FAKULTÄT FÜR !NFORMATİK
Faculty of Informatics

Smart Contracts

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Informatik

eingereicht von

D.I. Jürgen Wenisch
Matrikelnummer 8606182

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Ao. Univ.-Prof. Mag. Dr. Markus Haslinger

Wien, TT.MM.JJJJ

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Smart Contracts

DIPLOMA THESIS

Submitted in partial fulfilment of the requirements for the degree of

Diplom-Ingenieur

in

Informatik

by

D.I. Jürgen Wenisch
Registration Number 8606182

to the Faculty of Informatics
at the Vienna University of Technology

Betreuung:
Ao. Univ.-Prof. Mag. Dr. Markus Haslinger

Wien, TT.MM.JJJJ

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Erklärung zur Verfassung der Arbeit

Jürgen Wenisch

1160 Wien

Chlumberggasse 2

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen – die anderen Werken im Wortlaut oder dem Sinn nach entnommen worden sind, auf jeden Fall unter der Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 15.11.2017

Danksagung

Mein Dank gilt den Mitgliedern meiner Familie und meinen Freunden, die mich in den letzten Monaten bei der Anfertigung der Arbeit unterstützt und mir den „Rücken freigehalten“ haben. Besonderer Dank gebührt dabei meiner Mutter, und meiner Lebenspartnerin Nicole.

Bei Prof. Dr. Haslinger möchte ich für das in mich gesetzte Vertrauen und dafür bedanken, dass er mir freie Hand bei der Anfertigung der Arbeit gelassen hat und dabei immer als Ansprechpartner zur Verfügung gestanden ist.

Schließlich ist es mir ein Anliegen, auf die Bedeutung der Energiequellen Ukki, Shinno, Ashra, Fritzi und deren Freundeskreis hinzuweisen.

Anmerkungen

Das Recht ist männlich – besonders im Jahr 1811, in dem das Allgemeine Bürgerliche Gesetzbuch veröffentlicht wird. Da das ABGB immer noch das zentrale Werk des österreichischen Privatrechtes ist, muss man sich mit Gesetzestexten auseinandersetzen, in denen weibliche Personen bestenfalls mitgedacht, aber nicht benannt werden.

Um diese Schieflage auszugleichen, wird im ersten Teil der Arbeit, sobald Personen angesprochen werden, vorwiegend die weibliche Form verwendet. Auf Binnen-i und die ständige Nennung beider Geschlechter wird aus Gründen der leichteren Lesbarkeit verzichtet.

Kurzfassung

Neben der Kryptowährung Bitcoin werden Smart Contracts als Hauptanwendung der Blockchain-Technologie gesehen. Die Blockchain wird allgemein als dezentrales, verschlüsseltes Kontenbuch beschrieben, das es erlaubt, ohne zentrale Vermittlungsstelle beliebige Arten von Transaktionen zwischen Teilnehmern durchzuführen. Mithilfe eines geeigneten Algorithmus wird eine digitale Zusage an einen Vertragspartner gegeben, die beim Eintreten einer vorbestimmten Voraussetzung automatisch eingelöst wird und damit die Vertragsleistung automatisch erbringt.

Die potentiellen Anwendungsgebiete sind mannigfach. Sie reichen über die Möglichkeit, ein elektronisches Grundbuch zu führen, den Handel mit Strom oder Rechenleistung zwischen Verbrauchern, Zugangskontrolle zu Räumen oder Mietfahrzeugen über elektronische Schlösser, Sicherung der Authentizität von Geschäftspartnern bis zu Bereichen des e-Governments wie elektronisch unterstützten Wahlen.

Allerdings sind nach Ansicht zahlreicher Juristen die rechtlichen Rahmenbedingungen für derartige smarte Verträge derzeit noch weitgehend ungeklärt.

Das österreichische Zivilrecht räumt den Rechtssubjekten einerseits viele Freiheiten zur Gestaltung ihrer Rechtsverhältnisse ein, andererseits sind auch die dadurch nötigen Schutzmechanismen zahlreich.

Diese Arbeit beschäftigt sich mit der Frage, ob Smart Contracts grundsätzlich als Verträge im Sinne des österreichischen Zivilrechtes gesehen werden müssen, mit Beschreibung der Anwendungen und Umsetzungsmöglichkeiten von Smart Contracts und mit notwendigen Erweiterungen durch die Vorgaben des österreichischen Privatrechts.

Stichworte: Verträge, Vertragsrecht, Blockchain, Smart Contracts, Algorithmen

Abstract

In addition to the cryptocurrency Bitcoin, smart contracts are seen as the main application of blockchain technology. The blockchain is generally described as a decentralized, encrypted account book, which allows to carry out arbitrary types of transactions between participants without a central exchange. By means of a suitable algorithm, a digital promise is given to a contract partner, which is automatically solved on the occurrence of a predetermined prerequisite and thus automatically performs the contract's content.

The potential applications are manifold. They provide the opportunity to manage an electronic land register, trade in electricity or computing power between consumers, access control to apartments or rental vehicles through electronic locks, securing the authenticity of business partners, to areas of the e-Governent, such as electronically supported elections.

However, according to numerous lawyers, the legal framework for such smart contracts is still largely unresolved.

On the one hand, Austrian civil law confers on lawyers many freedoms for the shaping of their legal relations; on the other hand, the necessary protective mechanisms are numerous.

This thesis deals with the question of whether Smart Contracts have to be seen as contracts in the sense of Austrian civil law, with a description of the applications and implementation possibilities of Smart Contracts and with necessary extensions by the provisions of Austrian private law.

Keywords: Contracts, Contract Law, Blockchain, Ethereum, Algorithm

Inhaltsverzeichnis

1 Einleitung

1.1 Die Idee eines Smart Contract

Die Idee eines Smart Contract wurde zum ersten Mal 1995 vom Computerwissenschaftler Nick Szabo vorgestellt[1]. Er prognostizierte, dass mit der kostengünstigen Entwicklung geeigneter Algorithmen eine Menge an „digitalen Zusagen“ an Vertragspartner gegeben werden konnten, die bei Eintreten gegebener Voraussetzungen durch einen Vertragspartner automatisch eingelöst werden konnten. Mit diesen Zusagen könnten rechtlich bindende Verhältnisse geschaffen werden, die mit einem herkömmlichen, in der analogen Welt existierenden Vertrag zu vergleichen wären.[2]

Allerdings sind nach Ansicht zahlreicher Juristen die rechtlichen Rahmenbedingungen für derartige Verträge derzeit noch weitgehend ungeklärt.[3]

1.1.1 Ziel der Arbeit

Das Ziel der vorliegenden Arbeit ist die Analyse der möglichen Auswirkungen von automatisiert geschlossenen Verträgen auf das österreichische Rechtssystem.

Die der Blockchain zugrundeliegenden Technologien werden dargestellt, ebenso wie Anwendungsbeispiele für Smart Contracts. Außerdem werden die Bausteine des österreichischen Privatrechts präsentiert und mögliche Divergenzen der beiden Systeme herausgearbeitet.

Aus diesen Darstellungen sind folgende Forschungsfragen ableitbar:

- Inwieweit können Smart Contracts als Verträge im Sinn des Österreichischen Privatrechtes gesehen werden?

---

[1] *(Szabo, 1997)*

[2] *(Gord, 2016)*

[3] *(Heckmann & Kaulartz, 2016, S. 138)*

- Steht die automatische Exekution eines Smart Contract im Widerspruch zu den Sicherheitsnetzen, die das österreichische Zivilrecht seinen Rechtsunterworfenen im Fall des Abschlusses eines Rechtsgeschäftes gewährt?
- Besteht Handlungsbedarf für die Gesetzgebung, beispielsweise aufgrund der fehlenden technischen Möglichkeit der nachträglichen Vertragsaufhebung und „-vernichtung“ in durch die Blockchain gespeicherten Verträgen?

1.2 Eine Kryptowährung entsteht

Zentrale Institutionen wie Geldinstitute leben vom Vertrauen ihrer Kunden. Dieses Vertrauen wurde vor etwa 10 Jahren einer Probe unterzogen, als im Jahr 2007 eine globale Finanzkrise die Bankenwelt und den globalen Zahlungsverkehr erschütterte. Im Jahr 2008, kurz nach Ausbruch der Finanzkrise, erschien die Publikation „Bitcoin: A Peer-to-Peer Electronic Cash System“.[4]
Der Name des Autors, Satoshi Nakamoto, ist ein Pseudonym. Es ist bis heute nicht bekannt, ob es sich dabei um eine Einzelperson, eine Gruppe von Forschern oder um eine Institution handelt.
Sein (oder ihr) Ziel war es, ein Zahlungssystem zu entwerfen, das ohne die Funktion einer Vermittlungsstelle, also peer-to-peer, auskommt. Eine reine „peer-to-peer“ Version von elektronischem Geld sollte es ermöglichen, dass Online-Zahlungen direkt von einer Partei zur anderen geschickt werden, ohne ein Finanzinstitut zu durchlaufen.[5]

Nakamotos Publikation schlägt eine Lösung mittels digitaler Signaturen und in einer laufenden Kette zusammengefasster Transaktionen mit Zeitstempeln in einem dezentralen Netzwerk vor. Das Problem möglicher doppelter Transaktionen soll daher nicht von einer zentralen Vermittlungsstelle wie einem Bankinstitut überwacht werden, sondern durch die Kontrolle mittels der längsten Transaktionskette und der bei der Erstellung notwendigen maximalen Rechenleistung.

Die längste Kette dient nicht nur als Beweis für die Reihenfolge der Ereignisse mittels Zeitstempel, sondern ist auch der Beweis dafür, dass sie aus dem größten Pool der CPU-Leistung kam. Solange eine Mehrheit der

[4] *(Nakamoto, 2008)*

[5] *(Nakamoto, 2008, S. 1)*

CPU-Leistung von Knoten gesteuert wird, die nicht kooperieren, um das Netzwerk anzugreifen, erzeugt sie die längste Kette und überholt etwaige Angreifer.

Die Nachrichten über neue Transaktionen werden im Takt weniger Minuten verteilt, und die autonomen Netzknoten des peer-to-peer Netzes können dieses nach Belieben verlassen und ihm auch wieder beitreten. Beim Beitritt dient wieder die längste Transaktionskette als Beleg für die in der Zwischenzeit durchgeführten Transaktionen.

1.3 Merkmale

Als Vorteil dieser Technologie wird angepriesen, dass man Transaktionen eben nicht mehr an eine zentrale Vermittlungsstelle (z.B. Banken oder andere Zahlungsdienstleister) auslagern muss, deren Redlichkeit man ebenso vertrauen muss wie deren technischer Verlässlichkeit. Vielmehr sei man selbst Vermittlungsstelle und habe als Teil des Netzwerkes die volle Information über sämtliche Vorgänge.

Die Verschlüsselung wiederum stellt sicher, dass der Zugriff auf diese Daten nur durch autorisierte Endgeräte erfolgen kann und jede nachträgliche Änderung nachvollziehbar ist. Somit wird sowohl die Authentizität als auch die Integrität der Daten sichergestellt.

Nachfolgend eine Listung der wichtigsten Vorteile:

- Dezentrale Speicherung der Daten: Die Daten werden nicht, wie bei Server – Client Setups, an einer zentralen Stelle, sondern gleichermaßen auf allen Netzwerkknoten gehalten.

- Schutz vor nachträglicher Änderung: Die nachträgliche Änderung einer Transaktion wird Verwendung kryptographischer Methoden und Verkettung der Transaktionsblöcke nahezu unmöglich gemacht. Je weiter die Transaktion, die ein Angreifer manipulieren möchte, zurückliegt, desto höher ist der zu betreibende Rechenaufwand.

- Pseudonymer Zugang: Die Nutzer der Blockchain sind nur durch ihre öffentlichen Schlüssel registriert. Die Klarnamen sind nicht gespeichert und damit nicht rückverfolgbar. Erst durch die Analyse sehr vieler Transaktionsdatensätze und statistischer Methoden ist es denkbar,

dass Rückschlüsse auf Personen gezogen werden können.

- Transparenz der Einträge: Da die gesamte Blockchain auf alle teilnehmenden Netzwerkknoten verteilt und aktuell gehalten wird, ist das Transaktionsaufkommen prinzipiell für jede Person nachvollziehbar.

- Verwendung einer Kryptowährung: Bei Transaktionen stehen eigene Kryptowährungen zur Verfügung, die als Gegenwert für durch die Blockchain verwaltete Leistungen verwendet werden können.

- Absicherung durch ein Anreizsystem: Die Gültigkeit der einzelnen Transaktionen wird die Nutzer bestätigt. Der Einsatz des dafür nötigen Rechenaufwandes wird mit einem Prämiensystem belohnt. Dies macht es für etwaige Angreifer wirtschaftlich vorteilhafter, ihre Rechenleistung in die Bestätigung zu investieren anstatt in Attacken. [6]

[6] *Auflistung übernommen aus (Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 17)*

2 Technische Grundlagen am Beispiel Bitcoin

Für die Beschreibung der Blockchain-Technologie, die einen Teil der Grundlage für Smart Contracts bildet, ist das Beispiel Bitcoin aus zwei Gründen geeignet. Einmal ist Bitcoin das erste groß gewordene Projekt, das sich dieser Technologie umfassend bedient und gerade durch seine weltweite Verbreitung (Stand Herbst 2017) auf die Bedeutung der Blockchain hinweist.

Außerdem kann die Plattform, die als Basis für den Smart Contract dient, als Erweiterung der für Bitcoin verwendeten „Urform" verstanden werden. Buterin weist in seinem Ethereum White Paper sowohl auf die Beschränkungen im Bitcoin-System, die es zu überwinden galt als auch auf die Lösungswege, die zur Überwindung dieser Beschränkungen eingeschlagen wurden.[7]

2.1 Funktionsablauf

Das Kompetenzzentrum öffentliche Informationstechnologie (ÖFIT) des Fraunhofer-Instituts für offene Kommunikationssysteme beschreibt die Blockchain folgendermaßen:

Die Blockchain ist ein IT-Werkzeug, das verteilte Transaktionsabwicklung ohne Mittelsmann unterstützt. Die geografisch verteilten Nutzer einer Blockchain sind dafür verantwortlich, dass die durch die Blockchain verwalteten Transaktionen im Konsens genehmigt, durchgeführt und nachvollziehbar protokolliert werden.[8]

Die Blockchain ist ein peer-to-peer-Netzwerk. Jede Nutzerin nimmt über ihr Endgerät, also Computer, Mobiltelefon oder Tablet, auf dem die Blockchain-Software installiert ist, an dem Netzwerk teil. Die teilnehmenden Personen sind nicht über Klarnamen, sondern über Pseudonyme registriert. Dies sichert deren Anonymität.

Durch die Anmeldung wird ein „Wallet" vergeben. Dies ist ein persönliches Konto, mit dem das Guthaben an Bitcoins verwaltet wird. Bitcoin steht dabei für die Kalkulationseinheit, mit der über das Netzwerk kommuniziert wird, also als Name für die virtuelle Währung des Netzwerkes.

---

[7] *(Buterin, 2013)*

[8] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 8)*

Die Kommunikation zwischen Nutzern des Netzwerkes erfolgt über sogenannte Transaktionen. Dabei wird eine Kalkulationseinheit vom Wallet A auf das Wallet B übertragen. Der Kontostand von Wallet A wird also durch diese Transaktion um einen Betrag s verringert, und der Kontostand von Wallet B um den Betrag s erhöht.

Um der Sicherheit Rechnung zu tragen, sind Transaktionen und Nutzerzugänge verschlüsselt. Jede Teilnehmerin hält ein Paar aus öffentlichem und privatem Schlüssel, mit dem der sowohl der eigene Zugang zum Wallet ermöglicht wird, als auch eine Transaktion signiert wird, um deren Herkunft sicherzustellen.

