



HOCHSCHULE RUHR WEST
UNIVERSITY OF APPLIED SCIENCES

Rechtliche Aspekte des Blockchain im Vertragsrecht

Hausarbeit

in Modul IT-Recht

Studiengang Wirtschaftsinformatik
der Hochschule Ruhr West im vierten Semester

Samr Alakrad: 10013285

Shyiar Rashid: 10010765

Erstprüferin: Prof. Dr. Rolf Albrecht

Essen, 05. 05. 2022

Kurzfassung

Diese Arbeit befasst sich mit den Rechtlichen Aspekten des Blockchain im Vertragsrecht mit seinen rechtlichen und technischen Besonderheiten im Smart-Contracts. Zu Beginn wird ein Verständnis für die Blockchain und deren Umsetzung aufgebaut. Danach werden die gängigsten Anwendungsgebiete der Blockchain beleuchtet und die rechtlichen Vertragsarten der Kryptowährung, Datenschutzaspekte und Haftung erläutert. Darauf folgend wird in das Thema Smart Contracts eingeführt, es nach tatsächlicher und technischer Sicht definiert und die Rechtlichen Aspekte der Smart Contracts dargestellt. Das vorletzte Kapitel beschäftigt sich mit den Auswirkungen der Blockchain-Technologie auf den Schutz und die Stabilität von Smart Contracts, wobei das letzte auf die Vor- und Nachteile der Contracts eingeht. Am Ende schließt die Arbeit mit einem Fazit ab

Inhaltsverzeichnis

Kurzfassung	2
Inhaltsverzeichnis	3
Abbildungsverzeichnis	4
Abkürzungsverzeichnis	4
Vorwort	5
Einleitung.....	6
Anwendungsgebiete der Blockchain.....	7
1. Die Blockchain in der Finanzbranche	7
2. Blockchain im öffentlichen Sektor.....	9
3. Blockchain im Rechtswesen.....	9
4. Blockchain im Internet der Dinge.....	9
Vertragstypen	10
1. Erwerb von Kryptowährungen unter Einsatz von Geld.....	10
2. Bezahlung mit Kryptowährung.....	12
3. Mischformen und alternative Zahlungsmodelle.....	12
Blockchain und Datenschutz.....	13
Bitcoin und Haftung	14
Smart Contracts	16
Rechtliche Aspekte der Smart Contracts	16
Auswirkungen der Blockchain-Technologie auf den Schutz und die Stabilität von Smart Contracts	17
Vorteile und Nachteile von Smart Contracts	19
Vorteile.....	19
Nachteile	19
Fazit	21
Literaturverzeichnis	22
Erklärung	24

Abbildungsverzeichnis

Abbildung 1: Prinzip einer Blockchain [10, S.14]

Abbildung 2: Potenzial der Blockchain in Anwendungsbereichen der Finanzbranche [1, S.31]

Abkürzungsverzeichnis

KYC	Know Your Customer
P2P	Peer-to-Peer Architectur
IBM	International Business Machines Corporation
POC	Proof-of-Concept
DAOs	Decentralized autonomous organization
BGB	Bürgerliches Gesetzbuch
GewO	Gewerbeordnungsgesetz
VPN	Virtual private network
TOR	The Onion Router
DS-GVO	Datenschutz Grundverordnung
DAO	Decentralized Autonomous Organization

Vorwort

Diese wissenschaftliche Arbeit wurde im Rahmen des Faches IT-Recht der Wirtschaftsinformatik im vierten Semester an der Hochschule Ruhr West geschrieben.

Die vorliegende Leistung unterscheidet mehrere Teile, verfasst von Samr Alakrad und Shyiar Rashid, Studenten der Hochschule Ruhr West des Studiengangs Wirtschaftsinformatik. Assia Moharram sollte Mitglied der Gruppe sein, schied aber kurz vor der Einreichung aus. Assia sollte die Einleitung, der Erläuterung der Blockchain aus technischer und tatsächlicher Sicht, der Funktionsweise eines Blockchain-Systems am Beispiel von Bitcoin und der Umsetzung durch Unternehmen bearbeiten, Daher musste Samr nach Rücksprache am 04.05.2022 mit Ihnen die wesentlichen Punkte des Assia-Teils in der Einleitung bearbeiten, dazu hat er die Anwendungsgebiete der Blockchain, Vertragstypen der Kryptowährung und Datenschutzaspekte verfasst. Anschließend befasste sich Shyiar mit Bitcoin und Haftung, der Definition von Smart Contracts und ihren rechtlichen Aspekten, den Auswirkungen der Blockchain-Technologie auf Smart Contracts und den Vor- und Nachteilen davon.

Einleitung

Blockchain ist eine auf P2P-Datenübertragung basierende Technologie, die es Netzwerkteilnehmern (oft als Miner oder Schürfer bezeichnet) ermöglicht, Transaktionen ohne Intermediäre wie Banken oder Aufsichtsbehörden zu bestätigen, zu verifizieren und zu verbuchen. Transaktionsdaten werden dann in Blöcken gespeichert, mit einem Zeitstempel versehen und anschließend mit anderen Blöcken verkettet [2]. Damit hat jeder Block genau einen chronologischen Vorgänger und einen chronologischen Nachfolger. Aus dieser digitalen Verkettung entsteht eine Liste, die den Namen der Blockchain ausmacht [9].

