www.jusletter-it.eu

Luca Schmid

ChainLink und Smart Contracts

Anwendbarkeit im Schweizer Kaufvertragsrecht

ChainLink ist eine Plattform, die eine Verbindung zwischen Blockchain-Technologien und der realen Welt herstellt. In dieser Arbeit wird die Technologie eines Start Ups beleuchtet, auf die sogar Google in Zukunft setzen wird. Zudem wird die Umsetzung anhand möglicher Anwendungsbeispiele im Schweizer Kaufvertragsrecht geprüft.

Beitragsart: Blockchain
Region: Schweiz
Rechtsgebiete: Blockchain

Zitiervorschlag: Luca Schmid, ChainLink und Smart Contracts, in: Jusletter IT 12. November 2020

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1. Einleitung

[1] *Of the many diverse and fascinating challenges we face today, the most intense and important is how to understand and shape the new technology revolution.*[1]

[2] Zu dieser neuen technologischen Revolution gehört für Schwab auch die Blockchaintechnologie und Smart Contracts.[2] Beide Begriffe werden häufig diskutiert, jedoch ist man sich uneinig, welchen Einfluss diese Technologien auf unsere Zukunft haben werden.[3] Für Mielke & Wolff ist der Erfolg eines Smart Contracts von der Möglichkeit abhängig, rechtliche Zusammenhänge auf die Ebene der Programmierung zu bringen.[4] Unabdingbar ist dabei die Fähigkeit eines Smart Contracts, Daten aus unserer real existierenden Welt zu verarbeiten. Mit dem Geschäftsmodell von ChainLink wird das Einspeisen von Daten in Smart Contracts grundlegend revolutioniert.[5]

[3] Diese Arbeit widmet sich der Technologie von Smart Contracts i.V.m. der Datenlösung von ChainLink. Dem Leser sollen die technischen Grundlagen sowie deren Auswirkungen in der Praxis nähergebracht werden. In einem ersten Teil wird die Technologie hinter ChainLink und einem Smart Contract beschrieben. Anschliessend wird in einem zweiten Teil die Frage geklärt, welche technischen und rechtlichen Auswirkungen ein Kauf i.S. des Privatrechts mittels eines Smart Contracts hat. Dabei wird explizit auf die Beziehungen zwischen Unternehmen und Konsumenten eingegangen, wobei der Bezug zur Umsetzung nicht zu kurz kommen soll. Mit Abläufen, Beispielen und Programmcode wird veranschaulicht, welche technischen Voraussetzungen nötig sind und wie sich das Erstellen eines Smart Contracts gestaltet.

2. Smart Contracts

[4] Um die Funktion eines Smart Contracts verstehen zu können, ist es sinnvoll, die Funktionsweise einer Blockchain einzuführen. Eine Blockchain ist eine softwarebasierte Technologie, die jedem zugänglich ist und die alle in ihr ausgeführten Transaktionen auf dezentralen Datenbanken dokumentiert.[6] Alle Transaktionen werden wie in einem Logbuch chronologisch erfasst. Als

1 Schwab, 1.

2 Schwab, 155.

3 Mielke/Wolff, 2.

4 Mielke/Wolff, 8.

5 Ellis/Juels/Nazarov, 8.

6 Essebier/Wyss, 7.

einfaches Beispiel kann man sich eine Gruppe von Personen vorstellen, die alle ein Telefonbuch besitzen. Lernt eine Person aus der Gruppe eine neue Person ausserhalb dieser Gruppe kennen und notiert deren Nummer im eigenen Telefonbuch, wird diese Nummer automatisch auch in alle anderen Telefonbücher übernommen. Die Daten, die in einer Blockchain erfasst werden, sind über einzelne Blöcke miteinander verknüpft.[7] Der grosse Vorteil einer solchen Technologie ist, dass eine Transaktion, die einmal durchgeführt wurde, nur noch schwer abzuändern ist.