Damit ist die Transaktionshistorie der Blockchain für jede Teilnehmerin nachvollziehbar: die Transaktionsbeträge sind erkennbar, Quelle und Ziel der Transaktion sind allerdings durch das Pseudonym geschützt.[9]

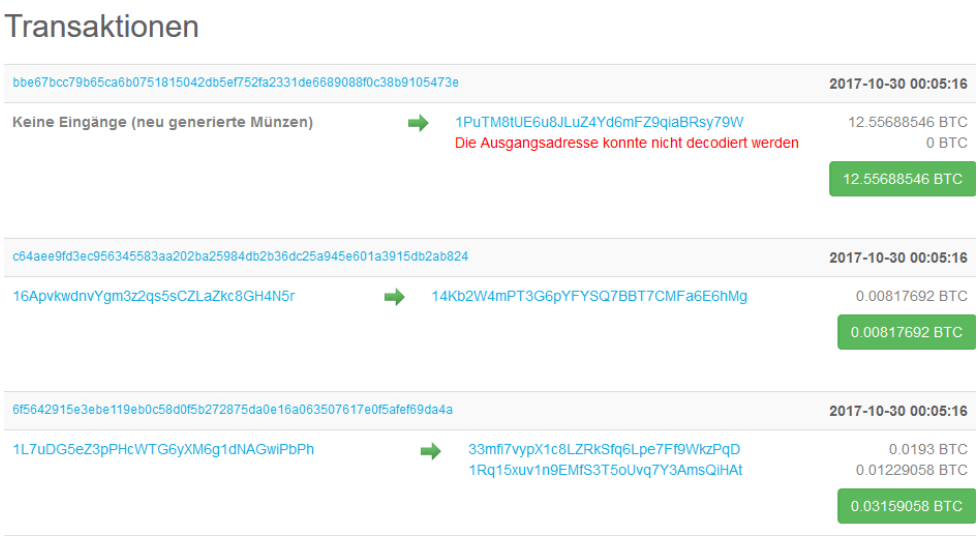
Die folgenden Abbildungen zeigen den Auszug einer Liste von Blöcken und den Auszug einer Liste von Transaktionen. Datum, Blockgröße und Größe der Transaktion sind ablesbar, Quelle und Ziel der Transaktionen sind durch eine Hashfunktion verschlüsselt.

[9] *Die Webadresse https://blockchain.info/de zeigt eine Liste der letzten erstellten Blöcke, durch Aufrufen eines Blockes werden die einzelnen Transaktionen sichtbar.*

<< Zurück **Blöcke gemined von 30/10/2017** Weiter >>

Höhe	Zeit	Hash	Größe (kB)
492273 (Hauptkette)	2017-10-30 00:05:16	00000000000000000a55e001663dea70e8c1be6d16a2bbcee0c5e2520a52eca	9.08
492274 (Hauptkette)	2017-10-30 00:10:01	000000000000000000935a64c0f5b863fe22c1928aa20daa4afd5a04705e35ea	1,055.02
492275 (Hauptkette)	2017-10-30 00:38:21	00000000000000000ae54fdd9ab802739cf80b567118d2a8f9431c9cca2b040	999.28
492276 (Hauptkette)	2017-10-30 00:41:55	00000000000000000b387d73485b358b1863b5864e68fe7d972b28f932eb675	1,108.2
492277 (Hauptkette)	2017-10-30 01:08:00	00000000000000000a0138d6ae237715da93e1e178d046b786c482e676d46bd	1,000.01
492278 (Hauptkette)	2017-10-30 01:17:48	000000000000000000727f1e8d25a964f533b0a959e2017f834c341d9996ea39	1,042.4
492279 (Hauptkette)	2017-10-30 01:19:30	00000000000000000009c55207c2be8bb05a93b9baa2555bba81209cf6cfe837e	998.21
492280 (Hauptkette)	2017-10-30 01:42:32	000000000000000000047f19060a3deb3cfecfa19d9270d4c9409a14bebd91d01	1,035.13
492281 (Hauptkette)	2017-10-30 01:53:53	000000000000000000742f775d8aeecc5b6d4a7d5d9ce468a66a3a3b2a8da32c	1,139.87
492282 (Hauptkette)	2017-10-30 01:54:33	000000000000000000099dc80ef6851f91ad126134fdb6e8f54889f9bf711ab44	1,106.12
492283 (Hauptkette)	2017-10-30 02:05:52	000000000000000000b38ed1abc10d188ec1334136787fe6c513209b3fe5c0a	1,049.57
492284 (Hauptkette)	2017-10-30 02:19:35	000000000000000002e5b52131810ce2541420f5a78ff0414d3f5029289902b	1,040.78

Abb. 1: Blöcke der Bitcoin Blockchain[10]



Transaktionen

bbe67bcc79b65ca6b0751815042db5ef752fa2331de6689088f0c38b9105473e — **2017-10-30 00:05:16**

Keine Eingänge (neu generierte Münzen) → 1PuTM8tUE6u8JLuZ4Yd6mFZ9qiaBRsy79W (Die Ausgangsadresse konnte nicht decodiert werden) — 12.55688546 BTC, 0 BTC

12.55688546 BTC

c64aee9fd3ec956345583aa202ba25984db2b36dc25a945e601a3915db2ab824 — **2017-10-30 00:05:16**

16ApvkwdnvYgm3z2qs5sCZLaZkc8GH4N5r → 14Kb2W4mPT3G6pYFYSQ7BBT7CMFa6E6hMg — 0.00817692 BTC

0.00817692 BTC

6f5642915e3ebe119eb0c58d0f5b272875da0e16a063507617e0f5afef69da4a — **2017-10-30 00:05:16**

1L7uDG5eZ3pPHcWTG6yXM6g1dNAGwiPbPh → 33mfi7vypX1c8LZRkSfq6Lpe7Ff9WkzPqD, 1Rq15xuv1n9EMfS3T5oUvq7Y3AmsQiHAt — 0.0193 BTC, 0.01229058 BTC

0.03159058 BTC

Abb. 2: Bitcoin Transaktionen[11]

[10] *Aus: https://blockchain.info/de/blocks/1509373767723 (Screenshot vom 30.10.2017)*

[11] *Aus: https://blockchain.info/de/block/00000000000000000a55e001663dea70e8c1be6d16a2bbcee0c5e2520a52eca (Screenshot vom 30.10.2017)*

Um eine gültige Transaktion durchzuführen, durchläuft die Blockchain-Software mehrere Schritte. Zuerst wird überprüft, ob der Guthabenstand hoch genug ist, um die Transaktion durchzuführen. Trifft dies zu, so wird der durch eine Hashfunktion codierte Inhalt der Transaktion an bekannte Netzwerkknoten weitergeleitet, welche diese Transaktion ihrerseits auch an die ihnen bekannten Knoten weiterleiten. Auf diese Art erfolgt eine kaskadenartige Verbreitung der Transaktion durch das Netzwerk. Damit wird der Wunsch, dass Wallet A eine Transaktion durchführen will, im gesamten Netzwerk bekannt. [12]

Die Aufgabe der Empfänger dieser Nachricht besteht nun darin, die Transaktion zu verifizieren und eine Übereinstimmung über diese Verifikation – den *Consensus* – zu erzielen. Die Erfüllung dieser Aufgabe erfolgt freiwillig und ist mit einem hohen Rechenaufwand verbunden.

Als Folgeschritt der Verifikation erfolgt der Eintrag dieser Transaktion in das Kontenbuch.[13] Dabei werden alle gegenwärtig offenen Transaktionen in einem Transaktionsblock zusammengefasst und dieser an die bisher existierende Kette von Blöcken angehängt. Als Anreiz und Gegenleistung für die dafür erforderliche Rechenleistung winkt der „Gewinnerin", also der Person, die die Transaktionen als erste bestätigen konnte, eine Gutschrift auf ihrem Konto. Diese Gutschrift beträgt gegenwärtig 12,5 BTC.

Halter, die sich an diesen Aufgaben beteiligen, werden „Miner" genannt. Da diese Tätigkeit einen hohen Rechenaufwand und damit auch einen hohen Aufwand an Energiekosten erfordert, hat sich mittlerweile das Mining weg von Privatpersonen zu Rechenzentren mit Spezialhardware und –software verlegt, an denen sich wiederum Privatpersonen beteiligen können, um an der Gutschrift zu partizipieren.

Das Konto des Miners, dem es gelingt, einen neuen Block zu erzeugen und ihn an die Kette anzuhängen, informiert die anderen Miner automatisch über die Verlängerung der Kette, damit die Transaktionen, die vom neuesten Block erfasst wurden, nicht weiter berücksichtigt werden.

Die übrigen Miner überprüfen die Gültigkeit des neuen Blockes. Sollten dabei Fehler gefunden werden, dann wird der letzte Block entfernt, die darin enthaltenen Transaktionen wieder zur Zusammenfassung freigegeben und

---

[12] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 8)*

[13] *Gebräuchlich ist der englische Begriff „Ledger".*

die Blockbildung erfolgt erneut. Fehler können dadurch entstehen, dass einzelne Transaktionen nicht durch die Guthaben des auslösenden Wallets gedeckt sind, weil beispielsweise zu viele Transaktionen zu schnell hintereinander abgewickelt werden, ohne dass die jeweiligen Vortransaktionen rechtzeitig bestätigt wurden. Dieses Problem wird typischerweise entdeckt, ist aber mit einer gewissen Latenzzeit behaftet. Die Erzeugung der Blöcke der Bitcoin-Blockchain erfolgt im Abstand von etwa zehn Minuten. Innerhalb dieser Zeit kann es also zu ungültigen Transaktionen kommen, die bei der Bildung eines Blockes, der auch diese fehlerhaften Transaktionen enthält, entdeckt werden.

In den folgenden Abschnitten werden die Bausteine, die zu einer erfolgreichen Bildung einer Blockkette erforderlich sind, genauer behandelt.

2.2 Netzwerk

Das Netzwerk ist die Summe aller Netzknoten, die eine Instanz der Blockchain-Software betreiben. Alle Netzknoten enthalten also die Kette der digitalen Signaturen.

Folgende Netzwerkoperationen sind zum Betrieb des Netzes erforderlich:[14]

1. Jede neue Transaktion wird an alle Knoten weitergeleitet.
2. Jeder Knoten fasst neue Transaktion zu Blöcken zusammen.
3. Jeder Knoten nimmt an der Berechnung des proof-of-work[15] für den aktuellen Block teil.
4. Der Knoten, der es schafft, den proof-of-work zu berechnen, leitet den damit bestätigten Block an alle Netzknoten weiter.
5. Die Netzknoten akzeptieren den neuen Block nur, wenn alle darin aufgenommenen Transaktionen gültig sind.
6. Wird ein Block akzeptiert, dann arbeiten die Knoten am nächsten Block der Kette, indem sie den Hash des letzten akzeptierten Block als den Vorgängerhash für den neuen Block verwenden.

Für den Fall, dass zwei Netzknoten verschiedene Versionen des letzten Blockes gespeichert haben und diese gleichzeitig an die anderen Knoten verbreiten, dann werden beide Versionen der Kette gespeichert. Jeder Knoten entscheidet anhand des Zeitstempels des Eintreffens, an welcher Version er weiterarbeitet. Sollte allerdings die andere Version durch einen neuen erfolgreichen proof-of-work länger werden, so wird seine Version der Kette verworfen und die andere Version als die neue längste Kette akzeptiert.

Sollte durch eine Störung im Netzwerk, oder dadurch dass eine Benutzerin sich temporär aus dem Netz abgemeldet hat, ein Block nicht an alle Knoten verteilt worden sein, dann fällt dies auf, sobald der nächste Block eintrifft, und die fehlerhafte Kette wird durch Anforderung des fehlenden Blockes erneuert. Dieser Mechanismus funktioniert nur unter der Voraussetzung, dass alle Blöcke zumindest von vielen Netzknoten erreicht werden.

---

[14] *Auflistung nach: (Nakamoto, 2008, S. 3)*

[15] *Siehe Kap. 2.6.3*

2.3 Verschlüsselung

2.3.1 Asymmetrische Kryptographie

Jede Nutzerin hält ein zusammenhängendes Schlüsselpaar aus öffentlichem und privatem Schlüssel. Der öffentliche Schlüssel (public key) wird an potentielle Kommunikationspartner weitergegeben, in dem er beispielsweise auf einem Keyserver hinterlegt wird. Der private Schlüssel (private key) darf jedoch nur von der jeweiligen Nutzerin verwendet werden und muss Außenstehenden gegenüber geheim gehalten werden.

2.3.1.1 Verschlüsselung von Nachrichten

Ein klassischer Anwendungsfall ist der der verschlüsselten Übermittlung von Nachrichten von Person A zu Person B. Da B seinen öffentlichen Schlüssel an A weitergegeben hat, kann A ihre Nachricht mit diesem Schlüssel verschlüsseln. B kann nun seinen privaten Schlüssel dazu verwenden, um die mit seinem öffentlichen Schlüssel generierte Nachricht wieder zu entschlüsseln.

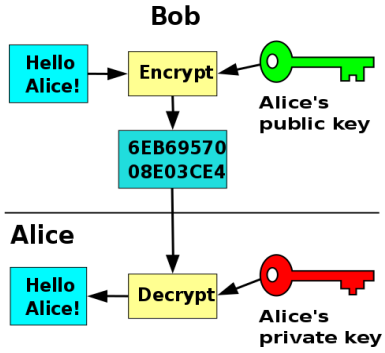


Abb. 3: Asymmetrische Verschlüsselung[16]

2.3.1.2 Digitale Signatur

Ein anderer Anwendungsfall ist die digitale Signatur von Nachrichten. Durch digitale Signatur kann die Authentizität einer Nachricht überprüft werden, also festgestellt werden, ob die Nachricht auch wirklich von der erwarteten Person stammt.
Als Beispiel kann A eine Nachricht an B senden, und B möchte sicherstellen,

[16] *Abbildung aus (Public-Key-Verschlüsselungsverfahren)*

dass diese Nachricht auch sicher von A stammt. A wird ihre Nachricht mit ihrem privaten Schlüssel signieren und diese an B übermitteln. B kann den öffentlichen Schlüssel von A nun dazu verwenden, um festzustellen, ob die Nachricht authentisch ist. Damit kann B ausschließen, dass ein bösartiger „man-in-the-middle“ die Nachricht abgefangen hat und durch eine neue Nachricht ausgetauscht oder modifiziert hat.

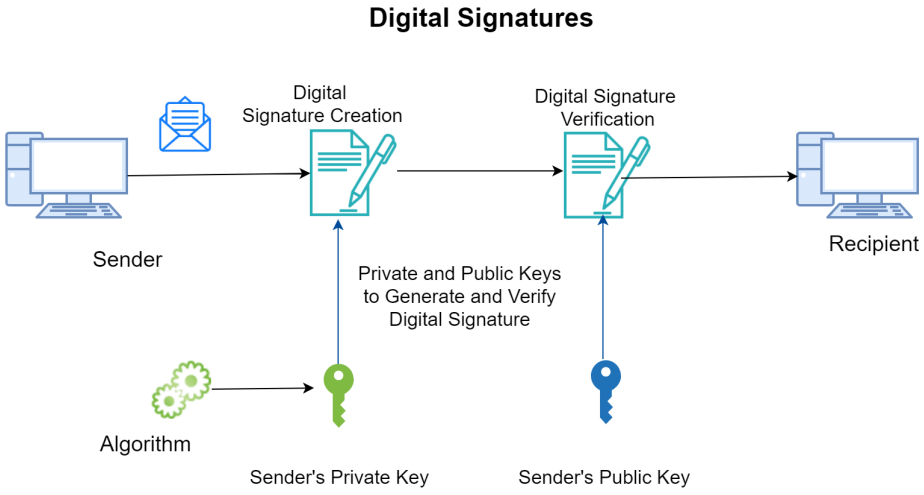


Abb. 4: Digitale Signatur mittels asymmetrischer Kryptographie[17]

Digitale Signaturen sind ein wesentlicher Bestandteil der Bitcoin-Software. Sie werden zum Signieren von Transaktionen und bei der Erstellung von Blöcken eingesetzt.