Um einen neuen Block zu erzeugen, muss ein Verschlüsselungswert (sog. Hash-Wert) des „Block-Headers“ mittels einer kryptografischen Funktion erzeugt werden, der einen bestimmten Zielwert unterschreitet. Hier kommt der Mining-Prozess ins Spiel, bei dem ein mathematisches Problem gelöst wird, um einen neuen Block zu erstellen [10, S.13].

Die folgende Abbildung veranschaulicht grafisch die im Blockheader gespeicherten Informationen und die Verknüpfung der Blöcke in einer Blockchain [10, S.14]:

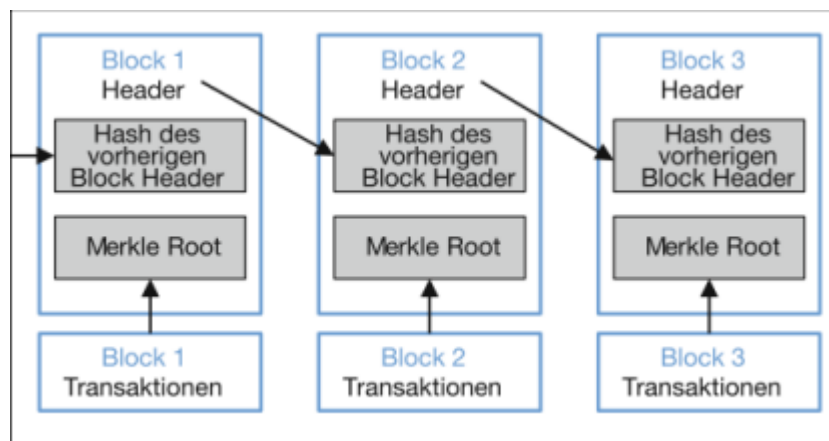


Abbildung 01: Prinzip einer Blockchain

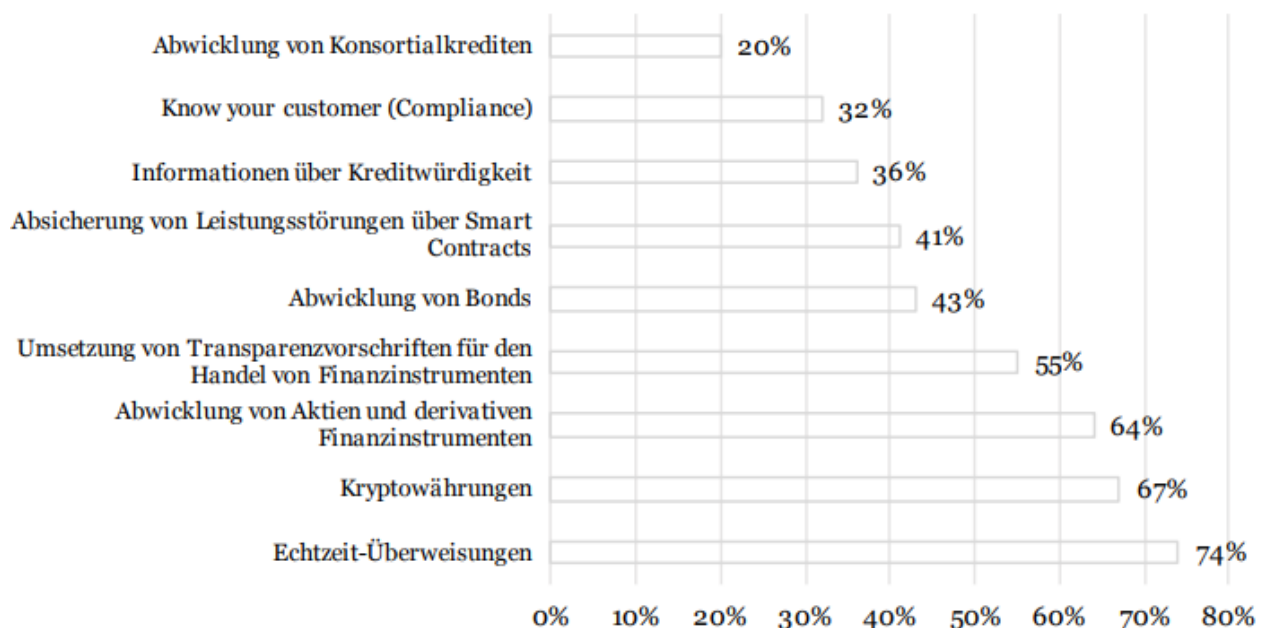
Die verschlüsselten Werte der einzelnen Transaktionen im Block und die Referenz auf den vorherigen Block bilden den Hash-Wert, der der Grundkomponente des Blocks zugrunde liegt. [10, S.13-15].

Im Gegensatz zu traditionellen Datenbanken ist die Blockchain ein globales Transaktionsregister zur sicheren Verarbeitung und Validierung von Datentransaktionen, das sicher Daten und Werte in einem geschlossenen Bereich mit nur identifizierten Teilnehmern überträgt und Betrug nahezu ausschließt [8].

Anwendungsgebiete der Blockchain

1. Die Blockchain in der Finanzbranche

Eine Studie von Cofinpro AG und IT-Finanzmagazin (2016) mit Fokus auf Schnelligkeit, Kosten und Transparenz hat gezeigt, dass Blockchain in folgenden Bereichen das größte Potenzial hat [1, S.30-31]:



Anteil der Befragten (n=84), Mehrfachnennungen möglich

Abbildung 1: Potenzial der Blockchain in Anwendungsbereichen der Finanzbranche

1.1. Zahlungsverkehr

In der Abbildung soll gezeigt werden, dass es sich eine deutliche Tendenz in Richtung Zahlungsverkehr erkennen lässt. 74 % der Befragten stimmen zu, dass dieser Bereich als der vielversprechendste in der Finanzbranche gilt [1, S.31-32].

