens der Parteien» im Sinne des schweizerischen Rechts kann ein Smart Contract offensichtlich nicht vornehmen.

[Rz 41] Die externe Datenquelle kann neben einer Website auch ein Sensor («hardware oracle») sein, der beispielsweise den Standort eines bestimmten Containers eruiert und, sobald der Container am vereinbarten Platz ist, den Input zur Zahlung an den Smart Contract übermittelt. An solchen Modellen experimentieren derzeit viele grosse Logistikunternehmen wie beispielsweise

41 Zur Beschreibung und zum Umfang der Transaktionsvergütung auf der Ethereum Blockchain siehe bspw. Meyer/Schuppli (Fn 2), 212.

42 http://www.oraclize.it/.

43 Vgl. bspw. Barlow Burke, Law of Title Insurance, 3. Aufl., New York 2000, 13–21.

Maersk.[44] Ein anderes Projekt integriert Sensoren in Medikamentenlieferungen, welche die Daten auf der Blockchain abspeichern, um aufzuzeigen, dass jederzeit weder die Mindesttemperatur unterschritten noch die Höchsttemperatur überschritten wurde.[45] Auch bei einem solchen Projekt lassen sich Smart Contracts nutzen, um abhängig von den Daten Transaktionen auszulösen oder eben zu verhindern.

VI. Fallgruppe 3: Drittpartei als Auslöserin einer Smart-Contract-Transaktion

1. Beschreibung der Fallgruppe

[Rz 42] Bei der dritten Fallgruppe befindet sich hinter dem Smart Contract eine Drittpartei, eine natürliche oder juristische Person, welche die Voraussetzungen für die Transaktion prüft und gegebenenfalls die Transaktionsfunktion auslöst. In der Praxis wird der Smart Contract in diesen Fällen so programmiert, dass die Transaktion mittels eines privaten Schlüssels der Drittpartei ausgelöst werden kann.

[Rz 43] Diese Ausgestaltung des Smart Contracts ist insbesondere dann sinnvoll, wenn für das transaktionsauslösende Ereignis entweder Ermessensspielraum vorhanden ist, oder sich die Informationen nur schwierig in binären Code übertragen lassen. Die Kriterien für die Auslösung der Transaktion werden, wie bei klassischen Escrow Agreements, ausserhalb des Smart Contracts vertraglich festgelegt. Die Drittpartei und nicht der Smart Contract muss prüfen, ob sie erfüllt sind.

[Rz 44] Auf den ersten Blick könnte man bei Konstellationen in dieser Fallgruppe argumentieren, dass kein Smart Contract benötigt werde, da mittels direkter Übergabe eines Wallets derselbe Zweck erfüllt werden könnte. Anstatt der Transaktion in einen Smart Contract könnte der Drittpartei ein privater Schlüssel übergeben werden, der den Zugriff auf die Vermögenswerte erlaubt. Der entscheidende Vorteil eines Smart Contracts ist aber die Möglichkeit zur Reduktion der Verfügungsmacht der Drittpartei auf den benötigten Kern: die Transaktion an die vordefinierte Partei. Dadurch kann das Risiko minimiert werden, dass sich die Drittpartei die Vermögenswerte in vertragswidriger Weise selbst aneignet oder an einen weiteren Dritten transferiert. Ebenfalls könnte bei der direkten Übergabe eines privaten Schlüssels nicht verhindert werden, dass sich der alte Inhaber eine Kopie des privaten Schlüssels macht und später auf die Vermögenswerte zugreift. Entsprechend können zwei Subfallgruppen definiert werden:

a. Umfassende Verfügungsmacht

[Rz 45] Bei einer umfassenden Übertragung der Verfügungsmacht erhält eine Drittpartei den vollen Zugriff auf die im Smart Contract vorhandenen Vermögenswerte. Sie hat daher faktisch die Möglichkeit, eine Transaktion an eine beliebige Person auszulösen, oder aber auch gar keine.

---

44 In einem ersten Schritt steht allerdings noch die sichere Erfassung der Daten im Vordergrund und nicht die eigentliche Transaktion, vgl. bspw. https://www.coindesk.com/worlds-largest-shipping-company-tracking-cargo-blockchain/.

