Smart Contracts

Booklet

STADLER VÖLKEL
RECHTSANWÄLTE · ATTORNEYS AT LAW

Hi there, welcome to #svlaw

Intro

Die Aufmerksamkeit rund um Smart Contracts, auch "intelligente Verträge" genannt, nimmt stetig zu. Neben der Tokenisierung von Vermögenswerten bilden Smart Contracts eine der aktuellsten Entwicklungen in der Blockchain-Community mit hohem Disruptionspotenzial.

Smart Contracts können die Anwendung der Distributed Ledger Technologie in der Praxis weiter ausbauen und die Vorteile von DLT sinnvoll nutzbar machen. Durch die Möglichkeit bestimmte Vereinbarungen von Computersystemen automatisch abwickeln zu lassen, können Smart Contracts über die IT-Branche hinaus bei der Umsetzung verschiedenster Projekte eingesetzt werden.

Dieses Booklet soll zunächst die Funktionsweise von Smart Contracts erläutern. Nach Aufarbeitung des "intelligenten" Merkmals wird auf die Anwendungsmöglichkeiten von Smart Contracts, insbesondere bei ICOs, STOs und anderen Anwendungen, eingegangen. Schließlich werden die rechtlichen Besonderheiten beim Einsatz von Smart Contracts behandelt.

Als Rechtsanwaltskanzlei beraten wir Sie und verfassen für Sie gern auch programmierte Verträge!

Was sind Smart Contracts?

Vereinfacht gesagt sind Smart Contracts Computerprogramme, die auf einer Blockchain gespeichert und ausgeführt werden. Zur Veranschaulichung kann ein Snack-Automat herangezogen werden. Der Automat ist darauf programmiert, Snacks nur dann auszugeben, wenn ein bestimmter Eurobetrag bezahlt wurde. Bei der Abwicklung des Geschäfts treffen nicht zwei Menschen aufeinander, sondern ein Mensch und eine Maschine. Das Computerprogramm, das den Automaten steuert, nimmt für dessen Betreiber:in die Verfügung (Snacks ausgeben) nur dann vor, wenn die zuvor festgelegte Bedingung (Eurobetrag bezahlen) erfüllt ist.

Im rechtlichen Sinne kommt selbstverständlich kein Vertrag mit dem Automaten zustande, sondern mit dem:der betreibenden Unternehmer:in, der:die das Geschäft unter Verwendung des Automaten durchführt. Klar ist also, dass "intelligente Verträge" keine grundlegend neuen Phänomene sind – deren Verlagerung auf Blockchains hingegen schon.

Der Unterschied zu den ersten Kryptowährungen, wie z.B. Bitcoin, besteht darin, dass diese lediglich als Tauschmittel konzipiert waren und die digitale Darstellung von Werteinheiten mit Tauschmittelfunktion im Vordergrund stand. Im Gegensatz dazu laufen Smart Contracts auf Blockchains, die ihren Nutzer:innen die Erstellung und Durchführung eigener Programmcodes ermöglichen. Die wohl bekannteste Blockchain für den Einsatz von Smart Contracts ist Ethereum. Auf der Ethereum-Blockchain können Funktionen programmiert werden, die weit über die Wertträger-Funktion der "herkömmlichen" Kryptowährungen hinausgehen. Smart Contracts können Krypto-Assets empfangen, verwalten und sogar mit anderen Smart

Contracts interagieren, wenn eine entsprechende Schnittstelle im Programmcode vorgesehen ist.

Der Programmcode ist über eine öffentliche Adresse auf der Blockchain abrufbar, nachdem er zunächst von dessen Programmierer:in mit dem dazugehörigen privaten Schlüssel digital signiert und auf der Blockchain abgelegt (deployed) wurde. Nach dem Ablegen des Programmcodes können Dritte den Smart Contract bedienen (mit ihm interagieren), wenn sie die entsprechende Adresse und Funktion zum Ausführen des Smart Contracts kennen.