Die bisherigen Probleme des digitalen Zahlungsverkehrs spiegeln sich in hohen Kosten und langen Transaktionszeiten wider. Dies kann jedoch durch die Blockchain nicht nur für Kryptowährungen, sondern auch für jede Währung gelöst werden. Bei internationalen Überweisungen fallen zum Beispiel durchschnittlich 6 % Gebühren an, während eine Blockchain-basierte Lösung diese Zahl auf 2 % senken lässt [1, S.32].

Ein konkretes Beispiel für die geringen Transaktionszeiten ist das Unternehmen Ripple. Es bietet eine Zahlungsplattform für die kostenlose (internationale) Transformierung und den Umtausch beliebiger Währung. Die gesamte Transaktionsabwicklung wird auf 5 bis 15 Sekunden reduziert, indem ein nativer Token verwendet wird, der die entsprechende Währung darstellt. Dieser Token wird innerhalb des Systems übertragen und kann schließlich gegen Bitcoin und dann gegen eine beliebige Währung eingetauscht werden [1, S.32-33].

Die von den Unternehmen auf den beiden Seiten hergestellten Übereinstimmungen bei der Wertübertragung ist eine weitere Möglichkeit, die verkürzten Transaktionszeiten einzuhalten [2].

1.2. Kapitalmarkthandel und wirtschaftliche Auswirkung von Blockchain

Der Prozess der Abwicklung von Wertpapiertransaktionen dauert in der Regel zwei bis drei Tage und umfasst mehrere Intermediäre für Angelegenheiten wie Absicherung des Kontrahentenrisikos und kann daher Kredit- und Liquiditätsrisiken sowie Kontrahentenrisiken schaffen. Das Zentralregister der Firma SETL konnte all diese Probleme lösen, indem es die Blockchain-basierten Abwicklungen in Echtzeit realisierte. Darüber hinaus wurden die Gemeinkosten für die Registrierung und Verwaltung von Wertpapieren reduziert und die Aufgaben von Intermediären beseitigt bzw. durch die Blockchain übernommen [1, S.33-35].

Blockchain hat im Anleihenhandel Fortschritte gemacht. Durch die obligatorische Synchronisierung aller Datenbanken wurde der zeitaufwändige Prozess der Verfolgung und Erfassung von Dokumentation und Eigentum reduziert bzw. eliminiert [2].

1.3. Compliance

Blockchain hat den Buchhaltungsprozess in der Bankenbranche im Bereich der Datenintegrität maßgeblich verändert. Als Beispiel könnte die Verhinderung der Manipulationen in der Buchhaltung wie das Zurückdatieren von Verträgen auf andere Perioden durch die Irreversibilität und zuverlässigen Zeitstempel von Transaktionen herbeiführen [1, S.35].

Die KYC im Finanzdienstleistungsbereich erfordert, dass Fachleute sich bemühen, die Identität, Eignung und Risiken zu überprüfen, die mit der Aufrechterhaltung einer Geschäftsbeziehung verbunden sind [3].

Andererseits spielte hierbei das auf einem Blockchain-System basierende Kundenregister eine hervorragende Rolle, das den Mehrfachaufwand bei KYC-Prüfungen eliminiert und die verschlüsselte Übertragung von Kundendaten ermöglicht [1, S.36].

2. Blockchain im öffentlichen Sektor

Blockchain wird nicht nur in der Wirtschaft, sondern auch im öffentlichen Sektor eingesetzt, indem Steuern von der Regierung über ein Blockchain-System erhoben werden. Dadurch wird die Transparenz erhöht und der mit der Zahlung und Erhebung von Steuern verbundene Verwaltungsaufwand reduziert. Darüber hinaus ermöglicht die Digitalisierung von Regierungssystemen mittels der Blockchain korruptionsfreie und transparente Wahlen, bei denen ein öffentlicher Schlüssel als Stimme zählt, wodurch es möglich wird, vollständig repräsentative Demokratien und Staatsmaschinen effizienter aufzubauen, da viele Prozesse über Smart contracts automatisiert werden könnten [1, S.37-39].

3. Blockchain im Rechtswesen

Blockchain wird insbesondere im Bereich der Verifizierung von Urheberschaft und Dokumenteninhalten, der Übertragung von Eigentumsrechten und der Vertragsdurchsetzung eingesetzt. Herkömmliche Verträge haben die Schwäche der sprachlichen Mehrdeutigkeit, aber Smart contracts, die sogenannte manipulationssichere Datenbank, mit ihrer Code-Eindeutigkeit können sie ersetzen und die anderen Nachteile beseitigen, indem sie digitale Eigentumsrechte effizient verfolgen und den Prozess der Vertragserstellung demokratisieren [1, S.39-40].

4. Blockchain im Internet der Dinge

Der Aufwand für die Pflege einer typischen Cloud-Architektur bzw. P2P-Architektur und der damit verbundenen externen Cloud-Dienste ist hoch, während die Implementierung eines autonomen P2P-Netzwerks mithilfe der Blockchain die Notwendigkeit eines dritten

Cloud-Dienstes beseitigen und die damit verbundenen Kosten reduzieren bzw. eliminieren könnte [1, S.41-42].