45 Vgl. «Data Integrity for Supply Chain Operations Powered by Blockchain», https://modum.io/.

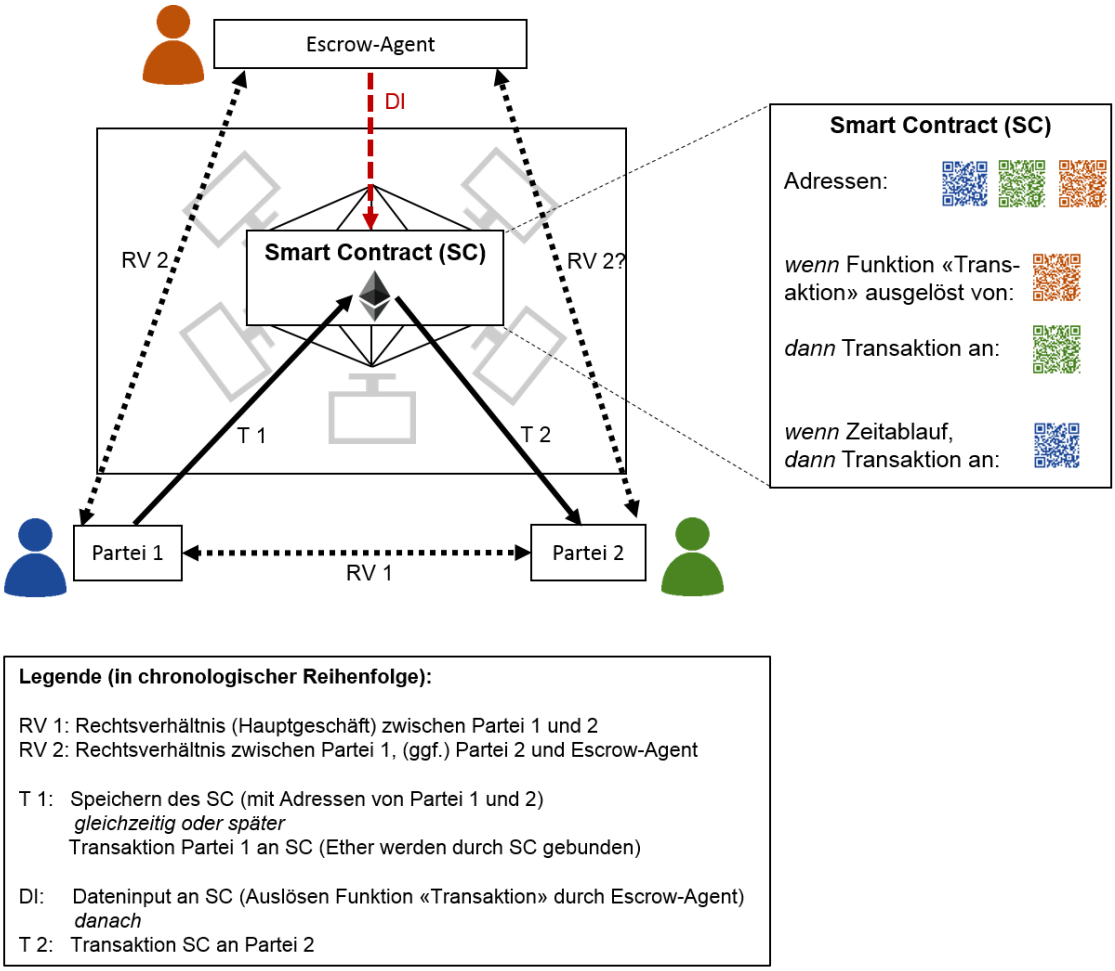
[Rz 46] Diese Konstellation ist nah an derjenigen eines Escrow Agreements, bei welcher beispielsweise ein Finanzintermediär als Escrow-Agent tätig wird und das erhaltene Geld bei sich oder einer Bank hinterlegt. Der Unterschied liegt aber darin, dass hier weder die Drittpartei noch eine andere Person die Vermögenswerte tatsächlich bei sich hinterlegen. Die Vermögenswerte sind zu jeder Zeit auf der dezentralen Blockchain abgespeichert.