All diese auf den ersten Blick bloß technischen Möglichkeiten sind keinesfalls praktisch bedeutungslos. Durch die individuellen Ausgestaltungsmöglichkeiten von Smart Contracts können komplexe Abwicklungssysteme erstellt und durchgeführt werden. Die praktischen Beispiele nehmen täglich zu.

Die "Intelligenz" der Verträge

Das Besondere an Smart Contracts ist, dass sie die Vorteile der Distributed Ledger Technologie vielfältig nutzbar machen. Bei Vereinbarungen, die mittels Smart Contracts durchgeführt werden, gibt es nämlich keine zentralen Intermediäre (z.B. Treuhänder:innen), die eine Transaktion überwachen und durchführen. Beim Einsatz von Smart Contracts überprüft stattdessen der Programmcode, ob die eigens festgelegten Bedingungen für eine Transaktion erfüllt sind oder nicht. Es handelt sich vereinfacht gesagt um "Wenn-Dann"-Funktionen, die individuell und komplex ausgestaltet werden können.

Die Parteien, die sich eines Smart Contracts bedienen, müssen nicht auf einen zentralen Server zugreifen, um die Transaktionshistorie oder Besitzverhältnisse von bestimmten Werteinheiten einzusehen, da die Datensätze und Protokolle auf der dezentralen Blockchain gespeichert werden. Die Dezentralität bewirkt, dass die Parteien die verarbeiteten Datensätze auf ihrem eigenen Gerät jederzeit und zeitlich unbegrenzt einsehen und überprüfen können.

Attraktiv wird der Einsatz von Smart Contracts auch durch die Minimierung von Transaktionskosten und die Steigerung der Transaktionsgeschwindigkeit, was aus dem Einsatz eines Computers (statt der Einbindung einer menschlichen Instanz) resultiert.

Der wohl bedeutendste Vorteil von Smart Contracts liegt in der automatisierten Abwicklung. Es interagieren bzw. verhandeln nicht zwei Menschen, sondern ein Mensch mit einem Computerprogramm. Dies ist vor allem in jenen Konstellationen sinnvoll, in denen die Parteien zwar kontrahieren wollen, sich aber nicht kennen und daher keine Vertrauensbasis für die Abwicklung eines "herkömmlichen" Vertrages besteht. Solche Parteien können einen Smart Contract einsetzen, wodurch sie nur mehr dem Computerprogramm vertrauen müssen. Das Vertrauen in das Computerprogramm ist dabei regelmäßig größer, da es durch den Programmcode selbst festgelegt (sowie digital signiert) wird und die Vorgänge aufgrund der Dezentralität der Blockchain jederzeit einsehbar sind. Der Vertrag wird schließlich nur unter den im Programmcode festgelegten Bedingungen durchgeführt, was das eigene Leistungsrisiko der Parteien minimiert.

Vermögensverknüpfung

Onchain und Offchain

Der finale Schritt eines Smart Contract-Prozesses ist die Zuordnung bzw. Übertragung von Werten oder, je nach Ausgestaltung, auch von Eigentumspositionen. Wenn alle fixierten Ereignisse und Voraussetzungen erfüllt sind, erfolgt die automatische Durchführung der Vereinbarung – also die Erfüllung der sogenannten Hauptleistungsplicht des Vertrages.

Die Übertragung kann sowohl "Onchain" als auch "Offchain" erfolgen. Bei der Abwicklung "Onchain" werden Vermögenswerte digital übertragen, wohingegen bei der "Offchain"-Abwicklung Eigentum an physisch vorhandenen Vermögenswerten übertragen wird.

Bei diesem Schritt spielen Token eine zentrale Rolle. Token sind digitale Abbildungen auf einer Blockchain, die mit Forderungen (z.B. Wertpapiere, Gewinn- oder Projektbeteiligungen) aber auch mit realen Vermögenswerten (z.B. Eigentum an Kunstwerken) verknüpft werden können. Durch die Verknüpfung von Token mit dem jeweiligen Vermögenswert können Smart Contracts mittels Übertragung jener Token auch Eigentum an diesen Vermögenswerten übertragen ("Offchain"). Der Smart Contract kann hingegen auch in der Übertragung von rein digitalen Tausch- oder Zahlungsmitteln münden, z.B. in der Übertragung von Bitcoins oder USDC ("Onchain").

