Digitales Vertragsmanagement

Smart Contracts – Was dahintersteckt

Mithilfe einer passenden Software kann man einen automatischen Vertragserfüllungsprozess ermöglichen, dieser wird Smart Contract genannt. Man kann diesen für vieles anwenden. Der Beitrag zeigt einen Überblick.

› Regula Heinzelmann

Ein Smart Contract ist ein auf der Technik der Blockchain basierendes Computerprogramm, das automatisch abläuft, sobald gewisse Bedingungen erfüllt sind. Die Postfinance schreibt darüber Folgendes: «Smart Contracts sind selbstausführende Programme, die auf einer Blockchain gespeichert werden und beim Erfüllen von vordefinierten Bedingungen eine oder mehrere Transaktionen oder Funktionen ausführen. Einmal ausgeführt, sind die Transaktionen rückverfolgbar und unwiderruflich.

Weiter sind die Bedingungen sowie die Funktionen jederzeit nachvollziehbar und transparent einsehbar. Dies ermöglicht vertrauenswürdige Transaktionen und Vereinbarungen zwischen verschiedenen Parteien, ohne die Notwendigkeit einer zentralen Instanz.»

Grundidee und Anwendung

Die Grundidee der Smart Contracts ist etwa 30 Jahre alt. Das Konzept der Smart Contracts wurde erstmals 1994 von Nick Szabo, einem amerikanischen Informatiker, entwickelt. Smart Contracts sind somit älter als der 2008 entstandene Bitcoin. Szabo definierte Smart Contracts als computergestützte Transaktionsprotokolle, welche die Bedingungen eines Vertrages ausführen. Inzwischen haben sich Software und KI natürlich sehr viel weiterentwickelt. 2018 publizierte der Bundesrat einen umfassenden Bericht über «Rechtliche Grundlagen für Distributed-Ledger-Technologie und Blockchain in der Schweiz».

kurz & bündig

- Ein Smart Contract ist ein auf der Technik der Blockchain basierendes Computerprogramm, das automatisch abläuft, sobald gewisse Bedingungen erfüllt sind.
- Der Vertrag kommt zustande, indem die Vertragsparteien ihre Willensäusserungen mittels Technik kundtun.
- Bei langfristigen Verbindungen mit Smart Contracts können Anpassungen nötig sein, dazu benützt man Blockchain-Orakel. Das sind Drittanbieter-Dienste, die Smart Contracts mit externen Informationen versorgen, was bei Blockchains und Smart Contracts normalerweise nicht möglich ist.

Die Anwendungsbereiche für Smart Contracts sind vielfältig. Überall, wo mehr als zwei Parteien involviert sind, um eine Transaktion abzuwickeln, können Smart Contracts eine effiziente und transparente Möglichkeit bieten. Bekannte Anwendungsgebiete sind zum Beispiel Börsen im Bereich DeFi (Decentralized Finance), Juweliere bei der transparenten Rückverfolgung von Edelsteinen oder Pilotprojekte im Lieferkettenmanagement. Man kann mit der Technik aber auch Publikumsverträge abschliessen für Waren- und Dienstleistungsangebote. Man unterscheidet dabei zwischen Off- und On-Chain-Verträgen.

Ein rein technischer Vorgang

Der Begriff «Contract» (Vertrag) gilt aus juristischer Sicht im Zusammenhang von sogenannten «Smart Contracts» als irreführend, weil es sich dabei nicht um einen obligationenrechtlichen Vertrag handelt. Es ist ein Software-Code, der dazu dient, Funktionen oder Aktionen auszuführen und zu protokollieren. Wenn eine nachprüfbare Bedingung erfüllt ist, vollzieht die Software eine bestimmte Reaktion, das ist ein rein technischer und kein juristischer Vorgang.

Der Vertrag kommt zustande durch die übereinstimmenden Willensäusserungen der Personen, die die Technik benützen. Dadurch werden die technischen Vorgänge juristisch verbindlich, also die Bestellung im Internet, Bestätigung des Anbieters, Zuweisungen von Token usw.

Die wesentliche Einschränkung von Smart Contracts besteht darin, dass man sie nicht mit Daten und Systemen ausserhalb ihres Blockchain-Kontexts verbinden kann. Diese Begrenzung ist auf die Natur der Blockchains zurückzuführen, bei der das gleiche Ergebnis bei gleicher Eingabe erzielt wird. Dies ist wichtig, um einen Konsens zu erreichen und ein grundlegender Aspekt der Blockchains.