In Zusammenarbeit mit Samsung nutzte IBM dies und implementierte einen POC namens ADEPT. Dabei soll eine Waschmaschine über Smart Contracts und DAOs autonom handeln, beispielsweise indem sie ihr Waschmittel selbst bestellt und bezahlt oder im Schadensfall ihren Garantiestatus prüft und einen geeigneten Handwerker bestellt, der abhängig vom Garantie-Status bezahlt werden kann [1, S.42-43].

Vertragstypen

Da Kryptowährung eine praktische Anwendung für Blockchain ist und auf der Blockchain-Technologie basiert, wird im Verlauf dieser Arbeit ausschließlich auf die schuldrechtliche Behandlung von Kryptowährungen eingegangen.

Dabei sind zwei Fälle zu unterscheiden. Zum einen ihre Anschaffung und zum anderen ihre Verwendung als Zahlungsmittel [4]:

1. Erwerb von Kryptowährungen unter Einsatz von Geld

1.1. Sachkauf i.S.d. § 433 BGB

Da Kryptowährungen als sonstige Gegenstände im Sinne des § 453 I Alt. 2 BGB einzuordnen ist, kommt das Kaufrecht, §§ 433 ff. BGB, in Betracht. Demnach ist der Kauf von Kryptowährungen gegen einen Geldbetrag als Kaufvertrag einzustufen [4].

1.2. Rechtskauf/ Kauf von sonstigen Gegenständen i.S.d. § 453 BGB

Denkbar wäre der Kauf von Rechten oder anderen Sachen nach § 453 BGB, wobei die Kryptowährung als unkörperlicher Gegenstand oder immaterielles Gut eher als Sache denn als Recht einzustufen ist. Der Verweis in § 453 Abs. 1 Alt. 2 BGB führt zur Anwendung der Vorschriften des Kaufrechts, wenn der Kauf von Kryptowährung als atypischer Kaufvertrag einzustufen ist, daher stellt ihr Kauf gegen Kaufpreis einen Kauf im Sinne der §§ 453, 433 BGB dar [4].

1.3. Atypischer Werkvertrag, § 631 BGB

Ein möglicher Vertragstyp für den Kauf von Kryptowährung ist der Werkvertrag nach § 631 BGB, wobei ein Erfolg geschuldet wird. Dieser Erfolg ist immer das Ergebnis einer vorangegangenen Leistung, ein sogenanntes Werk. Bei Kryptowährung wäre die erwartete Leistung die digitale Übertragung von Daten, die zu einer gültigen Transaktion führt. Demnach würde die Transaktion als geschuldete Erfolg gelten. Diese Auslegung würde jedoch als atypischer Werkvertrag eingestuft, da es sich um eine einfache Übertragung eines bereits bestehenden Gutes handelt. Fraglich ist aber der Erfolg dieser Transaktion. Es ist gegeben, wenn das P2P-Netzwerk die Transaktion als richtig bestätigt und dies in der Blockchain vermerkt. Diese Bestätigung liegt jedoch nicht in der Macht des Veräußerers. Außerdem ist das Abbild der Transaktion nicht der Erfolg, sondern nur dessen Dokumentation. Damit stellt sich die Frage, ob die Dokumentation des Transfers überhaupt als „Werk“ anzusehen ist! [4].

Sie ist keine vertragliche Verpflichtung des Verkäufers, sondern lediglich die faktische Folge der Entstehung der Verfügungsmacht über die Währungseinheiten, die dieser „Protokollierung“ logisch vorausgegangen ist. Dementsprechend käme ein atypischer Werkvertrag für den Kauf von Kryptowährung in Frage [4].

1.4. Mining als Dienstvertrag, § 611 BGB

Menschen übertragen Bitcoins rund um die Uhr über das Bitcoin-Netzwerk. Das Bitcoin-Netzwerk verarbeitet diese Transaktionen, indem es alle Transaktionen über einen bestimmten Zeitraum sammelt und in eine Liste (der sogenannte Block) einfügt. Es ist dann der Job des Miners, diese Transaktionen zu bestätigen und im Kontenbuch zu vermerken. Dieser Prozess nennt man Mining bzw. schürfen [5].

Ist die Schaffung einer Kryptowährungseinheit durch Mining also ein konkreter Erfolg, geschuldet, kommt ferner auch Dienstvertragsrecht in Betracht nach § 631 II BGB. Der Erhalt der Belohnung (Kryptowährungseinheit) ist jedoch zufällig, denn die Belohnung erhält derjenige, der als erster die Rechenoperation erfolgreich abgeschlossen hat. Aus Sicht des Miners ist dies ein großes Risiko. Um dem entgegenzuwirken, sollte das Vertragsprotokoll eher als Dienstleistungsvertrag konzipiert werden. Das bedeutet, dass Miner Rechenleistung und den Mining-Prozess geschuldet wird. [4] [6].

2. Bezahlung mit Kryptowährung

Kryptowährungen werden teilweise akzeptiert, um Waren und Dienstleistungen zu bezahlen. Dazu müssen die Parteien eine Zahlung in digitaler Währung vereinbaren [4].

Hierbei können verschiedene Verträge zustande kommen:

2.1. Kaufvertrag oder Tausch – auf den ursprünglichen Parteiwillen kommt es an

Grundsätzlich ist es sinnvoll, Verträge, bei denen eine Ware oder Dienstleistung mit Währungstoken bezahlt wird, als Kaufvertrag nach § 433 BGB einzustufen. Fraglich ist, ob der Currency Token als Kaufpreiszahlung im Sinne des § 433 II BGB.1 einzustufen ist [4].