b. Eingeschränkte Verfügungsmacht

[Rz 47] Neben der umfassenden Verfügungsmacht lässt ein Smart Contract die Möglichkeit zu, dass die Drittpartei nur in einem bestimmten, vordefinierten Umfang über die Vermögenswerte verfügen kann. Die Transaktion kann beispielsweise so vordefiniert werden, dass sie die Drittpartei nur noch an einen spezifischen Empfänger oder innerhalb eines spezifischen Zeitfensters auslösen kann.

c. Visualisierung

[Rz 48] Graphisch dargestellt sieht die Situation bei dieser Fallgruppe wie folgt aus:



Legende (in chronologischer Reihenfolge):

RV 1: Rechtsverhältnis (Hauptgeschäft) zwischen Partei 1 und 2
RV 2: Rechtsverhältnis zwischen Partei 1, (ggf.) Partei 2 und Escrow-Agent

T 1: Speichern des SC (mit Adressen von Partei 1 und 2)
gleichzeitig oder später
Transaktion Partei 1 an SC (Ether werden durch SC gebunden)

DI: Dateninput an SC (Auslösen Funktion «Transaktion» durch Escrow-Agent)
danach
T 2: Transaktion SC an Partei 2

Grafik 3: Klassischer Escrow-Agent als Auslöser der Smart-Contract-Transaktion

2. Qualifikation als Escrow Agreement

a. Sicherungsweck

[Rz 49] Der Zweck eines Escrow Agreements besteht wie dargelegt (II. oben) in der Sicherung der Forderung eines Gläubigers sowie des Vollzugs eines Hauptgeschäftes.[46] Voraussetzung zur Qualifikation der Konstellationen unserer dritten Fallgruppe als Escrow Agreements ist daher das Vorhandensein eines Hauptgeschäftes sowie ein durch die Nutzung des Smart Contracts verfolgter Sicherungszweck.

b. Tokens als taugliche Sicherungsobjekte

[Rz 50] In der Lehre wird die Ansicht vertreten, dass nur *bewegliche Sachen* taugliche Sicherungsobjekte eines Escrow Agreements sind, an denen Besitz und Eigentum begründet werden können.[47] Ob ein bestimmtes Objekt ein tauglicher Gegenstand sei, hänge von der Art des Sicherungsobjektes, dem darauf anwendbaren Recht und dem verfolgten Zweck ab.[48] Das Sicherungsobjekt müsse verwertbar sein und einen Vermögenswert aufweisen.

[Rz 51] Der Zweck der Einschränkung von Sicherungsobjekten auf bewegliche Sachen wird deutlich, wenn die in der Lehre erörterte Frage betrachtet wird, ob auch Naturkräfte taugliche Sicherungsobjekte darstellen können. Naturkräfte bilden gemäss Art. 713 des Schweizerischen Zivilgesetzbuches (ZGB; SR 210) Gegenstand des Fahrniseigentums, sind aber keine Sachen. Sachenrechtliche Bestimmungen sind soweit passend analog anwendbar. Eisenhut verneint die Tauglichkeit mit der Begründung, dass Naturkräften, zumindest zurzeit, das notwendige «Dauerdasein» fehle, das Besitz und Eigentum voraussetzen.[49] Aufgrund ihrer physikalischen Unbeständigkeit sei es nicht denkbar, dass Verfügungsgewalt über Energie einem Schuldner entzogen und auf einen Escrow-Agenten übertragen werden könne.[50] Naturkräfte kämen daher als Sicherungsobjekt nicht in Frage.[51]

[Rz 52] Unabhängig von der Beurteilung der Sachqualifikation von Blockchain Tokens[52] ist daher ersichtlich, dass die Möglichkeit zur Ausübung von Verfügungsgewalt das zentrale Kriterium für die Tauglichkeit als Sicherungsobjekt darstellt. In der Vergangenheit war eine solche Verfügungs-

---

46 In der Literatur teilweise auch als Grundgeschäft bezeichnet, wobei dieser Begriff für Verwirrung sorgen kann, da darunter teilweise auch das Verpflichtungs- als Gegenstück zum Verfügungsgeschäft verstanden werden kann; vgl. Eisenhut (Fn 5), 13.