Eine erwünschte Folge ist, dass beim Smart Contract Auseinandersetzungen von Parteien vermieden werden, weil die Technik genau vorprogrammiert ist, die Vertragserfüllung nicht vom individuellen Verhalten der Parteien abhängig ist und keine Diskussionen über den Vertragsinhalt notwendig sind. Problematisch wird es natürlich dann, wenn technische Pannen passieren und noch schlimmer, wenn Dritte unrechtmässig das System stören. Angemessener Schutz wird auch für Smart-Contract-Systeme empfohlen.

Die Blockchain-Orakel

Bei langfristigen Verbindungen mit Smart Contracts können Anpassungen nötig sein, zum Beispiel wegen sich verändernder Rohstoffpreise. Die Lösung für dieses Problem sind Blockchain-Orakel. Blockchain-Orakel sind Drittanbieter-Dienste, die Smart Contracts mit externen Informationen versorgen, was bei Blockchains und Smart Contracts normalerweise nicht möglich ist. Für viele vertragliche Vereinbarungen ist es jedoch notwendig, relevante Informationen von Dritten zu bekommen, um die Vereinbarung auszuführen. Die Orakel widersprechen dem Prinzip, dass in Abläufe auf der Blockchain nicht eingegriffen wird.

Blockchain-Orakel sind nicht die Datenquelle selbst, sondern die Funktion, die externe Datenquellen abfragt, überprüft und authentifiziert und dann diese Informationen weiterleitet, zum Beispiel Preisinformationen, die erfolgreiche Durchführung einer Transaktion, die von einem Sensor gemessene Temperatur oder die Dokumentation betreffend Übergabe der physischen Ware. Einige Orakel können auch Informationen nicht nur an Smart Contracts weiterleiten, sondern sie auch an externe Quellen zurücksenden.

Off- und On-Chain-Verträge

Beim Off-Chain-Vertrag schliessen die Parteien einen Vertrag im herkömmlichen juristischen Sinne ab, ohne dass dieser Vertragsschluss etwas mit der Blockchain zu tun hat. Das Computerprogramm wird erst im zweiten Schritt eingesetzt, um den Vertrag vollautomatisch abzuwickeln.

Beim Vertragsabschluss on chain besteht zuerst ein Smart Contract. Die Parteien schliessen in der Folge ihren Vertrag im juristischen Sinne mithilfe dieses Computerprogramms ab. Der Smart Contract dient nicht nur zur Durchführung, sondern auch bereits zum Abschluss des Vertrags. Stimmt eine Person den im Smart Contract enthaltenen Bedingungen zu, so entsteht ein Vertrag im juristischen Sinn (Art. 7 Abs. 3 OR).

Eine Partei kann diese Bedingungen zum Beispiel dadurch erfüllen, dass sie die im Smart Contract vorgesehene Summe eines Krypto-Assets an die angegebene Adresse überweist. Daraus kann man ableiten, dass die betreffende Person den im Smart Contract enthaltenen Antrag annimmt und die Bedingungen akzeptiert.

Ein Unternehmen kann auf einer Blockchain einen Smart Contract einrichten, der als automatische Verkaufsstelle funktioniert. Bietet der Smart Contract einer unbestimmten Anzahl von möglichen Kunden ein bestimmtes Produkt oder eine Dienstleistung an, so betrachten einige Juristen das als Einladung, eine Offerte zu stellen. Dann wäre die Überweisung des geforderten Betrags der Kryptowährung ein Antrag des Kunden und die Firma nimmt diesen an, indem sie einen Utility Token überweist. Der Smart Contract kann so programmiert sein, dass er die Anträge zusätzlicher Interessenten sofort ablehnt und die bereits bezahlte Kryptowährung auf das Konto des Senders zurücküberweist, sobald z.B. das Produkt ausverkauft ist.

Arten von Token

Nach dem Bericht des Bundesrates können Token individuell und sehr unterschiedlich ausgestaltet werden. Aus technischer Sicht kann ganz grundsätzlich zwischen Native und Non-Native Token unterschieden werden.

Native Token

Ein Native Token wird im Protokoll einer Blockchain implementiert und ist für deren Funktionieren zentral. Typischerweise wird das Validieren von Blöcken innerhalb einer Blockchain mit diesem Native Token entschädigt. Der Token ist damit ein wichtiger Bestandteil des Konsensmechanismus. Beispiele für Native Token sind etwa Bitcoin und Ether.