Währungstoken sind zumindest kein Geld, sie können aber auch andere Gegenstände als die Zahlung des Kaufpreises sein, etwa über abweichende Parteivereinbarungen. Hier kommt der Tauschvertrag (§ 480 BGB) in Frage, da das Bezahlen mit Kryptowährung bei Vertragsabschluss als Tauschvertrag §§ 453, 480 BGB einzuordnen ist [4].

Der einzige Unterschied zwischen einem Tauschvertrag und einem Kaufvertrag besteht darin, dass statt der Leistung eines Kaufpreises die Leistung eines Rechts- oder sonstigen Vermögenswerts, wie ein bestimmter Betrag einer Kryptowährung, vereinbart wird [4].

2.2. Kryptowährung als Gegenleistung beim Werk- und Dienstvertrag

Bei Dienst- und Werkverträgen wird nach §§ 611 I, 631 I BGB regelmäßig eine Vergütung geschuldet. Der Begriff der Vergütung erfasst jegliche Art der Vergütung, sofern es sich dabei um einen monetären Wert im Verkehr handelt, daher können diese Vertragstypen gemäß § 107 Abs. 1 GewO durch Zahlung von Kryptowährungen erfüllt werden [4].

3. Mischformen und alternative Zahlungsmodelle

Ein Beispiel hierfür ist der Softwarehersteller Qbix Inc. Nutzer seiner Software „Calendar 2“ können zusätzliche Softwarefunktionen „kostenlos“ freischalten. Dieser Prozess verdeutlicht den Übergang vom reinen Softwarekauf oder -miete zu einer Mischform der Dauerschuldverhältnisse in Form von (Dienst- oder Mietverträgen) [4]

Blockchain und Datenschutz

In Form von Token den elektronischen Geldbörsen („Wallets“) werden Blockchain-Werte den Netzwerkteilnehmer zugeteilt. Währenddessen die Wallet-Adressen öffentlich einsehbar sind, bleiben die Namen und Details der Eigentümer privat, wie die einzigartig zugewiesene Identifizierungscode des Wallets, das nach jedweder Transaktion aktualisiert wird, sofern sich das Wallet nicht an einer regulären Börse befindet, die sogenannte „KYC“ Verfahren [2]. Ein Beispiel hierfür ist der Kauf von Bitcoins oder das Bezahlen mit Bitcoins [7, S.3].

Zudem offeriert Blockchain durch die Verwendung von Konsensalgorithmen und rückwärtsverknüpften Blöcken eine sichere Verarbeitung und Überprüfung von Datentransaktionen auf der Basis eines PTP-Netzwerks, um Transaktionen praktisch unveränderlich zu machen [8].

Betreiber von Bitcoin-Börsen und Bitcoin-Dienstleistern verarbeiten Blockchain-Daten zusammen mit der Identifizierung der Konten ihrer Kunden auf Grundlage von Vertragsverhältnissen, ausdrücklicher Einwilligung und/oder gesetzlicher Erlaubnis. Nur weil Blockchain-Daten öffentlich verfügbar sind, bedeutet das nicht, dass sie auch Daten über ihre Kunden erhalten würden [7, S.2-3]. Kundendaten werden von Bitcoin-Börsen nur im Rahmen einer Strafanzeige oder anderer gerichtlicher Anordnungen an Dritten weitergegeben [7, S.3].

Bei Bitcoin wird der Inhaber der Bitcoin-Adresse oder zumindest die Bitcoin-Börse durch Ermittlung der IP-Adressen der Bitcoins ermittelt. Dafür sind allerdings VPN-Dienste oder TOR von Bedeutung, um IP-Adressen unkenntlich zu machen. Dazu könnten auch Mixer-Services verwendet werden, die viele Bitcoin-Konten miteinander vertauschen, um das Tracking zu erschweren [7, S.3].

Bitcoin und Haftung

1. Betreiber von Bitcoin-Knoten

Der Code ist dabei Open Source und jeder kann ihn nach Belieben ändern, aber wenn der Betreiber beschließt, vom Protokoll abzuweichen, käme dies einem Abschalten des eigenen Knotens gleich. Dies hat jedoch keine Auswirkungen auf die Bitcoins.

Hat der Knotenbetreiber praktisch keinen Einfluss auf die Verarbeitung personenbezogener Daten, ist zweifelhaft, ob er über die Zwecke der Verarbeitung bestimmt. Art. 26 Abs. 1 Satz 1 DS-GVO kommt nur dann zum Einsatz, wenn mehrere Parteien nach Absprache über die Zwecke agieren. Zwischen den Knotenbetreibern gibt es jedoch in der Regel gar keine Absprache über die Zwecke [7, S.4-5].

2. Mineur

Mineure, die zunächst mathematische Rätsel für einen Block lösen, um den nächsten Block definieren zu können sowie die festgelegte Belohnung zu erhalten, haben die Möglichkeit, einzelne Transaktionen zu selektieren oder auszuschließen. Transaktionen, die nicht vom Mineur aufgenommen werden, werden jedoch nicht dauerhaft abgelehnt, sondern können mit dem nächsten Block aufgenommen werden, zudem ein anderer Mineur die Lösung als Erster findet. Daher ist der Miner nicht verantwortlich für selbst erstellte Blöcke und die darin enthaltenen Transaktionen [7, S.4-5].