47 Eisenhut (Fn 5), 87.

48 Eisenhut (Fn 5), 87.

49 Eisenhut (Fn 5), 88 f.

50 Eisenhut (Fn 5), 88 f.

51 Eisenhut (Fn 5), 89.

52 Die Sachqualifikation von Blockchain Tokens ist noch umstritten: Eine Bejahung der Eigentumsmöglichkeit an Bitcoins («Under Swiss Law, users of Bitcoins can be qualified as owners of these Bitcoins in question in the sense of Article 641 SCC») findet sich in Barbara Graham-Siegenthaler/Andreas Furrer, The Position of Blockchain Technology and Bitcoin in Swiss Law, in: Jusletter 8. Mai 2015, ebenso hat die FINMA in der Vergangenheit bereits den Standpunkt vertreten, Bitcoins seien als Sachen in einem Konkurs grundsätzlich aussonderbar; a.A. sind bspw. Harald Bärtschi/Christian Meisser, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 141; Jean-Daniel Schmid/Alexander Schmid, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, in: Jusletter 4. Juni 2012, N 39. Zum insolvenzrechtlichen Schutz im Allgemeinen vgl. Benedikt Maurenbrecher/Urs Meier, Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen, in: Jusletter 4. Dezember 2017.

gewalt, soweit erkennbar, auf (körperliche) Objekte beschränkt. Die Blockchain-Technologie bietet nun aber die Möglichkeit, bei Tokens als Daten trotz mangelnder körperlicher Manifestation einen vergleichbaren Grad an ausschliesslicher Verfügungsgewalt zu erreichen. Tokens sind aufgrund ihrer kryptographischen und dezentralen Ausgestaltung, wie körperliche Objekte, nicht replizierbar.[53] Ebenso kann keine einzelne Partei Einfluss auf die Funktionalität der Tokens nehmen. Die Tokens können einzig vom Inhaber des relevanten privaten Schlüssels beherrscht werden. Diesem kommt die faktische, ausschliessliche Verfügungsgewalt über die Werteinheit zu. Im Gegensatz zu anderen Daten können Tokens nach Ausüben ihrer Hauptfunktion, der Transaktion, zudem nicht mehr vom ursprünglichen Inhaber genutzt werden. Die ausschliessliche Verfügungsgewalt geht dann auf den Inhaber eines anderen privaten Schlüssels über.

[Rz 53] Der Inhaber eines privaten Schlüssels hat demnach eine umfassende Verfügungsgewalt über die damit verbundenen Werteinheiten, vergleichbar mit derjenigen, die einem Besitzer eines körperlichen Objekts zukommt. Somit ist die Tauglichkeit eines Blockchain Tokens als Sicherungsobjekt zur Begründung eines Escrow Agreements gegeben.[54]

c. Faktische Verfügungsmacht über die Tokens

[Rz 54] Neben der abstrakten Verfügungsgewalt, die Voraussetzung für die Tauglichkeit als Sicherungsobjekt ist, muss die Drittpartei auch in tatsächlicher Hinsicht die Verfügungsmacht am Objekt übertragen bekommen. Die Verfügungsmacht setzt gemäss der Lehre einen qualifizierten Besitz voraus, weshalb Situationen mit offener Besitzlage oder Besitzkonstituten nicht in Betracht kommen, da in ersterer auch Dritte die Sachherrschaft ergreifen können, und in zweiterer die Sache im unmittelbaren Besitz des Veräusserers verbleibt.[55] Der Schuldner darf keine ausschliessliche Gewalt über das Sicherungsobjekt mehr haben.[56]

[Rz 55] In Bezug auf Smart Contracts stellt sich die grundsätzliche Frage, ob die Drittpartei über Verfügungsmacht verfügt, wenn ein Smart Contract und nicht sie selbst die Tokens als Vermögenswerte übernimmt und bindet. Die Tokens als Daten befinden sich zu jeder Zeit dezentral auf der Blockchain verteilt und es findet kein Austausch zwischen dem potentiellen Einleger und dem Escrow-Agenten statt. Der dezentral verteilte Smart Contract mit den Vermögenswerten wird lediglich so programmiert, dass die Drittpartei entweder alleine oder zusammen mit einer anderen Person die von den Parteien vordefinierte Transaktion auslösen kann.