[5] Das Benutzen einer Blockchain setzt ein Benutzerkonto voraus, bei dem jeder Nutzer über individuelle digitale Signaturen verfügt.[8] Um einen Datensatz in die Blockchain aufzunehmen, müssen zwei Kriterien erfüllt sein. Erstens muss der Datensatz eine Signatur haben, welche ihn verifiziert. Zweitens muss er verschlüsselt werden. Dem Datensatz wird in einem ersten Schritt jeweils über das Nutzerkonto eine Signatur verliehen, welche aus einem «private key» und einem «public key» besteht. Anschliessend wird jedes Datenpaket in der Blockchain mit einer Hashfunktion verschlüsselt. D.h. es wird eine individuelle Zahlenfolge für einen beliebigen Datensatz erstellt. Die Entschlüsselung dieser Zahlenfolge ist nahezu unmöglich. Eine Hashfunktion soll sicherstellen, dass jeder Datensatz wirklich nur einmal aufgeführt wird und ist eine Art individueller Fingerabdruck für die Transaktion. Die Daten werden nun in chronologischer Reihenfolge in den einzelnen Blöcken gespeichert, welche durch die Hashwerte verbunden sind. Jeder Block enthält eine Kopie des vorhergehenden Blocks. Um eine Änderung eines einzelnen Datensatzes durchführen zu können, muss jeder einzelne Block verändert werden. Einen einzelnen Block nachträglich noch abzuändern, wird durch diesen Vorgang nahezu verunmöglicht.

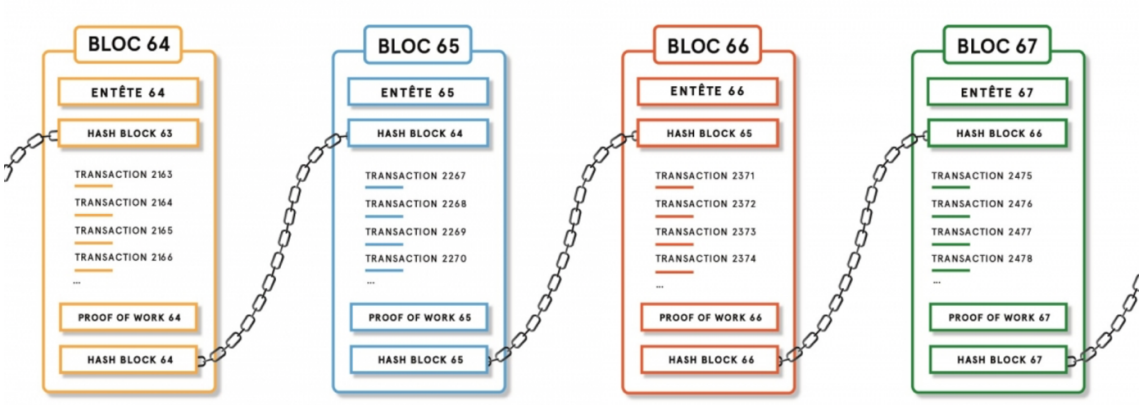

Abbildung 1: Aufbau einer Blockchain (Block Builder, 1.)

[6] Die Kopien der einzelnen Datenketten werden auf allen Rechnern des Netzwerks verteilt und laufend aktualisiert.[9] Gibt es in den einzelnen Blöcken jeweils falsche Angaben, die nicht mit den Daten in den anderen Blöcken übereinstimmen, werden diese gelöscht.

[7] Eine Blockchain bildet die Grundlage für einen Smart Contract. Bei einem Smart Contract handelt es sich um einen Programmcode oder eine Software, die in Abhängigkeit von zu de-

7 Dies erklärt auch den Namen der Technologie.

8 Essebier/Wyss, 10.

9 In diesem Zusammenhang wird auch von einer «distributed ledger technology» gesprochen.

finierenden Ereignissen Prozesse auslöst.[10] Der wortwörtliche Begriff Smart Contract erscheint bei seiner Übersetzung, hinsichtlich dessen Funktion, irreführend. Der Begriff «Contract» wird normalerweise nicht im rechtlichen Sinne verstanden, d.h. als Quelle einer Obligation. Vielmehr wird damit gemeint, dass der Vertrag einen Vorgang autonom abwickeln kann.[11] Vertragsbestimmungen können direkt im Code abgebildet werden, wobei die Vertragsregeln von einem Computer autonom ausgeführt werden.[12] Vorausgesetzt wird, dass das Computerprogramm automatisch prüfen kann, wann eine Vertragsbedingung erfüllt wurde. Dafür muss auf Daten ausserhalb der Blockchain zugegriffen werden können. Um an externe Daten zu gelangen, werden häufig Orakel eingesetzt. Ein Orakel kann eine automatisierte Dateneingabe oder auch eine Dateneingabe einer unabhängigen dritten Quelle sein.[13] Auch bei ChainLink handelt es sich um einen solchen Orakeleservice.