Gemeinsame Verantwortung kann in der Gesamtheit der Mineure sein, gemäß Art. 4 Nr. 7 DS-GVO. Voraussetzungen Allerdings sind die zuvor gemeinsame festgelegte Ziele (Art. 26 Abs. 1 Satz 1 DS-GVO) sowie die zuvor Bestimmung der Gruppenmitgliedern, da jeder, der auf der Suche nach einem passenden Nounce-Wert (der Wert, der zur Validierung eines Blocks notwendig ist) ist, ist ein Mineur [7, S.4-5].

3. Softwareentwickler

Softwareentwickler übernehmen keine Verantwortung, da sie weder die konkreten Verwendungszwecke der Bitcoin-Transaktionen noch die Mittel der Datenverarbeitung bestimmen, Art. 4 Nr. 7 DS-GVO [7, S.5].

4. Nutzer

Auf die Zwecke der Datenverarbeitung kann der Nutzer gezielt Einfluss nehmen, da er alleiniger Inhaber des privaten Schlüssels einer Bitcoin-Adresse ist, der für eine erfolgreiche Transaktion notwendig ist. Darüber hinaus hat er die Kontrolle über die Transaktion, die in der Blockchain aufgezeichnet wird, und niemand kann die Transaktion aus der Blockchain entfernen. Damit bestimmt er die Mittel der Datenverarbeitung. Daher ist er verantwortlich gemäß Art. 4 Nr. 7 DS-GVO für seine Transaktion [7, S.5].

5. Bitcoin-Handelsplätzen oder Geldbörsen-Diensten

Handelsplattformen oder zentralisierte Bitcoin-Geldbörsen-Dienste sind im Namen des Nutzers Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO. Infolgedessen können sie Transaktionen effektiv blockieren durchführen und einen erheblichen Einfluss auf die Datenverarbeitung haben [7, S.5-6].

Smart Contracts

Der Begriff Smart Contract wurde erstmalig 1997 von dem Informatiker und Rechtsberater Nick Szabo geprägt. Sie sind selbstausführende Verträge, die in der Blockchain gesichert und repliziert werden. Dabei sind die Vertragsbedingungen unmittelbar in den Code geschrieben und von Geräten wie PCs, Smartphones und anderen Clients wie Waschmaschinen automatisch durchgesetzt. Je nach Programmierstil kann ein Teil oder der gesamte Vertrag selbsttätig werden. Voraussetzung dafür ist, dass ein Programm auch prüft, ob die Parteien ihren Pflichten vollziehen können. Grundsätzlich können Benutzer nur auf die Daten zugreifen, die sich innerhalb der verfügbaren Blockchain befinden. Bei Smart Contracts müssen meist nicht zugehörige Vorfälle berücksichtigt werden. Dies erfolgt mithilfe in dieser Art bezeichnete Orakel. Ein Orakel kann entweder eine automatisierte Dateneingabe oder ein vertrauenswürdiger unabhängiger von Dritten sein, der gezielte Entscheidungen treffen kann bzw. muss. Dadurch lassen sich zukünftige Vorkommnisse mittels Blockchain-Technologie abbilden [11].

Rechtliche Aspekte der Smart Contracts

Smart Contracts werden als Verträge im Sinne des deutschen Rechts behandelt, die immer eine rechtsverbindliche Willenserklärung beinhalten und basiert auf dem Prinzip: „Code ist Gesetz“, der die relevanten Vertragsinhalte enthält. Dabei gilt die Sogenannte Wenn-Dann-Regel, die besagt: Wird eine im Vertrag festgelegte Bedingung erfüllt, hat dies automatisch zur Folge, dass die zuvor festgelegten Aktivitäten ausgeführt werden. Gleichzeitig werden alle Vertragspartner in Echtzeit über Statusänderungen informiert [14] [16].

In Form von Computercode repräsentieren Smart Contracts die rechtmäßig traditionellen Verträge, daher müssen die im Code vereinbarten Anforderungen erfüllt werden, aber sobald diese Vereinbarungen gegen die gesetzlichen Vorschriften verstoßen, sind sie unwirksam, wie Wucherverbote (§ 138 BGB) und Umgehungsverbote (§ 306a BGB) [13] [14].

Auswirkungen der Blockchain-Technologie auf den Schutz und die Stabilität von Smart Contracts

Auf der Blockchain-Technologie basierende Verträge weisen mehrere Merkmale auf. Hierfür könnte die Befreiung des Vermittlers bzw. des Dritten herbeiführen, die sogenannte Anonymität, die durch die Existenz eines globalen Netzwerks zu einer greifbaren Realität geworden ist. Dabei zeichnet die Blockchain-Technologie alle Transaktionen auf, die über alle Netzwerkgeräte hinweg stattfinden und werden dann in den jeweiligen Blöcken erfasst und somit im gesamten System gespeichert. Transaktionen werden vor der Speicherung überprüft, da eine Änderung oder Manipulation nach der Speicherung der Daten nicht möglich ist. Der Grund dafür ist, dass die Verschlüsselung verstreut ist, da die Eingabe falscher Daten zu Blöcken mit ungültigen Parametern führt und diese somit im Netzwerk nicht akzeptiert werden [15].