[Rz 56] Sofern die Drittpartei mittels eines privaten Schlüssels entscheidend auf die im Smart Contract gebundenen Vermögenswerte Einfluss nehmen kann, ist die notwendige tatsächliche Verfügungsmacht zu bejahen.

---

53 Möglich ist das Kopieren des Blockchain-Registers. Wenn die Währungseinheit aber im Sinne des Bitcoin Whitepapers definiert wird als Kette aus digitalen Signaturen («*chain of digital signatures*»), die sich auf der Gesamtheit der Protokolle befindet, so ergibt sich auch bei einer Kopie des Registers keine Replikation der Währungseinheit.

54 Sollte das Vorliegen eines Escrow Agreements dennoch verneint werden, so wären die von der Lehre und Rechtsprechung erarbeiteten Bestimmungen zumindest analog anwendbar.

55 Eisenhut (Fn 5), 116.

56 Eisenhut (Fn 5), 31.

d. Fazit

[Rz 57] Die Abwicklung der Transaktionen über einen Smart Contract steht der Qualifikation als Escrow Agreement nicht entgegen. Voraussetzung für die Bejahung des Escrow Agreements ist, dass die Drittpartei die tatsächliche Verfügungsmacht über die im Smart Contract gebundenen Tokens erlangt und der erforderliche Sicherungs- bzw. Durchsetzungszweck eines Hauptgeschäfts vorhanden ist.

3. Regulatorische Aspekte

a. Tokens als Einlage im Sinne des BankG beim Escrow-Agenten?

[Rz 58] Gemäss Art. 1 Abs. 2 des Bankengesetzes (BankG; SR 952.0) ist es natürlichen und juristischen Personen untersagt, ohne Bankenbewilligung gewerbsmässig Publikumseinlagen entgegenzunehmen. Die Begriffsbestimmung der (Publikums-)Einlage ist im Gesetz primär negativ umschrieben und daher wenig konkret. Als Publikumseinlagen gelten gemäss Art. 5 Abs. 1 der Bankenverordnung (BankV; SR 952.02) sämtliche Verbindlichkeiten gegenüber Kunden, unter Vorbehalt bestimmter, in Art. 5 Abs. 2 und 3 BankV aufgeführter Ausnahmen.

[Rz 59] Nicht als Einlagen gelten gemäss Art. 5 Abs. 3 Bst. a BankV Gelder, die eine Gegenleistung aus einem Vertrag auf Übertragung des Eigentums oder aus einem Dienstleistungsvertrag darstellen oder als Sicherheitsleistung übertragen werden. Hierbei handelt es sich gemäss dem FINMA Rundschreiben 2008/3 betreffend Publikumseinlagen bei Nichtbanken um «fremde Mittel ohne Darlehens- oder Hinterlegungscharakter».[57] Stünde jedoch ein solcher Hinterlegungscharakter im Vordergrund, wären die Vermögenswerte nicht direkt vom Ausnahmenkatalog der BankV umfasst.[58]

[Rz 60] Sofern die vom Smart Contract gehaltenen und dem Escrow-Agenten kontrollierten Gelder daher als Sicherheitsleistung zu erachten sind, fällt eine Qualifikation als Publikumseinlage ohne weitere Prüfung ausser Betracht. Falls im Einzelfall ein Hinterlegungscharakter vorhanden sein sollte, müsste die Aussonderbarkeit der Tokens im Konkurs gemäss Art. 242 des Bundesgesetzes über Schuldbetreibung und Konkurs (SchKG; SR 281.1) geprüft werden. Der Zweck des Verbots von Publikumseinnahmen liegt insbesondere im Schutz des Anlegers vor Verlusten im Falle des Konkurses der Gegenpartei. Vor diesem Hintergrund ist die Qualifikation eines übertragenen Vermögenswertes als Einlage dann nicht angezeigt, wenn dieser im Konkurs des Empfängers nicht in die Konkursmasse fallen würde.[59] Somit ist relevant, inwiefern an Tokens als Daten trotz mangelnder Körperlichkeit Eigentum i.S.v. Art. 641 ZGB begründet werden kann.