2.3.2 Hashfunktionen

Eine Hashfunktion ist eine mathematische Funktion, die aus jeder beliebig langen Zeichenkette eine (üblicherweise hexadezimal dargestellte) Zeichenkette fixer Länge, den Hash, erzeugt. Dieselbe Zeichenkette wird bei jeder erneuten Anwendung wieder denselben Hash ergeben, allerdings wird auch nur die kleinste Veränderung der Eingangskette den erzeugten Hash komplett verändern. Man könnte diesen Hash zum besseren Verständnis auch als „Fingerabdruck“ der Zeichenkette bezeichnen.[18]

---

[17] *Aus: (Electronic Signatures v. Digital Signatures, 2017)*

[18] *(Menezes, van Oorschot, & Vanstone, 1996, S. 322 ff)*

Bitcoin verwendet SHA-256[19], eine Funktion aus der Familie der von der Amerikanischen NSA entwickelten SHA-2 Verschlüsselungsfunktionen.

SHA-2 ist eine Menge von sogenannten kryptographischen Hashfunktionen. Kryptographische Hashfunktionen zeichnen sich dadurch aus, dass sich kollisionssicher und Einwegfunktionen sind.

Kollisionssicherheit einer Hashfunktion H bedeutet, dass es keine zwei Zeichenfolgen X und Y gibt, sodass die Hashes H(X) und H(Y) der Zeichenfolgen gleich sind. Man definiert auch schwache Kollisionssicherheit als Eigenschaft von H, wenn es praktisch undurchführbar ist, zwei Zeichenfolgen X und Y zu finden, für die H(X) = H(Y), die Hashes der unterschiedlichen Zeichenfolgen also ident sind. Die Notwendigkeit für die Definition der schwachen Kollisionssicherheit besteht in der Tatsache, dass es auf der Welt beinahe unendlich viele verschiedene Texte X gibt[20], aber nur eine endliche Anzahl von Outputs einer Hashfunktion aus endlich vielen Zeichen und mit endlich vielen Stellen.

Einwegfunktionen haben die Eigenschaft, dass die Berechnung des Funktionswertes h=H(X) einfach[21] durchführbar ist, die umgekehrte Berechnung der Funktion $X=H^{-1}(h)$ vielfach schwerer zu berechnen ist. Man findet also – vereinfacht gesagt – keine Möglichkeit, aus einem erzeugten Hash wieder die ursprüngliche Zeichenkette zu erzeugen.

Als Beispiel für eine SHA-256-Verschlüsselung soll der Hashwert des Wortes „Schlüssel“ berechnet werden. Output der Hashfunktion ist immer ein 64 Zeichen langer Hexadezimalstring:

SHA256(Schlüssel)=1fbd7a00cacba0b89a31bb00cd29e60d3f86c08dd7806b
be891642214672af0c

Auf amerikanischer Tastatur (ohne den Buchstaben „ü“) wird der Hash zu:

SHA256(Schluessel)=4acb9ae585c153b5336d4dda305eb0bae8f5ba7c256de
150b7b24424fb5ca8ad

---

[19] SHA steht für Secure hash algorithm

[20] Sobald jeder Text eine beliebige Länge einnehmen darf, existieren auch beliebig viele Texte

[21] Damit meint man, in polynomialer Zeit durchzuführen

Und mit einem Flüchtigkeitsfehler:

SHA256(Schüssel)=5244656bb20decad8dc31300ac818b7b8ff18bb3472c6b4c158de54d7b482b20

Dies zeigt, dass kleine Änderungen im Eingangstext nicht nur kleine, sondern umfassende Änderungen im Funktionswert zur Folge haben. In der Kryptologie spricht man in diesem Zusammenhang von Lawineneffekt.[22]

Um zu zeigen, dass auch längere Texte zu diesem String aus 64 Zeichen führen:

SHA256(Der Schlüssel liegt in der Schüssel)=
132bb608849f88b95764624e6182b253e6cee8c6316d888435882668166bddea

In der Praxis verwendet die Bitcoin-Software den Schlüsselalgorithmus zweimal hintereinander, erzeugt also das Ergebnis aus SHA256(SHA256(x)).

Es bleibt zu erwähnen, dass Bitcoin an einigen Stellen, die kürzere Hexadezimalstrings erfordern, den Algorithmus RIPEMD160 einsetzt, der 40 Zeichen lange Ausgaben erzeugt.

Die Tatsache, dass die SHA-2-Funktionsmenge von der NSA entwickelt wurde, nährt natürlich den Verdacht, dass staatliche Stellen über Hintertüren Zugriff zur Verschlüsselung erhalten könnten. Zur Ausräumung dieses Verdachtes sind die Verschlüsselungsalgorithmen offengelegt und etwaige backdoors sollten durch Überprüfung des Quellcodes früher oder später gefunden werden.

[22] *(Giese, Kops, Wagenknecht, de Boer, & Preuss, 2016, S. 44)*

2.4 Transaktionen

Aus technischer Sicht kann Bitcoin als System zur Umwandlung von Zuständen, also als Zustandsübergangssystem gesehen werden. Der Ursprungszustand wird durch eine Übergangsfunktion (eine *Transaktion*) in einen Folgezustand umgewandelt werden.

Nakamoto definiert einen „*electronic coin*“, also eine digitale Münze, als eine Kette von digitalen Signaturen.[23]
Das Übertragen einer Münze vom ursprünglichen Besitzer A auf die Zielperson B erfolgt nach nachfolgender Beschreibung.

A erzeugt eine digitale Signatur aus dem Hash der vorgehenden Transaktion und dem öffentlichen Schlüssel von B und fügt diese erzeugte Signatur an das Ende der Kette digitaler Signaturen. Diese Signaturen sind überprüfbar, daher wird auch die Besitzhistorie der digitalen Münze überprüfbar.

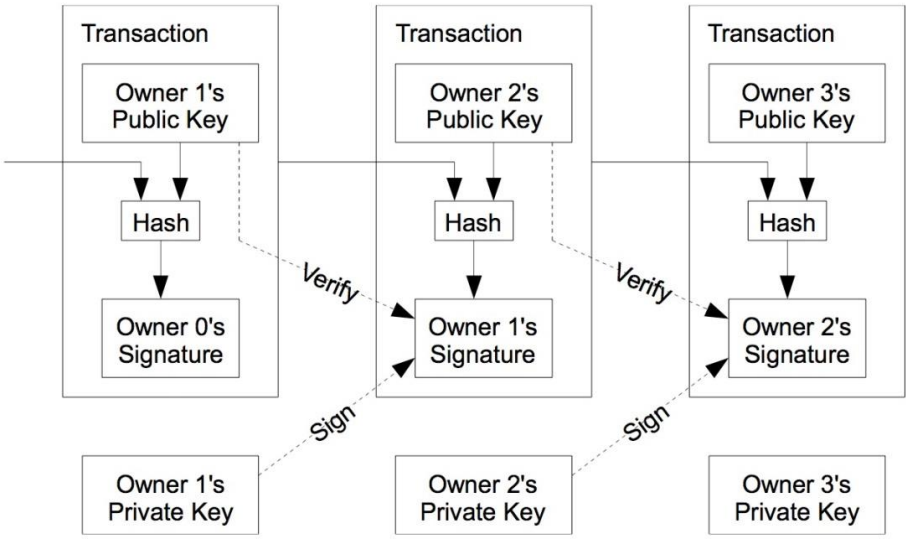


Abb. 5: Transaktionen und Verkettung[24]

[23] *(Nakamoto, 2008, S. 2)*

[24] *Abb. aus (Nakamoto, 2008, S. 2)*

Allerdings kann der Zahlungsempfänger nicht überprüfen, ob A diese Münze nur an ihn oder auch an eine andere Person weitergegeben hat. Bisher war zur Umgehung dieses Problems eine zentrale Kontrollstelle (etwa eine Bank) erforderlich, die das Vertrauen der Geschäftspartner A und B besaß und jede Transaktion zeitnah bestätigte. Dies schaffte eine Abhängigkeit des gesamten Zahlungssystems von dieser Kontrollstelle. Schwindet das Vertrauen in die Kontrollstelle, dann kann es passieren, dass Zahlungen zurückgehalten werden.[25]

Die zentrale Kontrollstelle verwendet zur Wahrung der Eindeutigkeit jeder Transaktion einen einfachen Weg: jede Münze wird von A auf das Konto der Bank eingezahlt und von dort an B ausgezahlt. Da A nur Münzen weitergeben kann, die sie hat, ist eine doppelte Überweisung ausgeschlossen.

In einem System ohne zentrale Kontrollstelle kann ähnlich vorgegangen werden, indem die Kontrollfunktion von allen anderen Teilnehmern am Zahlungssystem übernommen wird. Um dies ohne eine vertrauenswürdige Partei zu erreichen, müssen alle Transaktionen öffentlich zugänglich gemacht werden, die Kette digitaler Signaturen wird also für alle anderen einsehbar. Diese Kette muss zu jedem Zeitpunkt nur „legale“, also von der Mehrheit der Teilnehmer akzeptierte und bestätigte Transaktionen enthalten.

2.4.1 Zusammenfassen größerer Geldbeträge

Die bisher beschriebene Vorgangsweise zielt auf die Weitergabe einzelner Grundeinheiten ab. Bei der Zahlung größerer Geldbeträge ist es jedoch wenig praktikabel, eine Summe von Transaktionen seriell zu starten, deren Wert jeweils nur 1 Coin beträgt. Vielmehr möchte man einzelne coins zu einer größeren Summe zusammenfassen und diese Summe mittels einer Transaktion an die Empfängerin übertragen. Um dies zu ermöglichen, gestatten Transaktionen mehrere Inputs und Outputs. [26]

[25] *Die Bankenkrise von 2007 hat dafür den Beweis unter realen Bedingungen geliefert*

[26] *(Nakamoto, 2008, S. 5)*

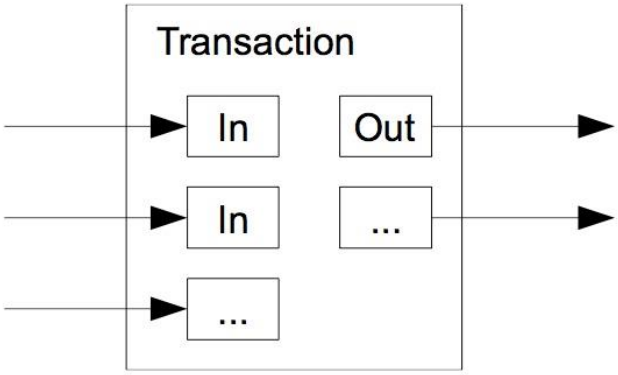


Abb. 6: Inputs und Outputs einer Transaktion[27]

Im Normalfall wird entweder ein einzelner Eingang aus einer größeren vorherigen Transaktion oder mehrere Eingänge, die kleinere Mengen kombinieren, verwendet. Dazu sind entweder ein oder zwei Ausgänge notwendig: ein Ausgang wird für die Zahlung verwendet und ein zweiter Ausgang bei Bedarf, der das „Wechselgeld“ zurück an den Absender schickt. Dies kann notwendig werden, da ja die Eingänge einen festen Wert aus den vorigen Transaktionen abholen, der nicht unbedingt mit dem Zahlungsziel übereinstimmen muss.

2.4.2 Unspent transaction outputs

Beim Studium der einschlägigen Literatur wird oft auf den Begriff „UTXO“ verwiesen. Unspent transaction outputs, kurz UTXO, sind outputs einer Transaktion, die noch nicht input einer anderen Transaktion geworden sind. Diese nicht ausgegebenen Coins kann man sich auch als Guthaben vorstellen, die Summe aller UTXOs würde der Geldmenge in realen Währungen entsprechen. Folgende Grafik kann die Funktionsweise verdeutlichen[28]:

[27] *Abb. aus (Nakamoto, 2008)*

[28] *(bitcoin.stackexchange.com)*

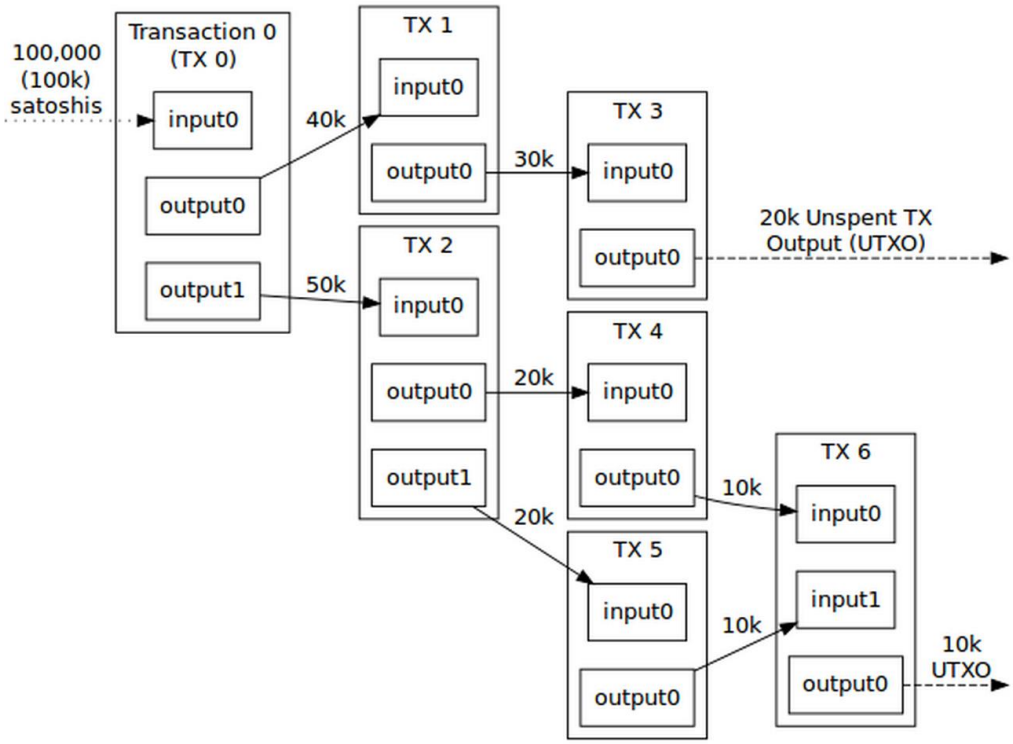


Abb. 7: Beispiel für UTXO[29]

[29] *(bitcoin.stackexchange.com)*

2.5 Bildung und Verkettung der Blöcke

Etwa alle zehn Minuten werden die kürzlich erzeugten Transaktionen zu Blöcken zusammengefasst und verschlüsselt. Jeder Block besteht aus einem „*Header*“ und einem „*Body*“. Der Header enthält vier Felder:

- Ein Zeitstempel
- Eine fortlaufende Nummer (Nonce)
- Den Hash des vorigen Blocks
- Eine mittels Hashfunktion codierte Liste der Transaktionen

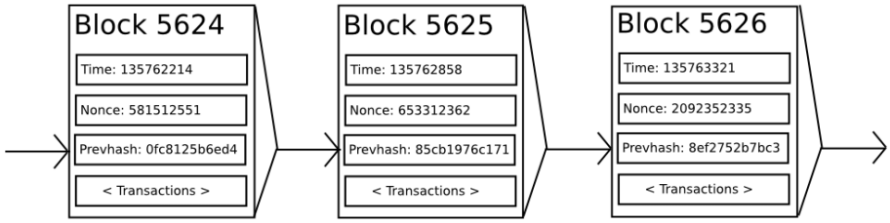


Abb. 8: Verkettung der Blöcke[30]

Die Verkettung der Blöcke entsteht dadurch, dass im Header eines Blockes auf den vorigen Block mittels dessen Hashfunktion verwiesen wird. Damit ist festgelegt, dass genau dieser und kein anderer Block der Vorgänger sein muss. Ziel der Verkettung ist der Schutz der Blöcke vor nachträglicher Manipulation.