[8] Die Basis eines Smart Contracts bildet der Quellcode. In diesem sind die Details der gewollten Transaktion gespeichert. Weiter hat jeder Nutzer ein «wallet». In diesem «wallet» werden analog zur Blockchain der «private key» und der «public key» gespeichert. Die Transaktionen der Nutzer werden bis zum Ausführen im «storage file» gespeichert. Wurde die Transaktion erfolgreich durchgeführt, wird sie im «register» abgelegt.

3. ChainLink

[9] Ein Smart Contract, basierend auf einem Code, der keine Informationen von der Aussenwelt erhält, ist in seiner Nutzung eingeschränkt. Vielmehr soll ein Smart Contract, wie ein herkömmlicher Vertrag, Gegebenheiten aus der realen Welt erfassen und rechtlich relevant regulieren. Hierfür braucht ein Smart Contract Zugang zu relevanten Daten. Will man in einem Smart Contract beispielsweise den Kauf einer Aktie zu einem bestimmten Kurs regeln, braucht der Contract Zugang zu börsenrelevanten Daten. Weiter soll es auch möglich sein, Zahlungen in verschiedenen Währungen abzuwickeln und übergreifende Verbindungen zwischen einzelnen Blockchains zu gewährleisten. ChainLink stellt in solchen Fällen mittels eines Oracleservices eine Lösung zur Verfügung. Das Ziel soll die Überbrückung von «on-chain» und «off-chain» Systemen sein.

10 Mielke/Wolff, 3.

11 Jaccard, 6 f.

12 Essebier/Wyss, 13.

13 Essebier/Wyss, 16.

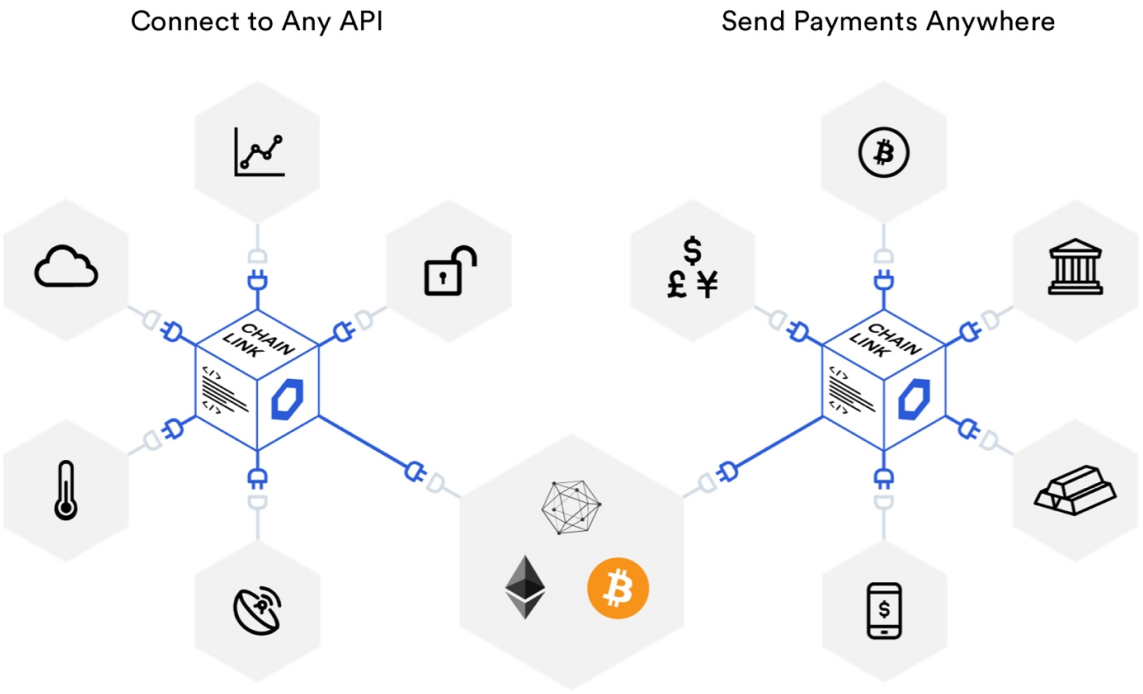

Abbildung 2: Möglichkeiten von ChainLink (SmartContract, 1.)