Die Blockchain-Technologie ist Open Source, sodass jeder diese Technologie in jeder Anwendung verwenden kann. Damit die Transaktion korrekt durchgeführt werden kann, muss sie allen Nutzern zwecks Protokollierung und deren Manipulationsverbot offengelegt werden. Hinzu kommt die einzigartige Eigenschaft (Unabhängigkeit) von Smart Contracts, die besagt, dass der Smart Contract seine Aufgabe unabhängig von seinem Nutzer erfüllt. Beispielsweise werden Gebühren für den Kauf von Artikeln ohne Bestätigung des Eigentümers oder Benutzers überwiesen [15].

Der Blockchain-Mechanismus genießt Vertraulichkeit und Anonymität, da diese Technologie Transaktionen ohne Offenlegung der wahren Identität unter Verwendung eines Pseudonyms ermöglicht. Der erste von ihnen ist ein persönlicher Schlüssel, der Details über die Identität der Person gibt, wobei der zweite ein öffentlicher Schlüssel ist, der mit dem persönlichen Schlüssel verknüpft ist und nur einen Spitznamen anzeigt [15].

Transaktionen werden verschlüsselt, wodurch sie sehr schwer zu durchdringen sind, und auf eine Weise verteilt, die eine Manipulation unmöglich macht. Darüber hinaus werden sie nach ihrer Ausführung niemals rückgängig gemacht. Bei Vertragsabschluss garantieren die Verschlüsselungs- und Verteilungsverfahren Verlust- und Veränderungsfreiheit und damit Transaktionsstabilität ohne Spielraum für Fälschungen und Betrug [15].

In der Phase der Implementierung des Smart Contracts spielen zwei wesentliche Merkmale eine wichtige Rolle für die Stabilität von Transaktionen [15]:

* Sofortige Durchsetzung, wobei die Umsetzung nicht mehr in den Händen einer Partei liegt

* und die Widerruflichkeit.

Vorteile und Nachteile von Smart Contracts

Vorteile

1. Sicherheit

Da Smart Contracts auf der Blockchain-Technologie basieren, sind sie mit Hilfe kryptografischer Maßnahmen gesichert und kommen was auch immer vor unbefugtem Zugriff [12].

2. Zuverlässigkeit

Perfekt programmierte Smart Contracts schließen Interpretationslücken in Vertragsklauseln nahezu vollständig aus [12].

3. Effizienz

Die automatisierten Transaktionen sparen viel Zeit, die bei der Verarbeitung vieler Papierdokumente auf herkömmliche Weise Z.B. beim Senden oder Übertragen an bestimmten Orten verloren geht [12].

4. Kein Dritter

Smart Contracts lösen das wichtigste Problem, das bei der Ausführung der Transaktion auftritt (das Vertrauensproblem zwischen den Parteien). Dritte wie Notare oder Rechtsanwälte sind bei Smart Contracts nicht unabdingbar notwendig [12].

5. Schnelligkeit:

Intelligente Verträge automatisieren Transaktionen mithilfe von Computerprotokollen und sparen Stunden dabei [12].

Nachteile

1. Eingeschränkte Modifikationsmöglichkeit

Smart Contracts sind fest und können nicht geändert werden. Problematisch wäre es beispielsweise, wenn das DAO gehackt würde. Millionen von Ethereum laufen Gefahr, aufgrund von Fehlern im intelligenten Vertragscode gestohlen zu werden.

2. Keine Garantien

Sinn und Zweck von Smart Contracts ist, dass alle Vertragspartner davon profitieren würden. Problematisch wird es, wenn jemand die Ware zurückgeben oder umtauschen möchte. Darüber hinaus ist der rechtliche Status von Smart Contracts ungewiss, sodass sie nicht zur aktuellen Rechtslage in verschiedenen Ländern auf der ganzen Welt passen.

Fazit

Blockchain-basierte Plattformen und Systeme entwickeln sich rasant weiter, da die Technologie zahlreiche Vorteile bietet und im Rahmen zahlreicher Anwendungen implementiert werden kann. Zudem bietet die Blockchain-Technologie nicht nur die fünf genannten Vorteile (Geschwindigkeit, Sicherheit, Datenintegrität, Netzzuverlässigkeit und Transparenz), sondern lässt sich auch in allen Geschäftsbereichen von Finanzen über Recht bis hin zum Internet der Dinge einsetzen.

Handelt es sich beim Kauf von Kryptowährung lediglich um die Übertragung von immateriellen Gegenständen, die weder Sachen noch Rechte sind, wobei der Veräußerer keinen Erfolg schuldet, kommt dann ein Kaufvertrag nach §453 Abs. 1 BGB zustande. Die Währungseinheiten sind dabei als sonstige Gegenstände gemäß § 453 Abs. 1 Alt. 2 BGB bzw. als sonstiges Recht i.S.d. § 823 BGB anzusehen. Anschließend kann nur das „Erschaffen“ neue Währungseinheiten oder die Nutzung von Rechenleistung (Mining) als Werk- oder Dienstvertrag behandelt werden [4]. Handelt es sich dagegen um eine Zahlung in Kryptowährung, so unterscheidet sich dabei zwei Fällen, Kauf- oder Tauschvertrag (auf den ursprünglichen Parteiwillen kommt es an) und Kryptowährung als Gegenleistung beim Werk- und Dienstvertrag.

Wie binnen jeglicher Technik, bringt ebenfalls der Einsatz von Smart Contracts gewisse Benefits und Nachteile, da Smart Contracts aus von Menschen geschriebenem Computercode erstellt werden und daher viele Konsequenzen haben, einschließlich der Tatsache, dass der Code Fehlern und Schlupflöchern unterliegt.