Erfolgt eine nachträgliche Manipulation, beispielsweise durch Veränderung oder Löschung einer Transaktion in einem Block, dann würde diese Operation den Hashwert des Blockes verändern. Da dieser auch ein Element des Folgeblockes (und damit indirekt aller weiteren Folgeblöcke der Kette) ist, müssten bei Manipulation auch alle Folgeblöcke nachträglich verändert werden. Da aber Kopien der Blockchain auf vielen Rechnerknoten im Netzwerk gespeichert sind, müsste ein Manipulator den Zugriff auf die Mehrheit dieser Rechner finden, um die Veränderungen gleichzeitig auch dort

[30] *Abbildung aus: (Buterin, 2013, S. 6)*

durchzuführen. Aus diesen Überlegungen betrachtet man die Blockchain als manipulationssicher.

2.6 Mining

Mining bezeichnet das Erzeugen neuer Geldeinheiten als Gegenleistung für verrichtete Arbeiten bei der Erzeugung neuer Blöcke.

Ein wesentliches Merkmal der Blockchain ist die verteilte Bildung eines Konsens darüber, dass durchgeführte Transaktionen gültig sind. Dabei kann jede Nutzerin und jeder Nutzer an der Konsensbildung mitwirken.[31]

2.6.1 Validierung

Der Begriff Validierung meint die Sicherstellung der Gültigkeit einer Transaktion. Es soll also im Wallet, für das die Transaktion durchgeführt wird, genügend Guthaben vorhanden sein, um diese Transaktion auch durchführen zu können.

Die installierte Blockchain-Software muss zumindest eine Reihe anderer Nutzer kennen, denen sie eine Nachricht über eine beabsichtigte Transaktion einer Teilnehmerin A zukommen lässt. Diese werden aufgefordert, die Transaktion zu validieren und die Nachricht an die den Adressaten bekannten Nutzer weiterzuleiten.[32]

Der Zustand einer Blockchain ist zu jedem beliebigen Zeitpunkt durch die Gesamtheit aller Transaktionen definiert, die bis dahin durchgeführt und bestätigt wurden.[33]

Zur Validierung einer neuen Transaktion ist es erforderlich, sich durch die Kette aller das fragliche Konto von A betreffenden Transaktionen durchzuarbeiten und zu überprüfen, ob der ermittelte Kontostand es erlaubt, die Transaktion durchzuführen.[34] Dazu werden alle in der Blockchain vorhanden Blöcke durchsucht und die zu A gehörenden Transaktionen extrahiert. Der validierende Miner benötigt also aus allen A betreffenden Blöcken die zugehörigen Transaktionen.

---

[31] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 10)*

[32] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 10)*

[33] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 10)*

[34] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 10)*

Die Größe der Blockchain wächst laufend und hat gegenwärtig (Oktober 2017) die Größe von 140 GB überschritten:

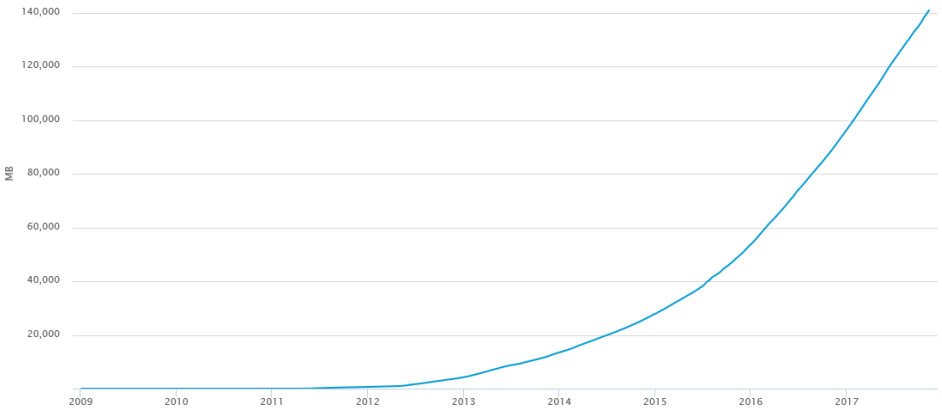


Abb. 9: Ressourcenbedarf der Bitcoin-Blockchain [35]

Aufgrund des Platzbedarfes ist verständlich, dass nicht alle Nutzerinnen eine vollständige Version der Kette auf ihrem Endgerät gespeichert haben können.

Um bei dem Schritt der Validierung das Replizieren ganzer Blöcke zu vermeiden, werden die Transaktionen eines Blockes nicht als Liste sondern als Blätter eines binären Hash-Baums gespeichert, dem sogenannten *Merkle-Tree*.[36]

2.6.1.1 Merkle-Tree

Der Merkle-Tree ist eine Datenstruktur in Form eines aus Hashwerten bestehenden binären Baumes.

Zur Bildung eines Merkle-Baumes aus einer gegebenen Anzahl von Transaktionen werden die Hashes von jeweils 2 Transaktionen zu einem neuen Hash (der 2. Generation) zusammengefasst, zwei Hashes dieser Generation wieder zu einem neuen Hash zusammengefasst, bis sich der Baum zu einem einzelnen Verzweigungsknoten verjüngt hat: der *Merkle Root*. [37]

---

[35] *Abbildung aus Blockchain.info. (Blockchain overall size)*

[36] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 10)*

[37] *(Merkle, 1982)*

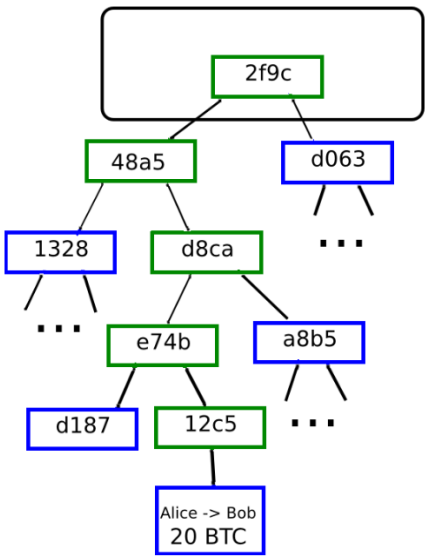


Abb. 10: Auszug eines Merkle Tree[38]

Um die Transaktion von 20 BTC von Alice zu Bob aus der Abbildung verifizieren, ist es nicht notwendig, alle Knoten des Baumes nachzurechnen. Vielmehr reicht es, dem grünen Pfad der Abbildung zu folgen und nur die Hashwerte dieser Verzweigungsknoten zu verifizieren.

2.6.2 Konsensfindung

Ist ein neuer Block mit validierten Transaktionen erfolgreich erzeugt und von seinem Miner in dessen lokale Kopie der Blockchain eingefügt worden, so muss im letzten Schritt dieser Block im Blockchain-Netzwerk verteilt und von anderen Minern validiert und in ihre lokalen Kopien der Blockchain eingefügt werden. Durch diese unabhängigen Überprüfungen neuer Blöcke durch Dritte wird der Konsens der Miner über die Validität der Blockchain hergestellt.[39]

Sobald der Block, welcher die neue Transaktion beinhaltet, an die ursprüngliche Blockchain angekettet wurde und die dadurch erzeugte neue Kette an hinreichend viele andere Teilnehmer des Netzwerks verteilt wurde, ist die Transaktion für beide Parteien bestätigt.

---

[38] *(Buterin, 2013, S. 9)*

[39] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 11)*

Folgende zwei Mechanismen werden am häufigsten zur Konsensfindung eingesetzt:

2.6.3 Proof of Work

Der Begriff *Proof-of-work* kann mit Arbeitsnachweis übersetzt werden. Proof-of-work ist gegenwärtig der wichtigste Algorithmus, um Konsens zu erzeugen. Dieser Algorithmus wurde ursprünglich dazu entwickelt, um E-Mail Spam und DoS[40]-Attacken zu unterbinden.

Beim Spam werden in kurzer Zeit großen Mengen an Mails gleichen Inhaltes automatisiert an verschiedene Absender versendet. DoS-Attacken erzeugen durch eine große Anzahl von Client-Anfragen an einen Server eine Überlastung des Servers oder eine Netzwerküberlastung. Dadurch wird erreicht, dass die am Server laufenden Dienste nicht mehr erreicht werden oder nicht mehr in akzeptabler Zeit auf Anfragen antworten können. Gemeinsam sind beiden Netzmissbräuchen, dass eine große Anzahl an Daten von einem Quellknoten in Richtung einem oder mehrerer Zielknoten geschickt wird.

Der Proof-of-work-Algorithmus setzt am Ausgangsknoten an: Er fordert vom Sender der E-Mail oder Steller der Anfrage einen Nachweis, das vor dem Senden einen Teil der CPU-Rechenleistung zum Lösen einer Aufgabe verwendet wird. Würde also ein Sender von Massenmails vor dem Versenden jeder E-Mail Rechenzeit und Energie aufwenden, werden Spam und DoS-Attacken unrentabel.

2.6.3.1 Hashcash

Der im Bitcoin-Protokoll verwendete Algorithmus trägt den Namen Hashcash. Hashcash ist ein proof-of-work-Algorithmus, der im Jahr 1997 von Adam Back vorgeschlagen wurde.[41] Vor seiner Implementierung im Bitcoin-Protokoll wurde Hashcash vor allem von Anbietern von Mailservices zur Prävention von Spam eingesetzt. Die Aufgabe zur Erbringung des Arbeitsnachweises besteht im Finden eines Hashwertes mit einer Anzahl von führenden Ziffern 0 zu einem teilweise bekannten Quelltext. Je nach Bedarf kann dabei die Anzahl der Ziffern 0 variiert werden, um die Schwierigkeit (*Difficulty*) zu erhöhen und damit die Bildung neuer Blöcke auf ein bestimmtes Intervall festzulegen. Bei Bitcoin ist das Intervall mit ungefähr 10 Minuten festgelegt.

---

[40] *DoS: Denial of Service*

[41] *(Back, 2002)*

2.6.4 Proof of Stake

Da der Mining-Prozess basierend auf dem Proof-of-Work sehr rechenintensiv, und damit sehr energieaufwendig ist, wird derzeit eine Reihe von Alternativen zu diesem Mechanismus untersucht. Einer der am intensivsten diskutierten Ansätze ist der des sogenannten Proof-of-Stake. Hierbei steht nicht die Rechenleistung eines Miners im Vordergrund, sondern die Menge der Währungseinheiten (Coins), die ein Miner besitzt. Proof-of-Stake lässt sich mit Anteilsnachweis übersetzen. Gemeint ist der Anteil an Token (also Währungseinheiten wie beispielsweise Bitcoin), die eine Nutzerin hält. [42] Entsprechend diesem Anteil wird auch die Aufgabe des Minings unter den Nutzern aufgeteilt.

Die Vorteile gegenüber dem Proof-of-Work bestehen in deutlich geringerem Energieverbrauch, weniger Tendenz zur Zentralisierung und erhöhter Sicherheit.[43]

[42] *(von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016, S. 7)*

[43] *(Proof of Stake FAQ)*

2.7 Anreizsystem

Zu klären ist, was eine Minerin dazu motivieren kann, die Gültigkeit einer Transaktion zu bestätigen und einen neuen Block an die Blockchain anzuhängen. Diese Tätigkeiten sind rechenintensiv und damit mit großem Energieaufwand verbunden und damit sie wirkungsvoll betrieben werden können, ist ein beträchtlicher Aufwand an Hardwarekosten zu entrichten.

Miner erhalten für das erfolgreiche Einfügen eines Blocks in die Bitcoin-Blockchain eine Belohnung von 12,5 BTC. Die Höhe dieser Belohnung für neue Blöcke wird alle vier Jahre halbiert. Auf lange Sicht werden daher die Transaktionsgebühren als Haupteinnahmequelle für Miner überwiegen. [44]

Die folgenden Erklärungen sind aus der Studie[45] des Kompetenzzentrums Öffentliche IT des Fraunhofer-Instituts für Offene Kommunikationssysteme FOKUS übernommen:

Sobald der Wert der Kryptowährung die Kosten für das Mining neuer Blöcke übersteigt, wird die Beteiligung an einer Blockchain für Miner wirtschaftlich interessant. War es am Anfang noch möglich, mit dem privaten PC am Mining teilzunehmen, so ist mittlerweile zu beobachten, dass Rechnerfarmen, bestehend aus speziell für das Mining entwickelter Hardware, aufgebaut werden, die sich ausschließlich mit der Erzeugung neuer Blöcke beschäftigen und sich dadurch finanzieren. [46]

Übersteigen die Aufwände für das Mining den Wert der damit erzeugten neuen Bitcoins, muss der Rechenaufwand über Transaktionsgebühren finanziert werden. Je aufwendiger es ist, am Mining-Prozess teilzunehmen, desto weniger Nutzer beteiligen sich daran, was langfristig zu Zentralisierungstendenzen führen kann. [47]

In der Bitcoin-Blockchain ist die Anzahl der jemals erzeugbaren BTC auf 21 Millionen beschränkt. Aus dieser Beschränkung resultiert die Tatsache, dass im Laufe der Zeit die Belohnung für das erfolgreiche Ermitteln eines neuen Blocks abnimmt und die Haupteinnahme eines Miners auf langfristige Sicht vorrangig aus Transaktionsgebühren besteht. Geht man davon aus, dass die Zahl der Nutzer der Bitcoin-Blockchain kontinuierlich steigt und somit die Zahl

---

[44] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 13)*

[45] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017)*

[46] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 13)*

[47] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 13)*

der Transaktionen zunimmt, wird dies als ein nachhaltiges Geschäftsmodell angesehen. [48]

[48] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 13)*

2.8 Arten der Blockchain[49]

Die Anwendung der Blockchain ist in verschiedenen Ausprägungen denkbar. Eine einfache Unterteilung erfolgt in öffentliche (*public*) und private Blockchains. An öffentlichen Blockchains kann jede Person teilnehmen, die die nötigen Beitrittsschritte durchführt, die je nach konkretem Projekt unterschiedlich sein können aber typischerweise die Installation der Software auf dem dafür vorgesehenen Endgerät und die Registrierung unter Verwendung des Schlüsselpaares (öffentlicher und privater Schlüssel) beinhalten.

Aber auch in privaten Netzen, in denen per se schon eine gewisse Menge von Vertrautheit zur Ausstattung gehört, kann durch Einsatz der Blockchain diese Vertrautheit und Sicherheit nochmal erhöht werden.

Eine andere mögliche Unterscheidung von Blockchains wird durch das Wortepaar *permissioned* und *permissionless* dargestellt. Diese Bezeichnung bezieht sich auf Schreibrechte in die Kette, also die Berechtigung, Transaktionen initiieren zu dürfen. Entsprechend gestattet eine *permissonless Blockchain* Zugriffsrechte ohne dass dafür eine spezielle Zulassung notwendig wird, während die *permissoned blockchain* diese Zulassung erfordert.

Die bislang bekanntesten Anwendungen „Bitcoin“ und „Ethereum“ fallen beide in die Rubrik der *public permissionless Blockchain*. Da Ethereum sich als Plattform versteht, die Anbietern von Diensten ein Gerüst zur Entwicklung eigener Applikationen anbietet, ist es in diesem Bereich notwendig, zu Testzwecken auch private Blockchains anzubieten.