Durch die Einbindung von Token in Smart Contracts eröffnen sich unzählige Ausgestaltungsmöglichkeiten, zumal Smart Contracts auch gegenseitig auf Daten anderer Smart Contracts zugreifen und miteinander interagieren können. Es ist also möglich, ganze Vertragskonstrukte digital abzubilden und mittels Smart Contract durchzuführen.

Anwendungsbeispiele

Generell sind Smart Contracts geeignet, standardisierte Prozesse effizient und kostengünstig zu gestalten und automatisiert durchführen zu lassen. Der Grund dafür ist, dass die im Programmcode hinterlegten Regeln überwacht und beim Vorliegen bestimmter Ereignisse (Trigger) bestimmte Aktionen selbstständig und automatisch ausgeführt werden.

Beispiel-Transaktion: A möchte einen Teil ihres Vermögens erst **dann** an B übertragen, **wenn** B seine eigene Leistung erbracht hat und ein bestimmtes Datum erreicht ist (Trigger). Der Smart Contract überwacht nun das Datum und die Leistungserbringung von B. Wenn das Ereignis eintritt, also das bestimmte Datum erreicht ist, überprüft der Smart Contract, ob B seine Leistung erbracht hat. Sind beide Voraussetzungen erfüllt, bewirkt der Smart Contract die Vermögensübertragung (z.B. Transfer auf die Adresse des B) automatisch, ohne das Zutun von A oder B.

Der erste Anwendungsfall von Smart Contracts war die Ausgabe neuer digitaler Assets mit dem Ziel initiale Finanzierungen für Unternehmen zu erreichen. Durch die stetig wachsende Anwendung und Akzeptanz von Smart Contracts bietet sich mittlerweile eine Vielzahl an Möglichkeiten. Das Security Token Offering möchten wir etwas näher vorstellen.

Security Token Offering (STO)

Ein relevanter Anwendungsfall von Smart Contracts sind Security Token Offerings (STOs). Dabei wird ein Token auf der Blockchain erstellt und mittels Smart Contract ausgegeben. Die Token können dabei mit unterschiedlichsten Rechten (z.B. Ansprüche auf Erträge des Projektes oder Gewinnbeteiligungen) verbunden werden, welche vor der Ausgabe zu definieren sind. Als Gegenleistung für die Ausgabe der Token erhält der:die Emittent:in Kapital.

Zu beachten ist, dass es sich bei den im Rahmen eines STO ausgegeben Token in der Regel um tokenisierte Wertpapiere oder andere Finanzinstrumente handelt. Um etwaige aufsichtsrechtliche Anforderungen zu erkennen und umzusetzen ist daher im Vorfeld besonderes Augenmerk auf die Ausgestaltung der mit den Token verknüpften Rechte zu legen.

Die Ausgabe der Token ist in solchen Fällen mit der klassischen Ausgabe von physischen Wertpapieren vergleichbar. Der Unterschied besteht darin, dass bei STOs keine Intermediäre für die Ausgabe erforderlich sind, also keine Emissionsbank, keine Zahlstelle und keine Vertriebsstelle.

Bei der erstmaligen Ausgabe von Token bleibt es jedoch nicht. Smart Contracts ermöglichen auch die Aufrechthaltung von Verzeichnissen über die Besitzverhältnisse der jeweiligen Token. Der Smart Contract regelt somit nicht nur die Ausgabe, sondern auch die Weitergabe und den Besitz der Token. Die Funktionalitäten von Verzeichnissen und Bedingungen sind nahezu unbegrenzt. Die wohl aktuell bekannteste Blockchain für die Anwendung solcher Smart Contracts ist wiederum Ethereum, wo sich mittlerweile auch technische Programm- und Schnittstellen-Standards etabliert haben.