[Rz 61] Die generelle Sachqualifikation von Kryptowährungen und anderen Blockchain Tokens ist mangels Körperlichkeit umstritten und bedarf noch einer vertieften Auseinandersetzung.[60] Die FINMA hat, nach Einholen mehrerer unabhängiger Gutachten aus der Lehre und Praxis, die Aussonderungsmöglichkeit von Bitcoins im Konkurs bei der Prüfung der Dienstleistung eines Wallet Providers mit Verweis auf die funktionale Ausrichtung des Sachbegriffs u.E. zu Recht bejaht.

---

57 FINMA Rundschreiben 2008/3 zu Publikumseinlagen bei Nichtbanken, Rz. 11 f.

58 Florian Schönknecht, Der Einlagebegriff nach Bankengesetz, GesKR 3/2016, 301.

59 Schönknecht (Fn 58), 301.

60 Für die Meinungen in der Lehre vgl. Fn 52.

Da die in einem Smart Contract gehaltenen Kryptowährungen gerade nicht mit anderen Kryptowährungen (z.B. des Escrow-Agenten) vermengt werden, ist deren Möglichkeit zur Segregation zudem technisch sichergestellt. Entsprechend kann auch aus dieser Perspektive die Anwendung des Bankengesetzes ausgeschlossen werden.

[Rz 62] Eine Unterstellung unter das BankG ist bei smart-contract-basierten Escrow-Konstellationen daher zu verneinen.

b. Unterstellung des Escrow-Agenten unter das GwG?

[Rz 63] Ein berufsmässiger Escrow-Agent ist dem Geldwäschereigesetz (GwG; SR 955.0) grundsätzlich dann unterstellt, wenn mit der Abwicklung des Escrow Agreements die Verfügungsbefugnis über fremde Vermögenswerte einhergeht. Gemäss dem FINMA-Rundschreiben 2011/1 zur Tätigkeit als Finanzintermediär nach GwG liege eine Dienstleistung für den Zahlungsverkehr vor, wenn der Finanzintermediär im Auftrag seiner Vertragspartei «liquide Finanzwerte an eine Drittperson überweist und dabei diese Werte physisch in Besitz nimmt, sie sich auf einem eigenen Konto gutschreiben lässt oder die Überweisung der Werte im Namen und Auftrag der Vertragspartei anordnet».[61] Zudem seien auch Personen, die für einen Auftraggeber «Buchgeldzahlungen nach den Weisungen desselben über ein sog. Durchlaufkonto an eine begünstigte Person weiterleiten» dem GwG unterstellt, da auch in solchen Fällen eine Verfügungsmacht über fremde Vermögenswerte vorhanden sei.[62]

[Rz 64] Voraussetzung für eine Unterstellung unter das GwG ist zunächst die Liquidität des durch den Smart Contract gebundenen Tokens. Falls es sich um einen nicht handelbaren Token handelt, fällt eine Anwendung des GwG ausser Betracht. Wird aber, wie in den obigen Beispielen, die Ethereum Blockchain und der Ether Token verwendet, so ist wohl von einem währungsähnlichen Token auszugehen,[63] der die notwendige Liquidität aufweist. Das tägliche Handelsvolumen des Ethers bewegte sich zwischen Juli und Oktober 2017 zwischen rund CHF 200 Millionen und bis zu über CHF 2.6 Milliarden.[64] Aufgrund des währungsähnlichen Charakters von Ether ist auch von einem Finanzgeschäft und nicht etwa von einem Handelsgeschäft, wie beispielsweise beim physischen Handel von Rohwaren, auszugehen.[65]