[49] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 15)*

2.9 Kritik

So umfassend die Vorteile und Möglichkeiten angepriesen werden – die Blockchain wird in ihrer Bedeutung mehrfach als wichtigste Neuerung seit der Erfindung des Internets bezeichnet - so umfassend erfolgt auch die Kritik. Bemängelt werden von der Unkenntnis der Identität des Erfinders und Autors der ersten Publikation S. Nakamoto über die Einschränkung der Dezentralität durch die Tatsache, dass die größten „mining organisations", die die für die Validierung der einzelnen Transaktionen notwendige Rechenleistung aufbringen können, allesamt in chinesischen Rechenzentren betrieben werden, bis zum Fehlen eines Ansprechpartners im Falle des Auftretens einer Ungereimtheit in einem Block und der damit fehlenden Vertrauensbildung zumindest in weniger technologieaffinen Bevölkerungsgruppen.

Trotzdem liegt es nahe, dass die Blockchain in viele Bereiche des wirtschaftlichen Lebens Einzug halten wird, da sie durch Automatisierung und Dezentralisierung zur Auslagerung von Personal und Rechenleistung an den Endkunden und damit zur Kostenreduktion der Unternehmen beiträgt.

3 Smart Contracts

3.1 Einführung

Neben Bitcoin werden Smart Contracts als Hauptanwendung der Blockchain-Technologie genannt. Die potentiellen Anwendungsgebiete sind mannigfach. Sie reichen über die Möglichkeit, ein elektronisches Grundbuch zu führen, den Handel mit Strom oder Rechenleistung zwischen Verbrauchern, Zugangskontrolle zu Räumen oder Mietfahrzeugen über elektronische Schlösser, Sicherung der Authentizität von Geschäftspartnern bis zu Bereichen des E-Governments und elektronisch unterstützten Wahlen und Wahlauswertungen.

3.2 Beschränkungen der Bitcoin-Skriptsprache

Das Bitcoin-Protokoll selbst enthält schon eine einfache Form einer Skriptsprache, mit der abgesehen von Bitcoin als Zahlungsmethode auch einfache Kontrakte verwirklicht werden können[50]. Allerdings taugt diese Sprache aus nachfolgenden Gründen nicht zur Erstellung komplexerer Programme.[51]

- Keine Möglichkeit, Schleifen zu programmieren (Fehlende Turing-Vollständigkeit)
- Keine Möglichkeit, externe Eingaben zu verarbeiten.
- UTXOs können nicht in verschiedenen Zuständen dargestellt werden.
- Es gibt keinen Zugriff auf Blockchain-Daten wie Nonce oder den Zugriff auf ältere Blöcke.

[50] *(Buterin, 2013, S. 11)*

[51] *(Buterin, 2013, S. 12)*

3.3 Ethereum

3.3.1 Einführung

Als der Hauptanbieter von Diensten im Bereich Smart Contracts hat sich gegenwärtig eine schweizerische Foundation namens Ethereum hervorgetan, die auf der gleichnamigen Plattform umfassende Toolsets zum Design und dem Betrieb eigener Anwendungen anbietet. Ethereum existiert seit 2015 und wurde durch Crowdfunding finanziert. Es existieren wenige Anwendungen, die allesamt stark beworben werden aber der Erfahrungsschatz ist noch dünn gesät.

Ethereum wurde Ende 2013 von dem Kryptologen Vitalik Buterin, vorgeschlagen. Die Entwicklung wurde im Juli-August 2014 durch Crowdfunding finanziert. Das System wurde am 30. Juli 2015 in Betrieb genommen.

Ethereum ist eine öffentliche, auf der Blockchain-Technologie basierende Distributed-Computing-Plattform mit eingebauter Vertragsfunktionalität. Es stellt eine dezentralisierte Turing-vollständige virtuelle Maschine, die Ethereum Virtual Machine (EVM), zur Verfügung, die Skripte über ein verteiltes Netzwerk öffentlicher Knoten ausführen kann. Ethereum stellt auch ein Token einer Kryptowährung namens *Ether* zur Verfügung, das zwischen Konten transferiert und für Berechnungen verwendet werden kann.

Neben dieser Währung existiert mit „Gas“ ein interner Mechanismus zur Preisfestsetzung bei Transaktionen, welcher der Zuweisung von Ressourcen im Netz dient.

3.3.2 Zustandsparameter

Der Zustand der Ethereum-Blockchain wird durch einzelne Objekte definiert. Diese Objekte werden als *Accounts* bezeichnet. Ein Account wird durch eine 20-byte Adresse dargestellt. Der Account beinhaltet 4 Felder.

3.3.2.1 Felder des Ethereum-Accounts

- Nonce: In der Kryptographie eine einmalig verwendete Zeichenkombination („Number used once“).[52] Im vorliegenden Fall

[52] *(Anderson, 2008)*

wird damit sichergestellt, dass jede Transaktion, die über den Account geführt wird, nur einmal durchgeführt wird.
- Ether Balance: Das Guthaben der Ethereum zugeordneten Kryptowährung Ether.
- Contract Code: Der Programmcode, der die Schritte definiert, die zur Umsetzung des smarten Vertrages notwendig sind.
- Storage: für etwaige Zwischen- oder Endergebnisse reservierter Speicherplatz, der zu Beginn unbelegt ist.

3.3.3 Nachrichten und Transaktionen

Die Begriffe *Messages* und *Transactions* im Ethereum-Protokoll unterscheiden sich vom Gebrauch im Bitcoin-Protokoll.

Die Message eines Ethereum-Kontos entspricht einer Transaktion im Bitcoin-Protokoll, wobei drei Unterschiede festzumachen sind:

- Die Ethereum-Message kann sowohl extern durch eine Teilnehmerin als auch intern durch einen Code (einen Contract) ausgelöst werden.
- Die Ethereum-Message kann zusätzliche Daten enthalten.
- Der Empfänger-Account hat auch die Möglichkeit, eine Antwort zu senden. [53]

Die Transaction wiederum bezeichnet das signierte Datenpaket, das die Message enthält und extern von einem Account gesendet wird.

Die Transaction enthält folgende Felder:

- Die interne Quelle der Message
- Den Empfänger der Message
- Den Betrag an Ether, der zum Transfer vorgesehen ist
- Ein Feld, das zusätzliche Daten für spezifische Anwendungen enthalten kann
- Einen Wert STARTGAS zur Berechnung der Transaktionskosten
- Eine Wert STARTVALUE zur Berechnung der Transaktionskosten [54]

[53] *(Buterin, 2013, S. 14)*

[54] *(Buterin, 2013, S. 14)*

Die Werte STARTGAS und STARTVALUE limitieren die Anweisungen des Codes anhand der Kosten pro ausgeführtem Schritt, um beispielsweise unendliche Schleifen oder andere Fehler im Code zu begrenzen. [55]

Durch die Einführung einer maximalen Anzahl von Ausführungsschritten einer Transaktion durch das Gas-Limit sollen der missbräuchliche Aufruf von Transaktionen verhindert und die Kosten eines Transaktionsaufrufs überschaubar gehalten werden. [56]

Der Programmcode, der die Übermittelung der Messages steuert, läuft in der sogenannten Ethereum Virtual Machine (EVM) und besteht aus einer Folge von Bytes, von denen jedes Byte jeweils einen Befehl enthält. [57]

3.3.4 Ethereum Blockchain

Die Ethereum Blockchain unterscheidet sich in wenigen Punkten von der in der Bitcoin-Umsetzung verwendeten Blockchain. So enthält ein Ethereum-Block neben den aus Bitcoin bekannten Feldern[58] auch den Ist-Stand und eine Liste der Transaktionen. [59]

Die Transaktionen werden in einer modifizierten Form des Merkle Tree, dem sogenannten Patricia Tree gespeichert, wodurch die Möglichkeit gegeben ist, einzelne Knoten im Baum einzufügen oder zu löschen. [60]

3.3.5 Decentralized Application

DApp ist die Kurzform für *Decentralized Application*, oder Verteilte Anwendung. Decentralized Applications verwenden ein peer-to-peer-Protokoll, das es einzelnen Knoten in einem Netzwerk erlaubt, direkt und ohne eine zentrale Vermittlungsstelle (z.B. einen Server, Switch oder Router) miteinander zu kommunizieren. Eine Besonderheit einer DApp ist (mangels Zentrale) die dezentale Speicherung aller Transaktionsdaten.

---

[55] *(Buterin, 2013, S. 14)*

[56] *(Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 14)*

[57] *(Buterin, 2013, S. 17)*

[58] *Siehe Kap. 2.5*

[59] *(Buterin, 2013, S. 18)*

[60] *(Buterin, 2013, S. 18)*

Die DApp kann als Vereinbarung zwischen dem Netzwerk und seinen Benutzerinnen aufgefasst werden, die auf einem dezentral verteilten Register (dem Ledger[61]) läuft.[62] Beispiele für diese dezentralen Register sind die Bitcoin-Blockchain oder die Ethereum-Blockchain.

Eine weitere wichtige Eigenschaft einer dezentralen Anwendung ist die Vermeidung eines *Central Point of Failure*[63] durch die Tatsache, dass Protokoll und Daten in einer dezentralisierten Blockchain gespeichert werden. Diese Eigenschaft erlaubt es auch einzelnen Teilnehmerinnen, das Netzwerk nach beliebiger Zeit zu verlassen und dem Netzwerk wieder beizutreten. Außerdem wird ein dezentraler Validierungsmechanismus verwendet (z.B. Proof-of-Work).

Die Klassifizierung von DApps kann in drei Typen erfolgen:[64]

- Type 1: Dezentrale Applikationen mit eigener Blockchain, beispielsweise Bitcoin, Altcoin und diverse andere Kryptowährungen
- Type 2: Dezentrale Applikationen, die auf der Blockchain einer Type 1 DApp aufsetzen, beispielsweise *Omni Protocol*[65]
- Type 3: Dezentrale Applikation, die auf der blockchain einer Type 2 DApp aufsetzen. Beispiel: Das SAFE Network setzt auf Omni Protocol auf und erzeugt Tokens

3.3.6 Decentralized Autonomous Organisation

Das Akromym DAO steht für *Decentralized Autonomous Organisation*.[66] Die DAO ist als eine komplexere Form der DApp aufzufassen. Die Möglichkeiten, die diese höhere Komplexität bietet, legen nahe, die DAO als eine Form von sich selbstregelnder Organisation aufzufassen.

Die Regeln dieser Organisation sind in der Blockchain gespeichert. Die Idee ist eine Umsetzung des Konzept eines Smart Contracts. Die Grundeigenschaften dieser Gebilde können wie folgt angeführt werden:

---

[61] *Ledger: engl. für Kontenbuch, im Sinn einer chronologischen Liste von Eintragungen*

[62] *(von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016, S. 6)*

[63] *Als* Central Point of Failure *werden Netzknoten bezeichnet, deren alleiniger Ausfall Funktionstörungen in größeren Teilen oder gleich im ganzen Netzwerk erzeugt.*

[64] *(von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016)*

[65] *(Omni Layer - Open-source,fully decentralized asset platform on the Bitcoin Blockchain)*

[66] *(von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016)*

Unveränderlichkeit: der Code ist durch Einzelne nicht abänderbar. Nur per Absprache kann eine Mehrheit der Teilnehmer eine Änderung des Codes genehmigen.

Unstoppbarkeit: Der Ablauf des Programmes kann, sobald es einmal gestartet ist, praktisch nicht mehr unterbrochen werden, da es dezentral auf allen Netzknoten läuft. Diese Tatsache erhebt besondere Ansprüche an die Qualität des Codes.

Unwiderlegbarkeit: Jede Transaktion findet Einzug in die Blockchain und ist dort einsehbar und unveränderbar auf lange Frist gespeichert.[67]

[67] *Aufzählung aus (von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016)*

4 Anwendungsbeispiele

4.1 Die Rolle des Intermediär

In vielen Bereichen des öffentlichen und privaten (besonders privatwirtschaftlichen) Lebens fungieren Intermediäre als Steuerzentralen für Kapital-, Güter- oder Dienstleistungsflüsse. So wie der Staat durch seine Behörden Regularien für Dienstleistungen bietet, so bieten private Betreiber für ihre Bereiche Vermittlungsdienste für den reibungslosen Ablauf diverser Geschäftsbeziehungen an. Banken steuern Geldflüsse, diverse Energieversorger übernehmen die Bereitstellung und Abrechnung von Strom, Gas oder Heißwasser, und Kommunikationsunternehmen bieten Content aller Arten über zentral gesteuerte Netzinfrastruktur an.

Ideen zur Automatisierung und Dezentralisierung gibt für in viele Bereiche und Branchen. Die Energieerzeugung wird vielfach durch Eigentümer von Solarpanels auf Dächern von Eigenheimen vorgenommen und die überschüssige Energie wird ins Stromnetz eingespeist. Content wird nicht mehr von Unternehmen sondern von Einzelpersonen generiert (Filme auf Youtube, Blogs), sodass sich auch hier neue Möglichkeiten ergeben können.

Einige Ideen sollen nachfolgend vorgestellt werden.

4.2 Behörden

4.2.1 Elektronisches Grundbuch

Schweden gilt in Europa als Vorreiter für die Integration der Blockchain ins öffentliche Grundbuch.[68] Mit März 2017 startete ein Testlauf des Grundbuches mit Testdaten zum Zwecke der Abklärung technischer, rechtlicher und wirtschaftlicher Auswirkungen. [69] Die Testphase wurde im Juli 2017 abgeschlossen und das modernisierte Grundbuch befindet sich seither im Livebetrieb. Verwendet wird eine Blockchain privater Ausprägung, um dem

[68] *(Grau, 2016)*

[69] *(Brandau, 2017)*

Staat weiterhin die Kontrolle und den Einfluss bei fallweisen Gesetzesänderungen zu gewähren.[70]

Ähnliche Projekte werden von den südamerikanischen Ländern Honduras und Brasilien verfolgt.

4.2.2 Elektronische Wahlen

Eine vielfach erwähnte Anwendung der Blockchain sind elektronisch unterstützte Wahlen. Nach allgemeiner Vorstellung soll dabei jede wahlberechtigte Person ein Wallet erhalten, und ihre Stimme abgeben, indem sie einen Token (also eine elektronische Münze) an die Person oder Liste ihrer Wahl überträgt. Dieses System bringt einige Vorteile mit sich:

- Da jede Person nur ein Token erhält, ist leicht nachvollziehbar, dass auch jede Person nur eine Stimme abgegeben hat. Eine komplizierte Herstellung und Aufbereitung von Wahlzetteln entfällt.[71]
- Eine Auszählung der Stimmzettel erfolgt automatisch, Nachwahlbefragungen, Hochrechnungen und Verzögerungen bei der manuellen Auszählung entfallen, ebenso wie das Stellen und der der Schulungsbedarf von Wahlbeisitzern.

Jedoch sind mehrere Vorgaben zu beachten, um eine Wahl gesetzeskonform durchzuführen. Die Grundlagen für die Wahlen zum österreichischen Nationalrat regelt der Artikel 26 des österreichischen Bundes-Verfassungsgesetzes (B-VG)[72]. Entsprechendes regelt Artikel 60 des B-VG für die Wahlen zum Bundespräsidenten.

Artikel 26 Absatz 1 B-VG lautet:

Der Bundespräsident wird vom Bundesvolk auf Grund des gleichen, unmittelbaren, persönlichen, freien und geheimen Wahlrechtes der zum Nationalrat wahlberechtigten Männer und Frauen gewählt; […]

---

[70] *(Wagenknecht, 2017)*

[71] *Man erinnere sich an die Wahl zum österreichischen Bundespräsidenten 2016, vor der Wahlzettel neu produziert werden mussten, weil sie den Vorgaben nicht entsprochen haben, was eine Terminverschiebung der Wiederholung der Stichwahl zur Folge hatte.*

[72] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Bundes-Verfassungsgesetz)*

Die elektronisch unterstützte Wahl auf Blockchain-Basis kann gegenwärtig mindestens zwei dieser von der Verfassung vorgeschriebenen Anforderungen nicht erfüllen.