[10] Architektonisch ist das Programm von ChainLink in zwei Systeme gegliedert. Einerseits wird ein Teil des Programms in Blockchain selbst ausgeführt («on-chain»), andererseits werden externe Datenquellen hinzugezogen («off-chain»), welche dem Benutzer die benötigten Daten zur Verfügung stellen.[14]

[11] Im «on-chain» System kann der Benutzer in einem ersten Schritt seine gewünschten «oracles» auswählen, sprich sich für diejenigen Datenpakete entscheiden, die er in einen Smart Contract einspeisen will. Anschliessend werden die externen Datenpunkte durch die Software von ChainLink angefragt und bei Erhalten der Information direkt für den Nutzer aggregiert.

[12] Das «off-chain» System von ChainLink besteht aus «off-chain oracles nodes», die mit dem Ethereum Netzwerk verbunden sind. «off-chain nodes» sind dafür verantwortlich, dass die von den Benutzern angefragten Daten gesammelt werden. Nach dem Erhalten der Daten, werden sie in die Blockchain von ChainLink eingespeist und an die entsprechende «on-chain» Verknüpfung weitergeleitet. Als Kompensation für das Betreiben eines «off-chain oracle nodes» werden die Betreiber bezahlt. Dies geschieht anhand des LINK-Token von ChainLink.[15]

[13] Der Sicherheit von «oracles» kommt in der gesamten Technologie von Smart Contracts ein hoher Stellenwert zu. Denn sind die gelieferten Daten dieser «oracles» falsch, wird der Vertrag evtl. zu Gunsten einer falschen Person abgewickelt. ChainLink unterscheidet sich in diesem Punkt von anderen «oracle-Anbietern». ChainLink bietet einen dezentralisierten Ansatz an, bei dem die Datenquellen und die einzelnen «oracles» dezentralisiert sind. Sprich ein einzelnes «oracle» fordert Daten von dezentralisierten, unabhängigen Quellen an. Die Software von Chain-

14 Ellis/Juels/Nazarov, 7 f.

15 Ellis/Juels/Nazarov, 10.

Link selbst fordert wiederum Daten von dezentralisierten, unabhängigen «oracle-Anbietern» an. Die erhaltenen Daten werden, wie erwähnt, von ChainLink aggregiert und anschliessend dem Benutzer zur Verfügung gestellt.[16]

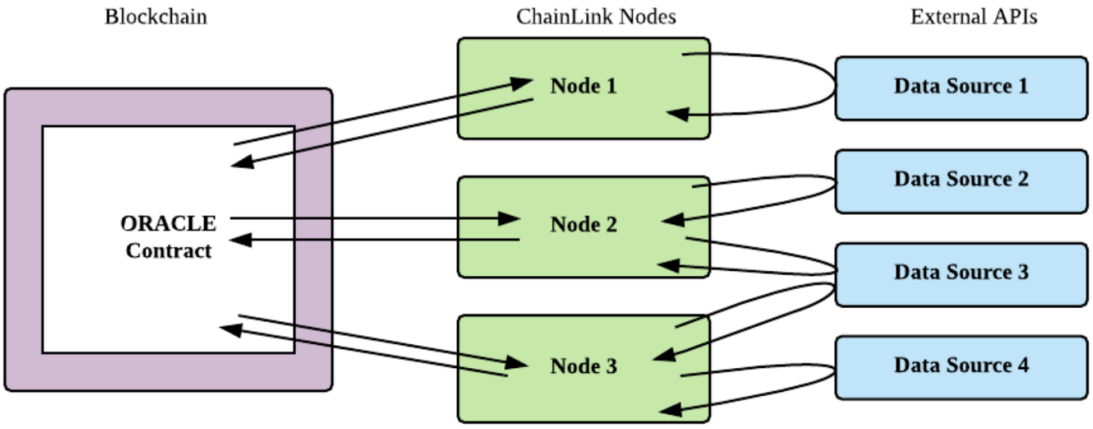

Abbildung 3: Interaktion zwischen Blockchain, ChainLink Nodes und externen Datenpunkten (Ellis/Juels/Nazarov, 12.)

[14] Das Aggregieren erfolgt entweder «on-chain» oder «off-chain», was billiger ist, da für jede Transaktion bezahlt werden muss. ChainLink bietet einen zusätzlichen Sicherheitsservice an. Dieser besteht aus vier Teilen: dem «Validation System», dem «Reputation System», dem «Certification System» und dem «Contract Upgrade Service».[17] Diese vier Teile überwachen die Richtigkeit der Transaktionen in der Blockchain selber und zeichnen das Verhalten der einzelnen «nodes» auf.