[Rz 65] Weiter muss einem Escrow-Agenten Verfügungsmacht über fremde Tokens auf einem Smart Contract zukommen. Gemäss den oben beschriebenen Varianten ist daher wie folgt zu differenzieren:

- Hat der Escrow-Agent eine umfassende und alleinige Verfügungsmöglichkeit über die im Smart Contract gehaltenen Vermögenswerte, so liegt bei einer berufsmässigen Ausübung grundsätzlich eine Dienstleistung für den Zahlungsverkehr i.S.v. Art. 4 der Geldwäschereiverordnung (GwV; SR 955.01) vor. Die umfassende Verfügungsmöglichkeit bedingt, dass der Escrow-Agent die Vermögenswerte faktisch frei transferieren kann, analog zur Situation bei Bar- und Buchgeld.

---

61 FINMA-Rundschreiben 2011/1 zur Tätigkeit als Finanzintermediär nach GwG, Rz. 58.

62 FINMA-Rundschreiben 2011/1 (Fn 62), Rz. 58.

63 Vgl. entsprechende Ausführungen in Ziff. 3.a. im Zusammenhang mit der Bankengesetzgebung.

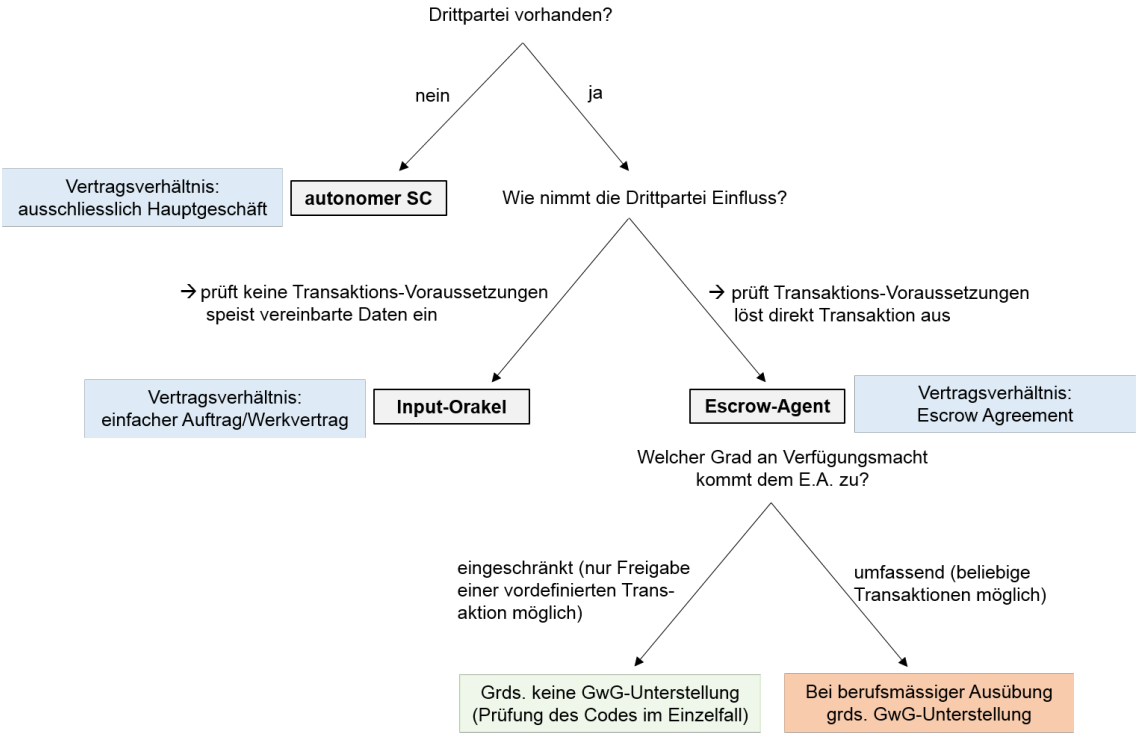
64 https://coinmarketcap.com/.