Non-Native Token

Non-Native Token werden demgegenüber nicht im Protokoll einer Blockchain selbst, sondern in einem darauf basierten Second-layer-Protokoll oder in einer Anwendung implementiert. Solche Token werden auf der zugrundeliegenden Blockchain erfasst und den jeweiligen Teilnehmern zugeordnet, sind aber nicht integraler Bestandteil dieser Blockchain selbst. Mit anderen Worten, die Blockchain funktioniert auch ohne diese Token.

Utility Token

Utility Token werden im Normalfall auf einer Blockchain erstellt und ausgegeben. Sie sind eine Form von Kryptowährung, die für den Zugang zu bestimmten Diensten oder Produkten in einem Blockchain-Netzwerk verwendet werden. Sie werden wie Gutscheine oder Eintrittskarten verwendet, um die Kunden zum Zugang zu bestimmten Funktionen oder Dienstleistungen in einem Blockchain-Netzwerk zu berechtigen. Es gibt jedoch auch einige Risiken und Herausforderungen im Zusammenhang mit Utility Tokens. Eine der grössten ist, dass es schwierig sein kann, den tatsächlichen Nutzen eines Utility Tokens zu bestimmen. Das kann dazu führen, dass Investoren oder Benutzer den Wert des Tokens nicht vollständig verstehen.

Security Token

Security Token gelten als Wertpapiere und unterliegen strengen regulatorischen Anforderungen. Sie dienen zur Darstellung des Eigentums an einem realen Vermögenswert, auch indem sie ihrem Inhaber Eigentumszugriff gewähren. Security-Token verbriefen Eigentum, Teileigentum oder Anteile an einem Vermögenswert oder Projekt, ähnlich wie herkömmliche Wertpapiere, zum Beispiel Aktien. Steigt die Unternehmensbewertung, steigt auch der Wert des Security Tokens. Unternehmen und Inhaber müssen dabei Regulierungen und Bundesgesetze einhalten, wie etwa den Howey-Test in den USA, der feststellt, ob ein Investitionsvertrag vorliegt und ob der Token für Akquisitionen mit erwarteter Rendite verwendet wird.

Token – juristische Bedeutung

Im Hinblick auf das Recht unterscheidet der Bericht des Bundesrates zwischen zwei Arten von Token:

- Token, die in erster Linie einen Wert innerhalb des Blockchain-Kontexts darstellen, zum Beispiel Kryptowährungen wie Bitcoin. In diesem Fall hat der Token selber einen Wert.
- Token, die ein ausserhalb der Blockchain bestehendes Recht (Forderung, Mitgliedschaft, dingliches Recht) abbilden und repräsentieren sollen. Nach dem Willen der Parteien repräsentiert der Token einen ausserhalb der Blockchain liegenden Wert oder verschafft Zugang zu einem solchen Wert.

Diese zwei zivilrechtlichen Kategorien stehen laut Bericht nicht in Widerspruch, sondern bilden die Grundlage zu der von der Finma vorgenommenen Unterscheidung in Zahlungs-, Nutzungs- und Anlage-Token. Diese Kategorisierung, welche auch von der Blockchain-Taskforce getragen wird, ist für die finanzmarktrechtliche Qualifikation der Token entscheidend. Aus zivilrechtlicher Sicht ist auch bei den Nutzungs-Token häufig von einer Forderung auszugehen. Wenn ein Token etwa Zugang zu einer Dienstleistung vermitteln soll, besteht darin die Abbildung eines werkvertraglichen oder auftragsähnlichen Anspruchs.

Zahlungs-Token beziehungsweise sogenannte Native Token, deren Wert sich auf Anwendungen in der Blockchain erschöpft, stellen nach der wohl herrschenden Ansicht rein faktische, immaterielle Vermögenswerte dar. Sie lassen sich keiner der Hauptkategorien des Zivilrechts zuordnen. Das Zivilrecht stellt für ihre Übertragung deshalb auch keine Anforderungen – und entsprechend keine Hindernisse – auf. In Bezug auf die Übertragung von Kryptowährungen (zum Beispiel Bitcoin, Ether) besteht deshalb kein Anpassungsbedarf im Zivilrecht.

Ob mit der Verschiebung von Token ganze Vertragsverhältnisse formlos übertragen werden können, ist nicht abschliessend geklärt und dürfte stark von der jeweiligen Ausgestaltung im Einzelfall abhängen.