4. Anwendungsbeispiel im Schweizer Kaufvertragsrecht

[15] Das Wesen des Smart Contracts ist das Umverteilen von Vermögenswerten.[18] Das Kaufvertragsrecht bietet sich deshalb besonders gut für Anwendungsbeispiele an. Im folgenden Teil wird zuerst auf allgemeine Modalitäten des Kaufvertrags eingegangen. Danach wird ein Anwendungsbeispiel erwähnt, welches technisch und rechtlich analysiert wird.

4.1. Der Kaufvertrag

[16] Der Kaufvertrag erfasst alle Verträge, die sich auf den Austausch einer Sache oder eines Rechts gegen eine monetäre Leistung beziehen.[19] Gemäss Art. 184 Abs. 2 OR müssen die Leistungen von Gläubiger und Schuldner Zug-um-Zug erfüllt werden, wobei man sich gemäss Art. 184

16 Steven *et al.*, 12.

17 Ellis/Juels/Nazarov, 12.

18 Weber, 5.

19 BSK OR I-Koller, N. 1 f.

Abs. 3 OR mindestens über den Preis einigen muss. Kaufverträge können nach den verschiedenen Arten des Kaufs unterschieden werden. In diesem Zusammenhang wird v.a. auf die Unterscheidung von Fahrniskauf (Art. 187 ff. OR) und Grundstückkauf (Art. 216 ff. OR) eingegangen. Ein real existierender Gegenstand kann in einem «distributed ledger» mittels eines Tokens abgebildet werden. Durch die automatisch veränderte Zuordnung des Smart Contracts lassen sich diese Tokens übertragen, wobei der neue Besitzer durch den Token Zugriff auf den Gegenstand in der realen Welt erhält.[20] Diese Vorgehensweise würde auch beim Fahrniskauf zur Anwendung kommen.

[17] Die Abwicklung eines Grundstückkaufs ausschliesslich auf Basis eines Smart Contracts erweist sich als schwierig, denn die Gültigkeit von Kaufverträgen, die ein Grundstück zum Gegenstand haben, bedürfen der öffentlichen Beurkundung. Ein Smart Contract entspricht nicht den Anforderungen der öffentlichen Beurkundung gemäss Art. 216 OR, weshalb bei einem solchen Vertrag die beschriebene Technologie nur beschränkt Anwendung findet.[21] Der Smart Contract könnte in Verbindung mit einem Grundstückkauf lediglich als Grundlage des Verpflichtungsgeschäfts dienen. Zusätzlich ist die Idee, beispielsweise ein Grundbuchregister in einer Blockchain abzuspeichern, nicht abwegig, vergleicht man das Fortschreiten der Blockchaintechnologie in der Verwaltung in anderen Staaten.[22] In einem solchen Fall wäre es möglich, die Daten aus dem Grundbuchregister direkt in den Smart Contract einzuspeisen.

[18] Zu den Pflichten des Verkäufers gehören die Übergabe des Kaufgegenstands und das Verschaffen des Gewahrsams.[23] Beim Grundstückkauf muss der Verkäufer zusätzlich die Grundbuchanmeldung abgeben und alle ihr entgegenstehenden Hindernisse beseitigen. Zu den Pflichten des Käufers gehört die Zahlung des Kaufpreises in Form von Geld.[24] Den Käufer trifft auch die Beweislast für die Zahlung des Kaufpreises.[25]

[19] Bei Verträgen zwischen Unternehmen und Konsumenten kommen häufig Allgemeine Geschäftsbestimmungen zum Einsatz. AGB sind «Vertragsbestimmungen, welche die Verwenderin oder eine Dritte hinsichtlich des Abschlusses einer Vielzahl von Verträgen vorformuliert und welche die Parteien nicht individuell verhandeln».[26] Die Grundlage für den Einsatz von AGB ist ein Rationalisierungsgedanke, der den Umgang mit vielen Kunden effizient gestalten soll. In der Schweiz besteht keine Regulierung, welche der AGB-Problematik umfassend Rechnung trägt.[27] Die Rechtsprechung beschränkt sich auf eine Inhaltskontrolle, welche anhand einer Geltungs- und Auslegungskontrolle durchgeführt wird.[28] Hier soll nicht weiter auf die rechtlichen Aspekte von AGB eingegangen werden. Wichtig ist jedoch, dass in diesem Zusammenhang das Anwendungspotential von Smart Contracts hoch ist und noch keine zureichenden Regulierungsbestimmungen bestehen.