65 Vgl. betreffend Rohwaren als Handelsgeschäft: Christoph K. Graber, GwG-Kommentar, 2. Aufl. 2013, N 18 zu Art. 2.

- Genauer zu betrachten sind diejenigen Fälle, in denen dem Escrow-Agenten nur eine eingeschränkte Verfügungsmacht über die Vermögenswerte zukommt. Dies ist beispielsweise der Fall, wenn er ausschliesslich eine im Voraus programmierte Transaktion an einen spezifischen, unabänderbaren Empfänger mittels Nutzung seines privaten Schlüssels freigeben kann. Die Überweisung wird dann von der Partei des Hauptgeschäfts direkt im Smart Contract implementiert und vom dezentralen Blockchain-System ausgeführt. Die Vermögenswerte werden daher, im Wortlaut des GwG, weder angenommen oder aufbewahrt, noch hilft der Escrow-Agent bei der Übertragung. Im Gegensatz zur obigen Situation bei einer umfassenden Verfügungsmöglichkeit überweist der Escrow-Agent keinen Vermögenswert und gibt auch keine Überweisung in Auftrag. Vielmehr verzögert er lediglich die Ausführung der bereits erstellten und nicht von ihm durchgeführten Überweisung. Aus unserer Sicht handelt es sich daher im Falle einer solchen eingeschränkten Verfügungsmacht noch nicht um eine Tätigkeit als Finanzintermediär i.S.v. Art. 2 Abs. 3 GwG. Nichtsdestotrotz wird in diesen Fällen eine genaue Einzelfallprüfung der im Smart Contract Code implementierten Verfügungsmöglichkeiten des Escrow-Agenten unabdingbar sein.

VII. Gesamtüberblick

[Rz 66] Zusammenfassend lassen sich folgende Varianten zur Nutzung eines Smart Contracts im Rahmen einer Forderungssicherung sowie der Durchsetzung eines Hauptgeschäfts festhalten:



Grafik 4: Übersicht Varianten

VIII. Fazit

[Rz 67] Smart Contracts ermöglichen es, Vermögenswerte dezentral und ohne Intermediär sicher zu halten und gezielt die Bedingungen für Transaktionen zu programmieren. Wie dargestellt wurde, lassen sich Smart Contracts dadurch vielseitig zur Abwicklung von Escrow-Verhältnissen nutzen. Je nach Konstellation und Art der transaktionsauslösenden Bedingungen kommen Smart Contracts ohne Drittpartei oder mit Drittpartei in Betracht. Bei letzteren lassen sich wiederum Situationen unterscheiden, in denen ein «klassischer» Escrow-Agent die Transaktion gezielt auslösen kann, und solche, bei denen die Drittpartei lediglich über ein Orakel Daten in den Smart Contract einspeist und dieser selbst gemäss den vordefinierten Bedingungen reagiert. Je nach Ausgestaltung und Nutzung des Smart Contracts unterscheiden sich die Vertragsverhältnisse und die damit verbundenen Rechte und (insbesondere Sorgfalts-)Pflichten deutlich.

[Rz 68] Nach wie vor bestehen im Zusammenhang mit Smart Contracts einige offene rechtliche Fragen. Da Smart Contracts das Potenzial bieten, Abwicklungen intermediärlos, effizienter und günstiger durchzuführen, werden sie in Zukunft vielseitig genutzt werden. Daher ist es bereits jetzt sinnvoll, sich den Konzepten, technischen Grundlagen und rechtlichen Fragen im Zusammenhang mit Smart Contracts vertieft zu widmen.

Andreas Glarner, Dr. iur., LL.M., Legal Partner bei MME Legal | Tax | Compliance.

Stephan D. Meyer, MLaw, LL.M., Doktorand an der Universität Zürich, Vollzeit-Mitarbeiter in einem interdisziplinären SNF-Projekt (Nr. 10001A_162442) zur Regulierung virtueller Währungen an der ZHAW School of Management and Law und Mitarbeiter im Crypto-Team von MME Legal | Tax | Compliance.