Technische Standards der Ethereum Blockchain für die Implementierung von Token: ERC-20 für die Entwicklung von Projekten, die auf die Ausgabe und Übertragung der Token abzielen. Für Non-Fungible Tokens, welche einzigartig und nicht austauschbar sind, kann der ERC-721 Standard dienen.

Security Token Offering (STO)

Beispiel

Beispiel Projektfinanzierung: Der Programmcode eines Smart Contracts bestimmt

> dass die in Form des Stablecoins USDC eingesammelte Finanzierungssumme an die Geschäftsführung erst dann ausbezahlt wird, wenn ein Mindestbetrag von USD 500.000 erreicht wird

und

> dass auch die Token, die einen bestimmten vermögensrechtlichen Anspruch der Anleger:innen repräsentieren, erst dann an die Investor:innen ausgegeben werden, wenn der Mindestbetrag erreicht wurde.

Sollte dieses Ziel nicht erreicht werden, erfolgt keine Ausgabe der Token und die Investor:innen erhalten ihr Kapital zurück.

Rechtliche Besonderheiten

bei Smart Contracts

Verträge können grundsätzlich (bei Vorliegen übereinstimmender Willenserklärungen der Parteien) auch mittels Smart Contracts abgeschlossen werden. Smart Contracts – als reine Computerprogramme – können aber auch so ausgestaltet werden, dass der Vertragsabschluss mit der Ausführung des Smart Contracts zusammenfällt. Der Vertrag kommt dabei unter den programmierten Bedingungen auf elektronischem Wege zustande.

Da Smart Contracts ein Programmcode zugrunde liegt, der die Bedingungen für die Durchführung der Vereinbarung festlegt, stellt er dessen Herzstück dar. Beim Einsatz von Smart Contracts hat der Programmcode daher den gesamten Vertragstext abzubilden. Es sind außerdem alle notwendigen Funktionalitäten abzudecken, da ein "Nachverhandeln" wie beim Kontrahieren zweier Menschen wegen technischer Besonderheiten nicht möglich ist. Stattdessen müsste ein neuer Smart Contract vereinbart werden, was nicht immer möglich ist. Es sollten daher alle möglichen Szenarien berücksichtigt und in Programmiercodes umgesetzt werden. Der Programmcode ist überdies so auszugestalten, dass er dem geltenden Recht entspricht. Smart Contracts bewegen sich nämlich nicht im rechtsfreien Raum (Code is law), sondern unterliegen den herkömmlichen Vertragsbeschränkungen des Zivilrechtes, wie etwa Wucher oder besonderen Formvorschriften für z.B. Liegenschaftskäufe.

Rechtliche Besonderheiten

bei Smart Contracts

In Bezug auf STOs ist insbesondere zu beachten, dass (abhängig von den mit den Token verbundenen Rechten) finanzmarktaufsichtsrechtliche Vorschriften anwendbar sein können. Eine rechtliche Prüfung des geplanten Projektes in enger Zusammenarbeit mit dem Programmier-Team ist daher unerlässlich.

Für die effektive Nutzung intelligenter Verträge ist also nicht bloß juristisches, sondern auch IT-spezifisches Fachwissen gefragt. Als Kanzlei mit jahrelanger Erfahrung im Fintech- und Krypto-Bereich arbeiten wir mit hochqualifizierten IT-Expert:innen zusammen, um Projekte unter Einbindung von Smart Contracts bestmöglich und rechtssicher umzusetzen.

Dein SV.LAW-Team

für den Bereich Smart Contracts

Oliver Völkel

Bryan Hollmann

Philipp Ley

Andreas Pfeil

Maya Kindler

Stefan Riedler

STADLER VÖLKEL
RECHTSANWÄLTE · ATTORNEYS AT LAW

Grafikdesign
Mag. Stefanie Wagner

IMPRESSUM
STADLER VÖLKEL Rechtsanwälte GmbH
Seilerstätte 24, 1010 Wien

Tel.: +43 1 997 1025
Fax: +43 1 997 1025 99

office@sv.law
www.sv.law

Bildnachweise
Adobe Stock

Druckhersteller
online Druck GmbH
Brown-Boveri-Straße 8
2351 Wr. Neudorf