Letztlich sind Smart Contracts daher nicht mehr und nicht weniger als Tools bzw. Programme, die einen Vertrag automatisch ausführen [13][14].

Literaturverzeichnis

- [1] Schlatt, V., A., Urbach, N., und Fridgen, G. 2016. Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, <https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/642/wi-642.pdf>, zuletzt abgerufen am: 05.05.2022
- [2] David, Knutson. 2018, 08.Mai. Was ist die Blockchain und warum wird sie die Wirtschaft revolutionieren?. Schroders. [URL:https://www.schroders.com/de/de/privatanleger/insights/maerkte/was-ist-blockchain-und-warum-wird-sie-die-wirtschaft-revolutionieren/](https://www.schroders.com/de/de/privatanleger/insights/maerkte/was-ist-blockchain-und-warum-wird-sie-die-wirtschaft-revolutionieren/), zuletzt abgerufen am: 05.05.2022
- [3] Wikipedia. 2021, September. Know your Customer. https://en.wikipedia.org/wiki/Know_your_customer, zuletzt abgerufen am: 05.05.2022
- [4] SHMATENKO, MÖLLENKAMP. 2018, 12.Juni. Digitale Zahlungsmittel in einer analog geprägten Rechtsordnung. <file:///C:/Users/Samr%20Alakrad/Downloads/SSRN-id3673969.pdf>, zuletzt abgerufen am: 05.05.2022
- [5] BTC ACADEMY. Bitcoin Mining. <https://www.btc-echo.de/academy/bibliothek/was-ist-bitcoin-mining/#:~:text=Wie%20funktioniert%20Bitcoin%20Mining%3F,Liste%20zusammenf%C3%BCgt%20%E2%80%93%20der%20sogenannte%20Block>, zuletzt abgerufen am: 05.05.2022
- [6] Gruber. Mining: So funktioniert das Schürfen nach Bitcoin. <https://futurezone.at/digital-life/mining-so-funktioniert-das-schuerfen-nach-bitcoin/400002913>, zuletzt abgerufen am: 05.05.2022
- [7] Jörn, Ergbuth; Joachim Galileo, Fasching. 2017. Wer ist Verantwortlicher einer Bitcoin-Transaktion? Zielkens: Datenschutz im kommunalen Straßenverkehrswesen, 561-565, <https://erbguth.ch/ZD12-2017.pdf>, zuletzt abgerufen am: 05.05.2022
- [8] Frank, Thole; Dr. Arthur, Dill; Peter, Schmitz. 2020, 28.April. Die Blockchain revolutioniert das Finanzwesen. Blockchain Insider. <https://www.blockchain-insider.de/die-blockchain-revolutioniert-das-finanzwesen-a-927206/>, zuletzt abgerufen am: 05.05.2022
- [9] Dirk, Siegel. Was sind die Chancen und Risiken der Blockchain?

URL:https://www2.deloitte.com/de/de/pages/innovation/contents/Blockchain-Game-Changer.html, zuletzt abgerufen am: 05.05.2022

[10] Leidecker. Untersuchung zu Potentialen der Blockchain-Technologie im öffentlichen Sektor. https://opus.bsz-bw.de/hsf/frontdoor/deliver/index/docId/953/file/Leidecker_Oliver-Masterarbeit.pdf, zuletzt abgerufen am: 05.05.2022

[11] Jana Essebier / Dominic A. Wyss, Von der Blockchain zu Smart Contracts, 24. April 2017.

https://www.vischer.com/fileadmin/uploads/vischer/Documents/Activities/JES_DOWY_Jusletter_Blockchain_04_2017.pdf, zuletzt abgerufen am: 05.05.2022

[12] Elzbeita Kliszcz, Smart Contracts – alles was man wissen muss, 16 Sep 2021 <https://imbstudent.donau-uni.ac.at/blockchain-mehr-als-nur-krypto/smart-contracts/>, zuletzt abgerufen am: 05.05.2022

[13] Jakob Junghöfer, Verbraucherverträge als Smart Contracts, Januar 2021 <https://ul.qucosa.de/api/qucosa%3A78097/attachment/ATT-0/>, zuletzt abgerufen am: 05.05.2022

[14] Prof. Dr. Dirk Heckmann, Alexander Schmid, Blockchain und Smart Contracts Recht und Technik im Überblick, Oktober 2017 https://www.vbw-bayern.de/Redaktion/Freizugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2019/Downloads/190509-Blockchain-und-Smart-Contracts_neu.pdf, zuletzt abgerufen am: 05.05.2022

[15] Michèle Finck, Grundlagen und Technologie von Smart Contracts, 2019 <https://www.jstor.org/stable/pdf/j.ctvn96h9r.4.pdf>, zuletzt abgerufen am: 05.05.2022

[16] Thomas Joos. 01.09.2021. Wie funktionieren Smart Contracts. <https://www.blockchain-insider.de/wie-funktionieren-smart-contracts-a-1049794/>, zuletzt abgerufen am: 05.05.2022

Erklärung

Hiermit erklären wir, dass wir die vorliegende Arbeit selbständig angefertigt haben. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut haben wir als solches kenntlich gemacht. Die vorgelegte Arbeit hat weder in der gegenwärtigen noch in einer anderen Fassung schon einem anderen Fachbereich der Hochschule Ruhr West oder einer anderen wissenschaftlichen Hochschule vorgelegen.

Essen, den 05. 05. 2022

Ort, Datum



Unterschriften

Essen, den 05. 05. 2022

Ort, Datum



Unterschriften