Zum ersten ist die Blockchain kein anonymes, sondern ein pseudonymes Medium. Eine Rückverfolgung der pseudonymen Stimmabgabe auf die hinter dem Wallet stehenden Person kann daher nicht grundsätzlich ausgeschlossen werden.[73] Hier könnten andere kryptographische Verfahren Lösungen bringen.[74]

Darüber hinaus ist der momentane Auszählungsstand zu jeder Zeit während der Wahl abrufbar, sodass man seine Stimmabgabe danach richten kann.[75]

Letztlich öffnet diese Art von Transparenz die Türe zum Stimmenverkauf.[76] Jede wahlberechtigte Person ist nämlich in der Lage, gegenüber Dritten nachzuweisen, dass sie genauso gewählt hat, wie es vom Dritten bestellt und bezahlt worden ist. Damit sind auch die Forderungen nach persönlicher und gleicher[77] Stimmabgabe umgangen.

4.3 Energieversorger

Das gängige Bild einer zentralen Energieversorgung sieht eine Masse an Konsumenten einer geringen Anzahl von Energieversorgern gegenüber. Diese Energieversorger sind z.B. Betreiber von Strom-, Gas- oder Fernwärmenetzen, Kraftwerksbetreiber, außerdem Anbieter, die die jeweilige Form des Energieträgers (Strom, Gas,..) vermitteln, also an die Endkunden weiterverkaufen.

Im neuen Bild der dezentralen Energieversorgung werden die Endkunden auch zu Energieerzeugern. Konsumenten werden zu Produzenten, die mit dem Begriff „Prosumer“ treffend beschrieben werden. Als gegenwärtig praktikable Technologie zur Wandlung des Konsumenten zum Prosumer zeigt

---

[73] (Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 22)

[74] (Zhao & Chan, 2016)

[75] Einer der Gründe für die Aufhebung der Stichwahl zum österreichischen Bundespräsidenten 2016 war die Tatsache, dass Zwischenergebnisse von schon ausgezählten Wahlbezirken veröffentlicht wurden, während die Wahl noch im Gange war.

[76] (Welzel, Eckert, Kirstein, & Jacumeit, 2017, S. 22)

[77] Gleiches Wahlrecht: jede wahlberechtigte Person hat die gleiche Anzahl von Stimmen (in Österreich eine Stimme, in Deutschland Erst- und Zweitstimme)

sich die Nutzung von Solarpanels zur Produktion von elektrischer Energie für den Eigenbedarf mit der Möglichkeit, Überproduktion in das überregionale Netz einzuspeisen und an andere Abnehmer zu verkaufen. Diese können (wie bisher) Elektrizitätsgesellschaften sein, denkbar ist aber auch ein direkter Verkauf an einen anderen Endkunden oder Prosumer.[78]

Neben Solartechnologie sind aber die verteilte Nutzung von Erdwärme oder – mit geeigneter regionaler Infrastruktur - die verteilte Produktion und Nutzung von Heißwasser denkbar. Eine sich schon im Betrieb befindende Anwendung zum Handel von Solarenergie ist das Brooklyn Microgrid.

4.3.1 Brooklyn Microgrid

Das Brooklyn Microgrid wurde 2016 mit dem Ziel gegründet, die Funktionalität und Praktikabilität eines dezentralen Stromnetzes mit Energieerzeugung aus Solarzellen zu testen. Ursprünglich wurden die Dächer von fünf Häusern mit Solarzellenpanelen ausgestattet.

Das zwischen den Panelen aufgespannte Microgrid ist ein Miniatur-Stromnetz, das seinen Bewohnern auch dann noch Strom liefern kann, wenn das regionale Netz aufgrund von Stromausfällen oder anderen Notfällen keine Energie mehr anbietet.[79] In einem Haushalt erzeugte Überkapazitäten werden in das Netz eingespeist und anderen Haushalten zum Verkauf angeboten.

Physikalisch verwendet dieses Gitter die herkömmlichen Stromleitungen[80], die Haushalte sind mit intelligenten Stromzählern (Smart Metern) ausgestattet und messen den eingehenden oder ausgehenden Stromfluss.

Die Abrechnung der Stromkonsumation und Stromlieferung an Nachbarhaushalte bedient sich der Blockchain als Medium zur Speicherung und Nachverfolgbarkeit. Die Abrechnung selbst wird durch Smart Contracts gesteuert, die Signale von den Stromzählern als die die Transaktion auslösenden Eingaben verwenden.

Gegenwärtig werden die Preise für Stromlieferungen noch „manuell“ verhandelt. Das System soll in Zukunft dahingehend weiterentwickelt werden,

---

[78] *(von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016)*

[79] *(Brooklyn Microgrid 101)*

[80] *(von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016, S. 20)*

dass Kunden nur mehr den Preis auswählen, zu dem sie den Strom beziehen wollen und die Transaktionen danach automatisch ablaufen lassen.[81]

4.4 Smarte Versicherungsverträge

Versicherungen haben die Funktion, sich gegen das Eintreten eines Ereignisses, das mit einer bestimmten Wahrscheinlichkeit behaftet ist, und einen Schaden verursachen würde, abzusichern. Die Funktion eines Versicherungsvertrages ist damit offensichtlich: Tritt das Ereignis ein, dann soll (zumindest aus der Sicht des Versicherungsnehmers) möglichst schnell die Versicherungssumme zur Kompensation des Schadens ausgezahlt werden. Eine zeitnahe automatische Auszahlung wäre daher aus der Sicht des Versicherungsnehmers der Optimalfall.

Das Konzept eines smarten Versicherungsvertrages sieht folgendermaßen aus: Alle möglicherweise eintretenden Schäden und die dafür vereinbarten Kompensationszahlungen werden im Vertragscode festgelegt. Auch werden die „*oracles*“, die Parameter und die Grenzwerte, bei deren Erreichen der Vertragsablauf (also die Auszahlung) ausgelöst werden soll, festgelegt. Externe Messgeräte geben im Fall eines möglichen vertragsauslösenden Ereignisses die nötigen Messwerte (z.B. Hochwasserstand, Windgeschwindigkeit, Regen- oder Hagelmenge) an den Vertragscode weiter. Im Fall eines positiven Triggerevents erfolgt die Auszahlung automatisch.

4.5 Sicherung der Werknutzungsrechte

Das österreichische Urheberrechtsgesetz (UrhG)[82] regelt die Nutzungsrechte an Werken. Mit Werken meint das UrhG persönlich geistige Schöpfungen aus den Bereichen der Literatur (z.B. Sprachkunst, aber auch Computerprogramme), der Tonkunst, der bildenden Künste oder der Filmkunst.

Das alleinige Nutzungsrecht des Urhebers legt §14 Abs 1 UrhG fest:

[81] *(von Perfall, Hillebrand, Smole, Lay, & Charlet, 2016, S. 20)*

[82] *(Urheberrechtsgesetz)*

Der Urheber hat mit den vom Gesetz bestimmten Beschränkungen das ausschließliche Recht, das Werk auf die ihm durch die folgenden Vorschriften vorbehaltenen Arten zu verwerten (Verwertungsrechte).

Zu den Verwertungsrechten zählen das Vervielfältigungsrecht, das Verbreitungsrecht, das Recht, seine Werke zu vermieten oder zu verleihen, und diverse auf die spezifische Art des Werkes eingehende Rechte. Zusätzlich sind Werke vor groben Veränderungen (z.B. bei Aufführungen) geschützt.

Der Urheber steht allerdings vor dem Problem, diese ihm zugesprochenen Rechte im Zeitalter der Digitalisierung und den damit einher gehenden Möglichkeiten der fehlerfreien originalgleichen Kopien durchzusetzen.

Smart Contracts können an dieser Stelle eine Urheberin bei der Wahrung ihrer Rechte unterstützen. Sind digitale Werke durch einen in der Blockchain hinterlegten Schlüssel geschützt, dann kann bei jeder Nutzungsanforderung durch einen Konsumenten eine automatische Zahlung über einen Smart Contract auf das Konto der Urheberin erfolgen und gleichzeitig des Werk temporär zur Nutzung freigegeben werden. Dies kann bei entsprechender Ausgestaltung des Vertrages sicherstellen, dass der Schöpfer bei jeder Nutzung seines Werkes automatische eine (zumindest kleine) Gebühr als Gegenleistung erhält, ohne eine Verwertungsgesellschaft für das Einheben dieser Gebühr beauftragen zu müssen oder im schlimmeren Fall die Nutzungsgebühr von säumigen Zahlern gerichtlich einzutreiben.

5 Das österreichische Vertragsrecht

5.1 Grundlagen

5.1.1 Was ist ein Vertrag?

Bydlinski definiert den Begriff des Vertrages folgendermaßen: *Verträge sind zwei- oder mehrseitige Vereinbarungen, die für die Beteiligten rechtlich verbindliche Regeln aufstellen*.[83]

Riedler verwendet den Begriff des Rechtsgeschäftes: *Rechtsgeschäfte sind (private) Willenserklärungen von Rechtssubjekten, die rechtlich durchsetzbar und von einem Rechtsfolgewillen getragen sind.*[84]

Die Begriffe Vertrag und Rechtsgeschäft werden schon im ABGB von 1811 verknüpft, in dem die Überschrift des 17. Hauptstückes im 2. Teil lautet: *Von Verträgen und Rechtsgeschäften überhaupt.*[85]

Daraus ist schon ablesbar, dass der Verträge eine Untermenge in der Menge aller Rechtsgeschäfte bilden, nämlich die der zwei- oder mehrseitigen. Folgende Begriffserklärungen sind in diesem Zusammenhang vorzunehmen:

- Rechtsgeschäft
- Rechtssubjekt
- Willenserklärung
- Rechtsfolgewillen

Nachfolgend soll ein kleines Fachvokabular rechtswissenschaftlicher Begriffe aufgebaut werden.

---

[83] *(Bydlinski, Grundzüge des Privatrechts für Ausbildung und Praxis, 2010, S. 127)*

[84] *(Riedler, 2010, S. 113)*

[85] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Allgemeines bürgerliches Gesetzbuch, Fassung vom 13.09.2017, 1811/2017)*

5.1.2 Rechtssubjekt

Rechtssubjekte haben Rechtsfähigkeit, d.h. sie sind Träger von Rechten und Pflichten. Rechtssubjekte können natürliche oder juristische Personen[86] sein.

Rechtsobjekte sind nicht Träger von Rechten und Pflichten sondern Gegenstand des Rechtsverkehrs. Zu den Rechtsobjekten zählt man Sache und Tiere.
Entsprechend ist die folgende Beziehung aufzustellen: Rechtssubjekte haben Rechte an Rechtsobjekten.

5.1.3 Willenserklärung

Der Terminus Willenserklärung ist gesetzlich nicht definiert. Nach heutiger Lehre[87] versteht man darunter

- eine Willensäußerung oder Willenshandlung, die auf die
- Herbeiführung von Rechtsfolgen[88] gerichtet ist und mit der
- ein Kundgabezweck verfolgt wird.

Mit Willensäußerung ist eine willentliche, also bewusst gesetzte Äußerung einer Person gemeint. Entsprechend gilt als Willenshandlung eine bewusst gesetzte körperliche Bewegung (und nimmt somit willenlose körperliche Reflexe aus).

Die erklärende Person ist an seine Willenserklärung nur dann gebunden, wenn damit ein Rechtsfolgewillen verbunden ist, sie also bereit ist, sich also den rechtlichen Folgen seines Willens zu unterwerfen. Damit ist sie auch bereit, die Folgen ihres Willens erforderlichenfalls durch staatlichen Zwang durchsetzen zu lassen.

Mit Kundgabezweck ist gemeint, dass die Äußerung oder Handlung dem Adressaten der Erklärung auch zur Kenntnis gebracht werden soll. Folglich erfüllt ein Vertragsentwurf, den man in seinem Schreibtisch aufbewahrt, noch keinen Kundgabezweck, auch dann nicht, wenn der Entwurf über Umwege an die Öffentlichkeit gelangt (z.B. weil es irrtümlich abgeschickt wurde).

---

[86] *z.B. GmbH, AG*

[87] *(Riedler, 2010, S. 125)*

[88] *Dies beschreibt den Begriff des* Rechtsfolgewillens

5.1.4 Rechtsgeschäft

Das Rechtsgeschäft ist *das* rechtliche Instrumentarium, das die Rechtsordnung dem Rechtssubjekt zur Gestaltung seiner Rechtssphäre zur Verfügung stellt.[89] Rechtsgeschäfte lassen sich in verschiedene Kategorien einteilen, von denen die wichtigsten nachfolgend beschrieben werden.

[89] *(Riedler, 2010, S. 114)*

5.2 Arten von Rechtsgeschäften

5.2.1 Einseitige und mehrseitige Rechtsgeschäfte

Ein Rechtsgeschäft kann aus einer oder mehreren Willenserklärungen bestehen. Je nachdem, wie viele Willenserklärungen für den Abschluss des Rechtsgeschäftes mindestens notwendig sind, erfolgt die Einteilung als einseitiges, zweiseitiges oder mehrseitiges Rechtsgeschäft.

Beispiele für einseitige Rechtsgeschäfte sind das Testament, das Vermächtnis oder die Kündigung. Als Beispiele für zweiseitige Rechtsgeschäfte können der Kaufvertrag, der Schenkungsvertrag oder der Werkvertrag angeführt werden. Der Gesellschaftsvertrag ist ein Beispiel für ein mehrseitiges Rechtsgeschäft, da es für den Abschluss der Zustimmung aller Gesellschafter bedarf.

5.2.2 Einseitig oder zweiseitig verpflichtende Rechtsgeschäfte

Ein einseitig verpflichtendes Rechtsgeschäft liegt vor, wenn dadurch nur ein Geschäftspartner zur Erbringung einer Leistung verpflichtet wird. In einem Schenkungsvertrag ist beispielsweise nur der Schenker zur Leistungserbringung (nämlich zur Übergabe des Geschenkes) verpflichtet. Der Beschenkte muss dafür keine Gegenleistung erbringen.

In einem zweiseitig verpflichtenden Rechtsgeschäft sind dagegen beide Geschäftspartner zur Erbringung einer Leistung verpflichtet. So ist in einem Kaufvertrag der Verkäufer zur Übergabe der Ware, der Käufer im Gegenzug vor, bei oder nach Erhalt der Ware zur Entrichtung des Kaufpreises verpflichtet.

Vor der Verpflichtung zu unterscheiden ist die *Zustimmung* zu einem Rechtsgeschäft. So muss bei einem Schenkungsvertrag auch der Beschenkte zustimmen, um den Vertrag gültig zustande kommen zu lassen, und kann nicht mit ungewünschten Gütern zwangsbeglückt werden.

5.2.3 Empfangsbedürftige Rechtsgeschäfte

Oft ist eine Grundvoraussetzung für die Gültigkeit eines Rechtsgeschäftes, dass die Willenserklärung, die eine Partei abgibt, von der anderen Partei zur Kenntnis genommen werden kann. Eine Kündigung oder eine Rücktrittserklärung von einer Kaufvereinbarung können nur rechtswirksam

werden, wenn der Vertragspartner davon Kenntnis erlangt. Wie der Zugang dieser Willenserklärung zu erfolgen hat, legt die *Empfangstheorie* [90] fest.