20 Weber, 8 f.

21 Jaccard, 21.

22 Dezentrale Verwaltung, 1.

23 BSK OR I-Koller, N 5.

24 BSK OR I-Koller, N. 7.

25 BSK OR I-Koller, N. 10 f.

26 BGE 4C.282/2003 E. 3.1.

27 Huguenin, N. 609.

28 Huguenin, N. 611.

4.2. Anwendungsbeispiele

4.2.1. Aktienkauf

```
Kaufvertrag(rightA=«100 Aktie à 10 CHF»,
rightB=«10’000 CHF»,
p = «July 2020») =
when withinPeriod(p)
to Holder rightA   with   to Counterparty rightB
then terminate
```

Abbildung 4: Codebeispiel (Szabo, 5.)

[20] An diesem Beispiel soll die Funktionsweise eines Smart Contracts veranschaulicht werden. Die erste Zeile beschreibt den Namen der Klausel oder die Art des Vertrags. Hierbei handelt es sich um einen Kaufvertrag, bei dem 100 Aktien zu einem Nennwert von 10 CHF je Aktie verkauft werden. Die Aktien sollen im Juli 2020 gekauft werden, wenn der Kurswert der Aktien 10’000 CHF beträgt. Zeile vier definiert den Zeitpunkt der Übergabe. «right A» und «right B» beschreiben Gläubiger und Schuldner. «then terminate», in der letzten Zeile, stellt sicher, dass alle Rechte nach Abschluss dieses Vertrags auch wieder gelöscht werden.

[21] Der Quellcode verfügt momentan noch über keine Schnittstellen zur Aussenwelt. Um den Blockchain-basierten Code mit externen Daten zu verbinden, wäre der Einsatz eines Orakels notwendig. Dieses könnte Daten wie den aktuellen Börsenkurs, den Wert von Währungen oder das aktuelle Datum dem Smart Contract zur Verfügung stellen. Da Aktien an sich externe Daten darstellen, müssen diese in Form von Tokens in die Blockchain übertragen werden. Wird im Juli 2020 der Wert von 10’000 CHF des Aktienpakets erreicht, wechseln diese Tokens automatisch den Besitzer und das Geld wird transferiert. Anschliessend wird die Transaktion durch «then terminate» in das «register» verschoben, wo sie weiterhin für alle Parteien einsehbar ist. An diesem Beispiel wird ersichtlich, wie wichtig die Zufuhr von unabhängigen Daten für einen Smart Contract ist. Werden die Daten i.c. lediglich von einem beliebigen Orakel zur Verfügung gestellt, wird das gesamte technologische Konstrukt fehleranfällig und die eigentlichen Vorteile eines Smart Contracts gehen verloren.

[22] Analysiert man Beispiele, bei denen Unternehmen mit Konsumenten interagieren, ist es lohnenswert, sich gewisse betriebswirtschaftliche Gegebenheiten vor Augen zu führen. Aus Sicht des Unternehmens wird bei Konsumentenverträgen eine hohe Kundenfluktuation angestrebt.[29] Hinzu kommt, dass der Gewinn für solche Unternehmen die oberste Priorität darstellt. Dabei soll der Kunde die gängigsten Zahlungsmethoden benutzen. Weiter müssen – um allfällige Rechtsstreitigkeiten zu vermeiden – die Datenschutzrechte der Kunden gewahrt werden.

[29] Heinemann, 3.

[23] In der Praxis gibt es auch explizit Beispiele zur Anwendung der Technologie von ChainLink. Google LLC kündigte 2019 öffentlich die Zusammenarbeit mit ChainLink an. Dabei können über Google-Clouddienste Daten via ChainLink in einen Smart Contract eingespeist werden.[30] Des Weiteren wird ChainLink als Vorreiter im Bereich der europäischen PSD2 Bankenregulierung gehandelt.[31] Bei PSD2 handelt es sich um einen Trend in der Bankenregulierung, qualifizierten Dritten Einblicke in die Transaktionen von Kunden zu gewähren. Dies würde v.a. die Sicherheit und die Kostenoptimierung im Bankensektor vorantreiben. Durch die hohen Sicherheitsstandards und die dezentralen Orakel könnte ChainLink in Zukunft auch in diesem Bereich Daten den verschiedenen Blockchains zur Verfügung stellen.

4.2.2. Technische Würdigung

[24] Analog zum Einsatz von AGB sind Smart Contracts für Unternehmen effizient. Einmal programmiert, können sie beliebig vervielfältigt werden. Der Effizienzgedanke zieht sich sogar noch weiter, denn ist ein Smart Contract richtig programmiert und widerspiegelt er den Willen der Parteien, fallen keine Kosten für die Rechtsdurchsetzung an. Da der Vertrag autonom ausgeführt wird, werden beide Parteien daran gehindert, den Vertrag zu manipulieren.