Praxisbeispiel

Auch die Universität Luzern publizierte einen Bericht über Smart Contracts und Blockchains. Als Beispiel für eine prakti-

sche Anwendungsmöglichkeit nennt der Bericht den Gesundheitsbereich. Durch die automatische Abwicklung von Patientenrechnungen zwischen den Krankenkassen, Ärzten und den Patienten können Fehler reduziert und massive Kosteneinsparungen realisiert werden.

Diese Kosteneinsparungen kommen einerseits durch die Reduktion der Kontrollinstanzen und andererseits durch die Eliminierung der Leistungsbeurteilung zustande. Ganz unproblematisch sind solche automatischen Zahlungsabwicklungen aber gerade in diesem Bereich nicht. Die rechtlichen Aspekte, um die Gültigkeit solcher Verträge zu klären, stellen momentan eine grosse Hürde bezüglich der Implementierung von Smart Contracts dar. Zudem wird die Umsetzung von Smart Contracts mit dem Anspruch des korrekten Umgangs mit hochsensiblen Patientendaten erschwert. Die Privatsphäre der Patienten muss jeweils sichergestellt sein, damit der umschriebene Prozess in der Praxis Anwendung finden kann.

Allgemeine Vorschriften

Es gibt einige allgemeine Vorschriften für Internetverträge, die man auch bei Smart Contracts beachten sollte. Besonders wichtig sind folgende Vorschriften in Art. 3 s UWG – werden diese nicht beachtet, gilt das Angebot als unlauter. Der Anbieter muss klare und vollständige Angaben über seine Identität und seine Kontaktadresse einschliesslich derjenigen der elektronischen Post bekannt geben. Die einzelnen technischen Schritte zum Vertragsabschluss müssen übersichtlich für die Kunden gestaltet sein und so, dass man Eingabefehler vor der Bestellung erkennen und korrigieren kann. Der Anbieter hat die Bestellung des Kunden unverzüglich auf elektronischem Wege zu bestätigen.

Ein Smart Contract gibt die Parteien nur in Form einer Adresse an, die eine fortlaufende Nummer ist und mit dieser kann man eine natürliche oder juristische Person nicht identifizieren. Nötig wäre, dass Smart Contracts die Identität der Parteien enthalten und die Plattformen entsprechende Programme anbieten müssen.

Weiter gilt auch für den Internethandel die Preisbekanntgabeverordnung (PBV). Der Anbieter muss den tatsächlich zu bezahlenden Preis in Schweizerfranken (Detailpreis) bekannt geben mit dem gut sichtbaren Hinweis «zahlungspflichtig bestellen». Wird die Dienstleistung über einen Fernmeldedienst mit Vorbezahlung abgerechnet, müssen die Kunden die Annahme des Angebots gegenüber ihrer Fernmeldefirma ausdrücklich bestätigen (Art. 11 a bis PBV). Man sollte auch darauf hinweisen, ob der Verkäufer die Transportkosten zu bezahlen hat.

In der EU gelten für den Abschluss von Internetverträgen die Informationspflichten des Anbieters sowie das Widerrufsrecht. Diese Regelungen beruhen auf der Verbraucherrechterichtlinie 2011/83/EU. «

Weiterführende Links

- www.postfinance.ch/de/blog/anlagewissen/smart-contracts.html

Abhandlung des Bundesrates:

- www.newsd.admin.ch/newsd/message/attachments/55150.pdf
- www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73398.html
- https://sites.hslu.ch/applied-data-science/wie-smart-contracts-die-zahlungsabwicklung-im-bereich-healthcare-veraendern/
- https://digilaw.ch/smart-contracts/
- www.coinbase.com/de/learn/crypto-glossary/what-is-a-blockchain-oracle-in-crypto
- www.handelskammerjournal.ch/de/smart-contracts-in-der-rechtspraxis
- www.coinbase.com/de/learn/crypto-basics/utility-tokens-vs-security-tokens-what-are-the-differences
- www.coinpro.ch/glossar/utility-token/

Porträt

Regula Heinzelmann
Juristin und freischaffende Journalistin

Regula Heinzelmann studierte Rechtswissenschaften an der Universität Zürich und arbeitet seit 1984 als selbstständige Autorin mit Schwerpunkt auf wirtschaftlichen und juristischen Themen. Für Unternehmen verfasst sie PR-Texte und Vertragsmuster. Die freischaffende Journalistin wohnt in Dietikon und lebt zeitweise in Berlin.

Kontakt

rhz@bluewin.ch
www.heinzelmann-texte.ch