5.2.4 Entgeltliche Rechtsgeschäfte

Entgeltliche Rechtsgeschäfte sind jene, bei denen der Leistung einer Partei die Gegenleistung der anderen Partei gegenübersteht.[91] Eine eindeutige Definition enthält §917 ABGB[92]:

Bei einem entgeltlichen Vertrage werden entweder Sachen mit Sachen, oder Handlungen, worunter auch die Unterlassungen gehören mit Handlungen, oder endlich Sachen mit Handlungen und Handlungen mit Sachen vergolten.

Daraus geht hervor, dass mit „entgeltlich“ nicht ausschließlich eine monetäre Vergütung als Gegenleistung für eine erbrachte Leistung gemeint ist. Vielmehr kommt als Gegenleistung eine Sache oder eine Dienstleistung genauso in Frage.
Es ist wichtig, hervorzuheben, dass Leistung und Gegenleistung miteinander verknüpft sind: bleibt eine Partei säumig, so ist auch die andere Partei zur Erbringung der Gegenleistung nicht verpflichtet. Man bezeichnet diese Verknüpfung auch als *synallagmatischen Vertrag.*[93]

Im Gegensatz dazu stehen die unentgeltlichen Verträge. Der Vertragspartner ist bei Erhalt der Leistung nicht an eine Gegenleistung gebunden. Der Schenkungsvertrag ist zwar als zweiseitiges Rechtsgeschäft zu sehen, da der Beschenkte den Willen bekunden muss, das Geschenk entgegennehmen zu wollen. Allerdings ist der Beschenkte zu keiner Gegenleistung verpflichtet. Somit ist der Schenkungsvertrag ein einseitig verpflichtendes Rechtsgeschäft.

---

[90] *Siehe dazu Kap. 555.4.4*

[91] *(Riedler, 2010, S. 116)*

[92] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Allgemeines bürgerliches Gesetzbuch, Fassung vom 13.09.2017, 1811/2017)*

[93] *(Riedler, 2010, S. 117)*

5.3 Weitere Begriffserklärungen

5.3.1 Konsensualvertrag und Realvertrag

Konsensualverträge kommen durch Einigung (Konsens) der Parteien zustande, ohne dass eine Sachübergabe erfolgen muss. Realverträge sind dagegen erst dann rechtswirksam, wenn zusätzlich zu Parteieneinigung auch die Sachübergabe hinzutritt.[94] Erst diese Sachübergabe verpflichtet den Vertragspartner zur Gegenleistung.[95]

Kaufvertrag, Schenkungsvertrag, Werk- und Arbeitsvertrag, Miet- und Leasingvertrag sind Beispiele für einen Konsensualvertrag, während die Typen Verwahrungsvertrag[96] und Leihvertrag[97] in die Gruppe der Realverträge fallen.

5.3.2 Schuldrecht und Sachenrecht

Das Privatrecht kann auch grob in Schuldrecht und Sachenrecht aufgeteilt werden. Das Schuldrecht beleuchtet mögliche Verpflichtungsgründe, die ein Rechtssubjekt gegenüber einem anderen Rechtssubjekt eingehen kann. Ist ein Rechtssubjekt eine Verpflichtung eingegangen, dann schuldet es einem anderen Rechtssubjekt die Erfüllung eines Anspruches, einer Leistungserbringung.[98] Durch Erbringen dieser Leistung erlischt die Schuld (und damit der Anspruch) des Leistungserbringers gegenüber dem Leistungsempfänger

Das Sachenrecht behandelt Eigenschaften von Rechtsobjekten, also Eigenschaften an Sachen oder Tieren.[99] Der wichtigste Teil des Sachenrechts behandelt das *Eigentum* an Sachen, andere Bereiche befassen sich mit dem *Pfand* an beweglichen oder unbeweglichen Sachen oder mit *Dienstbarkeitsrechten*.[100] Ein wesentlicher Teil des Eigentumsrechts beschäftigt sich mit dem Übertrag des Eigentums von einer Person zu einer

---

[94] *(Riedler, 2010, S. 117)*

[95] *Vgl. auch Kap. 4.4, Vertragsschlussmechanismus*

[96] *Nach den §§ 957 ff ABGB*

[97] *Gemäß §§ 971 ff ABGB*

[98] *(Riedler, 2010, S. 15)*

[99] *Siehe Kap. 5.1.2*

[100] *(Riedler, 2010, S. 15)*

anderen. Dieser Eigentumsübertrag ist wesentlicher Bestandteil des Verkaufes einer Ware.

Das ABGB unterscheidet das dingliche Sachenrecht vom persönlichen Sachenrecht.[101] Das dingliche Sachenrecht geben einer Person Rechte an Sachen ohne Rücksicht auf etwaige dritte Personen. Dagegen übertragen persönliche Sachenrechte nur Rechte an einer Sache gegenüber einer bestimmten anderen Person. Persönliche Sachenrechte sind also obligatorische Rechte, sie wirken nur gegen eine gesetzlich oder vertraglich gebundene Person, den Schuldner.

Dingliche Sachenrechte werden im § 308 ABGB aufgezählt:

Dingliche Sachenrechte sind das Recht [...] des Eigentums, des Pfandes, der Dienstbarkeit und des Erbrechtes.

Das dingliche Recht an einer Sache gibt einer Person das unbeschränkte Recht, über diese Sache unbeschränkt zu verfügen (bis hin zur Zerstörung der Sache).

5.3.3 Verpflichtungsgeschäft

Das Verpflichtungsgeschäft verpflichtet einen Vertragspartner zu einer zukünftigen Leistung, beispielsweise zur Übergabe einer verkauften Sache oder zu einer Dienstleistung – er *schuldet* die Leistungserbringung. Der Leistungsempfänger erhält also einen schuldrechtlichen Anspruch auf eine Leistung und wird dadurch zum Gläubiger.

Beispiel: Bei einem Kaufvertrag über einen Computer verpflichtet sich Vertragspartner A zur zukünftigen Lieferung des Gerätes und Vertragspartner B zur zukünftigen Bezahlung des Kaufpreises nach Lieferung. Ein Kaufvertrag ist also als gegenseitiges Verpflichtungsgeschäft zu verstehen.

5.3.4 Verfügungsgeschäft

Ein Verfügungsgeschäft gibt einem Vertragspartner die unbegrenzte Verfügungsgewalt über eine Sache oder überträgt die unbegrenzte Verfügungsgewalt von einem Vertragspartner auf den anderen. Das Verfügungsgeschäft ist ein unerlässlicher Bestandteil des Eigentumserwerbs,

---

[101] *§ 307 ABGB*

da Eigentümer einer Sache nur jemand sein kann, der unbegrenzt (also ohne Mitsprachemöglichkeit durch andere Personen) über die Sache verfügen kann (also berechtigt ist, sie beispielsweise weiterzuverkaufen, zu verändern oder auch zu zerstören).

5.3.5 Beispiele

5.3.5.1 Kaufvertrag

Ein Kaufvertrag wird zwischen zwei oder mehreren Personen abgeschlossen, die eine Sache gegen Geld (als Gegenleistung) abhandelt. Der Kaufvertrag ist demnach ein mehrseitig verpflichtendes, empfangsbedürftiges und entgeltliches Rechtsgeschäft.

5.3.5.2 Schenkungsvertrag

Ein Schenkungsvertrag wird ebenso zwischen mehreren Personen abgeschlossen, wobei eine Person eine Leistung erbringt, ohne dass die Vertragspartei eine Gegenleistung erbringen muss. Sie muss aber der Schenkung zustimmen. Falls sie ablehnt, kommt kein Vertrag zustande. Der Schenkungsvertrag ist also ein mehrseitiges, einseitig verpflichtendes, empfangsbedürftiges Rechtsgeschäft.

5.3.5.3 Testament

In einem Testament verfügt eine Person über die Weitergabe ihres Eigentums nach ihrem Ableben. Das Testament ist ein einseitiges, nicht empfangsbedürftiges, nicht verpflichtendes und nicht entgeltliches Rechtsgeschäft.

5.4 Vertragsschluss

In diesem Kapitel wird der Fokus auf den Abschluss eines zweiseitigen Vertrages gelegt. Der am häufigsten zur Anwendung gelangende Fall ist der des Kaufvertrages, der nachfolgend vorgestellte Mechanismus kommt aber gleichermaßen bei anderen Vertragstypen wie Schenkungsvertrag oder Werkvertrag zur Anwendung.[102]

Das ABGB regelt die „*Abschließung eines Vertrages*“ [103] im § 861 folgendermaßen:

„Wer sich erklärt, daß er jemandem sein Recht übertragen, das heißt, daß er ihm etwas gestatten, etwas geben, daß er für ihn etwas tun, oder seinetwegen etwas unterlassen wolle, macht ein Versprechen; nimmt aber der andere das Versprechen gültig an, so kommt durch den übereinstimmenden Willen beider Teile ein Vertrag zustande. So lange die Unterhandlungen dauern, und das Versprechen noch nicht gemacht, oder weder zum voraus, noch nachher angenommen ist, entsteht kein Vertrag.“

In Kurzform: ein Vertrag kommt dadurch zustande dass A ein Versprechen macht und B dieses Versprechen annimmt. Es sind also zwei Willenserklärungen [104] notwendig: ein Versprechen und die Annahme desselben. Die Rechtswissenschaft verwendet hierfür die Termini *Angebot* und *Annahme*.

Diese beiden Schritte werden im Folgenden näher beschrieben.

5.4.1 Angebot

Um als Angebot im vertragsrechtlichen Sinn zu gelten, muss eine Willenserklärung vier Voraussetzungen erfüllen:[105]

1. Die Willenserklärung muss inhaltlich bestimmt sein: es muss klar verständlich erkennbar sein, was das Ziel des Angebotes ist (z.B. der Verkauf eines Fahrzeuges)

---

[102] (Riedler, 2010, S. 123)

[103] Siebzehntes Hauptstück: Von Verträgen und Rechtsgeschäften überhaupt (Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Allgemeines bürgerliches Gesetzbuch, Fassung vom 13.09.2017, 1811/2017)

[104] Siehe dazu Kapitel 4.3.1

[105] Siehe auch (Bydlinski, Bürgerliches Recht Band I Allgemeiner Teil, 2007, S. 127)

2. Sie muss den gesetzlich geforderten Mindestinhalt aufweisen: es müssen die vertraglichen Mindestbestandteile (*essentialia negotii*) enthalten sein. Bei einem Kaufvertrag sind dies die betreffende Ware und der Kaufpreis. Aufgrund eines Angebotes, sein Auto verkaufen zu wollen, kann noch kein Kaufvertrag abgeschlossen werden, da das Angebot keinen Kaufpreis enthält.
3. Sie muss einen Bindungswillen des Anbieters zum Ausdruck bringen: mit dem Ausdruck des Bindungswillens räumt der Anbieter der Adressatin das Recht ein, mit einer einseitigen Annahme des Angebotes (bespielweise durch ein einfaches „ja“) den Vertrag zustande zu bringen.[106]
4. Sie muss der Vertragspartnerin zugehen. Die Adressatin muss vom Angebot auch Kenntnis erlangen (es darf nicht in einer Schreibtischlade liegenbleiben).

Klar von einem Angebot zu unterscheiden ist die sogenannte Einladung zur Angebotslegung (*invitatio ad offerendum*): Dazu zählen „Angebote“ in Werbeprospekten, Schaufenstern und dergleichen. Hier kann sich die Anbieterin noch gar nicht binden wollen, da sie noch nicht weiß, wie hoch die Nachfrage nach dem Produkt sein wird und ob sie genügend Waren vorrätig hat. Daher sind üblicherweise Waren, die in einem Prospekt angeboten werden, mit dem Vermerk wie „solange Vorrat reicht“ versehen.

Fraglich ist, wie lange ein Angebot gültig ist und ob es nach einer gewissen Zeitdauer erlischt. Klarerweise erlischt das Angebot bei Annahme oder Ablehnung desselben.

Der Gesetzgeber hat aber auch für einige andere Fälle Vorkehrungen getroffen. So regelt § 862 ABGB die Dauer der Gültigkeit des Angebotes auch für den Fall, dass diese nicht explizit im Angebot ausgewiesen ist.

Demnach muss der unter Anwesenden oder mittels Fernsprechers[107] gemachte Antrag sofort angenommen werden, der einem Abwesenden gemachte Antrag längstens bis zu der Zeit, in der der Angebotsleger unter normalen Umständen das Eintreffen der Antwort erwarten darf.[108]

---

[106] *(Riedler, 2010, S. 129)*

[107] *Telefon*

[108] *§ 862 ABGB*

5.4.2 Annahme

Das ABGB unterscheidet die *Annahme durch Willenserklärung* von der *Annahme durch Willensbetätigung*.

5.4.2.1 Annahme durch Willenserklärung

Die Willenserklärung kann ausdrücklich oder konkludent (d.h. stillschweigend, durch Handlungen, die keinen Zweifel an der Annahme lassen) erfolgen. Dies geht aus der Formulierung des § 863 Abs 1 ABGB hervor:

„Man kann seinen Willen nicht nur ausdrücklich durch Worte und allgemein angenommene Zeichen; sondern auch stillschweigend durch solche Handlungen erklären, welche mit Überlegung aller Umstände keinen vernünftigen Grund, daran zu zweifeln, übrig lassen.“[109]

So kann die Bekanntgabe einer Kontonummer an einen Geschäftspartner, der eine Zahlung schuldet, als stillschweigende Annahme aufgefasst werden.[110]

Jedoch gilt bloßes Schweigen nach österreichischem Recht nicht als Zustimmung, außer den Schweigenden hätte eine Redepflicht getroffen.[111] So gibt § 1081 ABGB an, dass eine Sache, die bereits zur Probe oder Besichtigung an den Käufer übergeben wurde, bei Schweigen des Käufers nach Ablauf der Probezeit als Zustimmung zum Kauf der Sache gilt.

Ebenso wie das Angebot dem Erklärungsempfänger zugehen muss, muss auch die Annahme des Angebotes dem Anbietenden zugehen.[112] Hier ist ebenso wie bei der Angebotslegung die Empfangstheorie maßgeblich.

Die Annahme des Angebotes muss rechtzeitig erfolgen. Rechtzeitigkeit richtet sich vor allem nach der Geltungsdauer des Angebotes, die in Kapitel 5.4.1 behandelt wurde, und in § 862 ABGB geregelt ist. Über die Rechtzeitigkeit der Annahme selbst gibt § 862a ABGB Auskunft:

„Als rechtzeitig gilt die Annahme, wenn die Erklärung innerhalb der Annahmefrist dem Antragsteller zugekommen ist. Trotz ihrer Verspätung

---

[109] *§ 863 Abs 1 ABGB*

[110] *(Riedler, 2010, S. 136)*

[111] *In § 1081 ABGB gilt bei Sachen, die zum Zwecke der*

[112] *(Riedler, 2010, S. 139)*

kommt jedoch der Vertrag zustande, wenn der Antragsteller erkennen musste, dass die Annahmeerklärung rechtzeitig abgesendet wurde, und gleichwohl seinen Rücktritt dem Anderen nicht unverzüglich anzeigt.“[113]

Die Annahmeerklärung kann demnach vom Angebotsempfänger bis zur tatsächlichen Kenntnisnahme durch den Anbietenden auch grundlos widerrufen werden. Vergleichbares gilt auch für die Angebotslegung: auch das Angebot kann bis zur tatsächlichen Kenntnisnahme widerrufen werden.[114]

5.4.2.2 Annahme durch Willensbetätigung

Der § 864 Abs 1 ABGB befasst sich mit Annahmen in den Fällen, in denen Erklärungen nicht zu erwarten sind:

„Ist eine ausdrückliche Erklärung der Annahme nach der Natur des Geschäftes oder nach der Verkehrssitte nicht zu erwarten, so kommt der Vertrag zustande, wenn dem Antrag innerhalb der hierfür bestimmten oder den Umständen angemessenen Frist tatsächlich entsprochen wird.“[115]

Das bedeutet, eine Annahme durch Willensbetätigung ist rechtlich nur dann wirksam, wenn eine Annahme durch Willenserklärung entweder nach

- der Natur des Geschäftes oder
- der Verkehrssitte nicht zu erwarten ist, oder
- Der Anbieter auf eine Annahme durch Willenserklärung verzichtet hat.[116]

Ein Beispiel dafür ist der Erwerb eines Getränkes aus einem Automaten. Gemäß der Natur des Geschäftes ist eine Antwort auf das Angebot durch Willenserklärung nicht sinnvoll (solange der Automat nicht auf Spracheingaben reagiert), die Annahmebekundung muss daher durch andere Arten der Verständigung erfolgen.