[25] Obwohl in der Theorie ein Smart Contract beliebig oft vervielfältigt werden kann, treten Probleme im Bereich der Skalierbarkeit auf.[32] Sollen Smart Contracts global und auf Grundlage des gleichen Systems verwendet werden, führt dies zu Engpässen in der Serverkapazität. Mit der aktuellen Ausgestaltung von Smart Contracts i.V.m. ChainLink wäre die Bewältigung von sehr hohen Transaktionsmengen nicht möglich. Zukünftige technologische Entwicklungen könnten dieses Problem jedoch beheben.

[26] Wird der Quellcode eines Smart Contracts richtig programmiert und valide mit den jeweiligen Orakeln verbunden, führt dies zu seiner Unveränderbarkeit. Da sämtliche Nutzer eine Kopie des geschlossenen Smart Contracts besitzen, müsste dieser in jedem «ledger» abgeändert werden, um den Vertrag erfolgreich manipulieren zu können.[33] Die dezentrale Speicherung der Daten schafft in diesem Sinne auch Unabhängigkeit. Personen wären im besten Fall nicht mehr auf Anwälte oder sonstige rechtliche Massnahmen angewiesen, da sich der Vertrag mit vollkommener Wahrscheinlichkeit selbst durchsetzt. Es wird eine vergleichbare Unabhängigkeit zu Bitcoin geschaffen, einer Währung, die nicht mehr von Zentralbanken eines Landes abhängig ist, sondern durch das Kollektiv einer Blockchain reguliert wird.

[27] Schliesslich steht und fällt die Anwendung eines Smart Contracts mit dessen Konnektivität. Je mehr Lebenssachverhalte in einer Blockchain durch Token oder andere Daten abgebildet werden können, desto eher breitet sich dessen Anwendbarkeit aus. Dabei profitieren v.a. Unternehmen, die bis zu diesem Zeitpunkt im Digitalisierungsprozess schon weit fortgeschritten sind. Lässt man als Konsument beispielsweise eine Bestellung über die Schweizer Post abwickeln, kann jeder Lieferungsschritt nachverfolgt werden. Würde man die Datenschnittstelle bei der Post ausbauen, könnte man das Erhalten und Bezahlen des Gegenstands so takten, dass beides im gleichen Zeitpunkt passiert.

---

30 Allen, 1.

31 Botta *et al.*, 1.

32 Goodaudience.

33 Essebier/Wyss, 40.

4.2.3. Rechtliche Würdigung

[28] Transaktionen mittels eines Smart Contracts enthalten stets auch rechtliche Vorteile. Durch die Selbstdurchsetzung und Unveränderbarkeit entsteht Rechtssicherheit. Die versprochene Leistung kann nicht mehr grundlos verweigert werden.[34] Im Sinne des römischen Rechts kommt diese Tatsache dem Grundsatz «pacta sunt servanda» zu Gute.[35] Ist der Smart Contract in der entsprechenden Blockchain programmiert, kann von dem zuvor bestimmten Code nicht mehr abgewichen werden. Dies kann unter Umständen auch zu stossenden Resultaten führe, da ggf. der Vertrag durch veränderte, unvorhergesehene Umstände nicht mehr im Sinne der «clausula rebus sic stantibus» angepasst werden kann.[36] Zusätzlich müssen Vertragsnormen in einem Smart Contract nicht mehr ausgelegt werden. Nach dem Grundsatz «code is law» brauchen die einzelnen Kriterien des Quellcodes keine weitere Konkretisierung.[37]

[29] Ein Vertrag kommt gemäss Art. 1 Abs. 1 OR durch gegenseitig übereinstimmende Willensäusserung zustande. Der Vorgang der Willensäusserung kann nicht durch eine Maschine ersetzt werden.[38] Deshalb ist es wichtig, dass beide Parteien den Vertragsinhalt in den Grundzügen verstehen. Da Konsumenten und KMU die Technologie bis anhin noch nicht benutzen, kann darauf zurückgeführt werden, dass es noch keine benutzerfreundliche Schnittstelle gibt. Bei grösseren Unternehmen sind die Ressourcen vorhanden, genügend Wissen in diesen Bereichen zu mobilisieren. Ausserdem erscheint es als illusorisch zu fordern, ein Smart Contract müsse in eine natürliche Sprache übersetzt werden.[39]

[30] Tritt nach Vertragsabschluss eine Leistungsstörung ein, sei sie technischer oder rechtlicher Natur, kann diese nicht direkt im Smart Contract antizipiert werden. Aus dem obigen Programmcode wird ersichtlich, dass mit der Zeile «then terminate» der Smart Contract im «register» gespeichert wird und eine Veränderung des Codes nun unmöglich geworden ist. Eine unabhängige Schiedsstelle oder ein Gericht müssten in solchen Fällen zur Hilfe gezogen werden, um den Konflikt zu lösen.

[31] Wird ein Smart Contract i.S. einer AGB verwendet, verschlechtert sich dadurch die Stellung des Konsumenten. Nicht nur sind Konsumenten im Nachteil, was den Inhalt von vorformulierten AGB betrifft, sondern sind konkret auch mit einem Quellcode konfrontiert, den sie eventuell gar nicht lesen können. Ferner ist für den Konsumenten auch nur schwer ersichtlich, auf welchen Daten der Smart Contract basiert. In dieser Hinsicht stimme ich der Forderung nach einer standardisierten Beschreibungssprache der rechtlichen und technischen Dimension zu, die es den Benutzern auf beiden Seiten vereinfachen soll, den vorliegenden Vertrag zu verstehen.[40] Weiter müssten explizite Regelungen zum Konsumentenschutz ausgearbeitet werden, die den technischen Anforderungen entsprechen.

34 Essebier/Wyss, 36.

35 Weber, 22.

36 Weber, 22.

37 Gantner, 1 f.

38 Weber, 5.

39 Weber, 10.

40 Mielke/Wolff, 8.

5. Fazit

[32] In dieser Arbeit wurden zuerst Smart Contracts und ChainLink technisch untersucht. Danach wurde an einem Praxisbeispiel aus dem Kaufvertragsrecht aufgezeigt, welche technischen und rechtlichen Implikationen die Abwicklung eines solchen Vertrags hat.

[33] Aus dem technischen Teil wurde ersichtlich, dass die grundlegenden Abläufe eines Smart Contracts komplex sind und ohne die Vernetzung eines Orakel-Dienstleisters wie ChainLink kaum auskommen. Der zweite Teil wurde mit dem Quellcode eines Aktienkaufs eingeführt. Hier fällt auf, dass sich die Programmiersprache von Smart Contract zu Smart Contract unterscheiden kann. Die fehlenden Standards wurden auch bei der technischen Würdigung aufgegriffen. An dieser Stelle kann hervorgehoben werden, dass durch Smart Contracts Effizienzgewinne erwartet werden können, diese aber mehrheitlich Unternehmen zu Gute kommen, die im Digitalisierungsprozess fortgeschritten sind. Die rechtliche Würdigung beschäftigte sich unter anderem mit der Willensbildung der Vertragsparteien und den Leistungsstörungen. Dabei ist zu beachten, dass allfällige Leistungsstörungen nicht direkt im Smart Contract antizipiert werden können. Weiter ist es für die individuelle Willensbildung der Vertragspartei unabdingbar, den Vertrag in der vorliegenden Programmiersprache zu verstehen. Auch hier erscheinen grosse Unternehmen mit spezialisiertem Personal gegenüber dem Konsumenten im Vorteil. Deshalb scheint es auch hier angebracht, Regulierungen und einheitliche Standards einzuführen, um die technischen Effizienzgewinne und die Rechtssicherheit nutzen können.

[34] Weiterführende Forschung könnte im Bereich der Anbieter von Smart Contracts betrieben werden. Die Möglichkeit einer unkomplizierten Nutzung eines Smart Contracts würde das Potenzial der Technologie vervielfachen. Des Weiteren erscheint mir das Festlegen von technisch, wie auch rechtlich einheitlichen Begriffen bei Smart Contracts als unabdingbar.

[35] Die autonome Durchsetzbarkeit und die Unveränderbarkeit eines Smart Contracts haben das Potenzial, sich wiederholende Prozesse selbst zu erledigen. Es lässt sich jedoch nicht jedes Detail der Aussenwelt innerhalb einer Blockchain abbilden. Der Beruf des Anwalts wird weiterhin bestehen bleiben, sein Arbeitsumfeld wird sich jedoch drastisch ändern.

Luca Schmid ist Rechtsstudent an der Universität St. Gallen (HSG).