Die annehmende Person muss eine Aneignungs- oder Gebrauchshandlung setzen: Dazu zählt z.B. der Einwurf einer Münze in einen Automaten. Diese Annahmehandlung muss von einem Willen zum Vertragsabschluss begleitet sein. Besteht dieser Wille nicht, dann muss er auch vom Annehmenden

---

[113] *§ 862a ABGB*

[114] *(Riedler, 2010, S. 141)*

[115] *§ 864 Abs 1 ABGB*

[116] *(Riedler, 2010, S. 145)*

zeitgerecht geltend gemacht werden, wodurch der Vertrag als nicht geschlossen gilt. Fälle, in denen der Vertrag zustande kommt und beeinsprucht werden soll, werden unter Abschnitt 5.9 behandelt.

Die Annahme durch Willensbetätigung ist nicht zugangsbedürftig, somit ist bei der Rechtzeitigkeit der Annahme nicht der Zeitpunkt des Zuganges sondern der Zeitpunkt des Vornehmens der Annahmehandlung maßgeblich. Trotzdem kann die Annahme bis zur tatsächlichen Kenntnisnahme durch den Angebotssteller widerrufen werden.

5.4.3 Konsens[117]

Voraussetzung für einen gültigen Vertragsschluss ist der Konsens der Vertragsparteien. Die Rechtswissenschaft unterscheidet dabei zwischen verschiedenen Formen von Konsens.

Natürlicher Konsens liegt vor, wenn der jeweilige subjektive Wille der Vertragsparteien übereinstimmt.

Normativer Konsens dagegen bezeichnet das Übereinstimmen der objektiven Erklärungswerte der Willenserklärungen der Parteien. Das Abweichen des objektiven Erklärungswertes vom subjektiven Willen einer Partei wird als Erklärungsirrtum bezeichnet.

Die Ermittlung des objektiven Erklärungswertes erfolgt anhand der *Vertrauenstheorie*, nach der der objektive Erklärungswert einer Willenserklärung so zu verstehen ist, wie sie ein objektiv-redlicher, verständiger und sorgfältiger Empfänger der Erklärung verstehen musste und durfte.[118]

Die Interpretation eines Vertrages ist derart vorzunehmen, dass die erkennbare Absicht der Parteien zu erforschen und auf die Umstände des Falles Bedacht zu nehmen ist.[119] Dabei schadet eine irrtümliche

---

[117] *(Riedler, 2010, S. 200)*

[118] *§863 ABGB*

[119] *(Riedler, 2010, S. 206), siehe auch § 914 in Verbindung mit § 863 ABGB*

Fehlbezeichnung durch die Parteien nach allgemeiner Lehrmeinung nicht – *falsa demonstratio non nocet*.[120]

5.4.4 Zugang einer Erklärung

In den vorigen Kapiteln wurde für einen gültigen Vertragsschluss der Zugang der Willenserklärung an den Erklärungsempfänger vorausgesetzt. Die regulären Arten des Zuganges und deren Ablaufe können noch genauer untersucht werden.
Der Zugang einer Willenserklärung beurteilt sich nach der sogenannten *Empfangstheorie*, die auf §862a des ABGB beruht.[121] [122]

„Nach der Empfangstheorie ist eine Erklärung jedenfalls zugegangen, wenn sie der Empfänger tatsächlich zur Kenntnis nimmt.“ [123]

Dieser erste Satz bedarf keiner weiteren Erklärung. Allerdings kann eine Erklärung auch auf andere Arten gültig an den Erklärungsempfänger gelangen:

„Zugang ist aber schon vorher gegeben, wenn die Erklärung derart in den Machtbereich des Empfängers gelangt, dass sich dieser unter normalen Umständen von ihrem Inhalt Kenntnis verschaffen kann und Störungen nur mehr in seiner Sphäre, nicht mehr beim Absender oder der Übermittlungsanstalt möglich sind.“[124]

Hier ist besonderes Augenmerk auf die Formulierung „*unter normalen Umständen [..] Kenntnis verschaffen kann*“ zu legen. Die tatsächliche Kenntnisnahme der Erklärung ist also nicht notwendig, vielmehr reicht die bloße Möglichkeit, die Willenserklärung zur Kenntnis zu nehmen.

5.4.5 Widerruf eines der Erklärenden

Festzustellen, ob die Willenserklärung ordnungsgemäß zugegangen ist, kann im Fall eines Widerrufes des Angebotes oder auch dessen Annahme

---

[120] *(Riedler, 2010, S. 206)*

[121] *(Riedler, 2010, S. 130)*

[122] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Allgemeines bürgerliches Gesetzbuch, Fassung vom 13.09.2017, 1811/2017)*

[123] *(Riedler, 2010, S. 130)*

[124] *(Riedler, 2010, S. 130)*

entscheidend sein. Denn vor Zugang ist die Erklärung noch nicht wirksam und kann daher vom Erklärenden noch widerrufen werden.[125] Nach erfolgtem Zugang entfaltet die Erklärung ihre Bindungswirkung und gibt dem Empfänger das Recht, den Vertrag durch einseitige Annahme der Erklärung innerhalb einer etwa vorher festgelegten Zeit zu schließen. Dies wird auch als Gestaltungsrecht des Empfängers bezeichnet.

5.4.6 Privatautonomie

Ein wesentlicher Bestandteil des österreichischen Zivilrechtes ist die Privatautonomie. Die Privatautonomie ermöglicht es jedem Rechtssubjekt, durch freie eigene willentliche Entscheidung seine Rechtsverhältnisse eigenverantwortlich nach Belieben innerhalb der gesetzlich vorgegebenen Schranken zu gestalten.[126]

Die mit dieser Gestaltung verbundenen Handlungen äußern sich in sogenannten Rechtsgeschäften. Rechtsgeschäfte (oder Verträge) sind Willenserklärungen von Rechtssubjekten, die rechtlich durchsetzbar und von einem Rechtsfolgewillen getragen sind.[127]

Die Privatautonomie findet sich in verschiedenen Ausformungen, dazu gehören unter anderem die Inhaltsfreiheit, die Typenfreiheit und die Formfreiheit.

Aus dem Grundsatz der Privatautonomie folgt die grundsätzliche Möglichkeit, einen Vertrag auch durch aufeinander abgestimmte Algorithmen zu vereinbaren, die den Vertragsinhalt automatisiert vollziehen.

Allerdings sind verschiedene weitere Aspekte für die Gültigkeit eines Vertrages relevant.

---

[125] *(Riedler, 2010, S. 133)*

[126] *(Riedler, 2010, S. 108)*

[127] *(Riedler, 2010, S. 113)*

5.5 Erfordernisse eines gültigen Vertrages[128]

5.5.1 Geschäftsfähigkeit

Für die Wirksamkeit eines Vertrages ist die Geschäftsfähigkeit der vertragsschließenden Parteien zu berücksichtigen. Kinder unter sieben Jahren sind unfähig, ein Versprechen zu machen oder es anzunehmen.[129] Gleiches gilt für Personen über sieben Jahre, die „den Gebrauch der Vernunft“ nicht haben. [130]

Personen im Alter von 7 bis 14 Jahre gelten als *unmündig Minderjährige*[131] und sind in dem Maß beschränkt geschäftsfähig, dass sie alterstypische geringfügige Alltagsgeschäfte vornehmen können.[132]

Mündig Minderjährige[133] fallen in die Altersgruppe von 14 bis 18 Jahre und sind bei bloß beschränkter Geschäftsfähigkeit berechtigt, über die ihnen zur freien Verfügung überlassenen Sachen und über ihr Einkommen aus eigenem Erwerb frei zu verfügen, ohne die Befriedigung ihrer Lebensbedürfnisse zu gefährden.[134]

Personen, denen ein Sachwalter bestellt ist, können ein zu ihrem Vorteil gemachtes Versprechen annehmen. Geben sie selbst ein Versprechen ab, so ist die Gültigkeit des fallweise geschlossenen Vertrages vom Einverständnis des Vertreters oder des Gerichtes abhängig. Bis diese Einwilligung erfolgt, kann die Vertragspartnerin nicht zurücktreten, aber eine angemessene Frist zur Erklärung verlangen.[135]

Welche Auswirkung hat nun ein Vertragsschluss mit einem Mitglied der jeweiligen Altersgruppe?
Eine Willenserklärung eines Kindes ist absolut nichtig, ein darauf begründeter Vertrag gilt als nicht geschlossen. Zur Abgabe einer Willenserklärung bedarf

---

[128] *So lautet auch der entsprechende Abschnitt im 17. Hauptstück des ABGB*

[129] *§865 Satz 1 ABGB*

[130] *§865 ABGB*

[131] *§21 Abs 2 ABGB*

[132] *§170 Abs 3 ABGB*

[133] *§21 Abs 2 ABGB*

[134] *§170 Abs 2 ABGB*

[135] *§865 ABGB*

das Kind seines gesetzlichen Vertreters, der die nötigen Erklärungen abgibt und entgegennimmt. Allerdings kann auch eine nachträgliche Zustimmung des gesetzlichen Vertreters die rechtliche Unwirksamkeit des Vertrages nicht beheben.[136] Davon ausgenommen und daher zulässig sind jedoch alterstypische Geschenke[137], wie geringfügige Geldgeschenke zum Ankauf eines Eises.[138]

Die beschränkte Geschäftsfähigkeit einer unmündig minderjährigen Person, die jünger als 14 Jahre ist, erlaubt zwar außerhalb dem Abschluss alterstypischer, geringfügiger Alltagsgeschäfte keinerlei Vertragsabschlüsse. Allerdings sind geschlossene Verträge schwebend unwirksam. Die Vertragspartnerin bleibt gebunden, die gesetzlichen Vertreter können den Vertrag durch Zustimmung Wirksamkeit verleihen, oder ihn rückwirkend ungültig setzen.

Unmündig minderjährige Personen, die älter als 14 Jahre sind, sind in der Lage, Geschäfte aus Mitteln des eigenen Erwerbs oder zur freien Verfügung gestellten Mitteln[139] abzuschließen, solange dadurch die Befriedigung ihrer Lebensbedürfnisse nicht gefährdet ist. Entsprechend können bei Gefährdung der Lebensbedürfnisse Verträge gerichtlich für unwirksam erklärt werden.

5.5.2 Wahre Einwilligung

Dieser Abschnitt des 17. Hauptstücks des ABGB behandelt die Voraussetzung für eine gültige Einwilligung. Nach § 869 ABGB muss die Einwilligung frei, ernstlich, bestimmt und verständlich sein.[140] Die Folgeparagraphen befassen sich mit List und Drohung, Irrtum und den Mechanismen der Rückabwicklung des schon geschlossenen Vertrages und allfälliger Wiedergutmachung.[141]

5.5.3 Möglichkeit und Erlaubtheit

Der erste Satz des § 878 ABGB lautet:

---

[136] *(Bydlinski, Bürgerliches Recht Band I Allgemeiner Teil, 2007, S. 51)*

[137] *Gemäß §170 Abs 3 ABGB*

[138] *(Bydlinski, Bürgerliches Recht Band I Allgemeiner Teil, 2007, S. 53)*

[139] *beispielsweise Taschengeld*

[140] *§ 869 ABGB*

[141] *Siehe dazu auch Kapitel 5.9*

Was geradezu unmöglich ist, kann nicht Gegenstand eines gültigen Vertrages werden.

Diese Maxime wird ergänzt durch den ersten Absatz des § 879 ABGB. Dieser lautet:

Ein Vertrag, der gegen ein gesetzliches Verbot oder gegen die guten Sitten verstößt, ist nichtig.

Näher erläutert wird Abs 1 durch den Folgeabsatz. In § 879 Abs 2 ABGB werden Verträge aufgelistet, die beispielgebend für den Abs 1 leg. cit.[142] sind. Behandelt werden die Vermittlung medizinischer Fortpflanzung gegen Entgelt ebenso wie das Ausnutzen einer Zwangslage oder Unerfahrenheit.

Der §879 Abs 3 ABGB verweist auf allgemeine Geschäftsbedingungen und Vertragsformblätter. Dies wird in Abschnitt 5.6 näher behandelt.

5.5.4 Form der Verträge

Das Privatrecht lässt seinen Rechtsunterworfenen die Möglichkeit, seine Rechtssachen – mit wenigen Ausnahmen – in selbst gewählter Form zu regeln. Der § 883 ABGB erläutert genauer:

Ein Vertrag kann mündlich oder schriftlich; vor Gerichte oder außerhalb desselben; mit oder ohne Zeugen errichtet werden. Diese Verschiedenheit der Form macht, außer den im Gesetze bestimmten Fällen, in Ansehung der Verbindlichkeit keinen Unterschied.[143]

Genaueres über die Erfordernisse eines Vertrages, bei dem durch das Gesetz oder aufgrund des Wunsches der Vertragsparteien die Schriftform notwendig ist, regelt der § 886 ABGB. In diesen Fällen besteht die Notwendigkeit, eine Unterschrift zu leisten, oder Setzung eines notariell beglaubigten Handzeichens vor zwei Zeugen.

---

[142] *Legis citatae (lat.: Recht zitiert): In dem gerade zitierten Gesetz*

[143] *§ 883 ABGB*

5.6 Allgemeine Geschäftsbedingungen[144]

Allgemeine Geschäftsbedingungen sind vorformulierte, standardisierte Vertragsbedingungen, die ein Vertragspartner für alle oder eine bestimmte Gruppe von Verträgen erstellt.[145] Dies stellt den Vertragspartner, der diese AGB nicht formuliert hat, vor die Wahl, diese Bedingungen zusätzlich zu akzeptieren oder vom Vertragsabschluss Abstand zu nehmen. Entsprechend rigide verlangt das Recht vom Aussteller der AGB, diese gut wahrnehmbar und klar formuliert dem Empfänger kenntlich zu machen. Im Streitfall wird nach österreichischem Recht in einem dreistufigen Verfahren geprüft, ob und wie weit die AGB für die Umsetzung eines geschlossenen Vertrages Gültigkeit erlangt haben.

5.6.1 Einbeziehungskontrolle

Um die AGB zum Vertragsinhalt zu erheben, müssen sie bei der Angebotserstellung deutlich gemacht werden. In Geschäftsräumen erfolgt dies durch Aushang an gut sichtbarer Stelle im Geschäftslokal, auf dem schriftlichen Vertragstext durch einen Verweis auf umseitig gedruckte AGB und im Falle des online abgeschlossenen Geschäftes auf den deutlichen Hinweis (z.B. mittels Verlinkung) auf die betreffende Textstelle auf der Website. Dabei ist es nicht ausschlaggebend, ob der Kunde die AGB tatsächlich liest, sondern es reicht, dass er gemäß der Vertrauenstheorie wissen musste, dass der Anbieter unter Einbeziehung der AGB den Vertrag abschließen wollte.

Der gültige Vertragsschluss erfordert die Zustimmung des Kunden auch zu den AGB, wobei diese Zustimmung ausdrücklich oder konkludent erfolgen kann. Die konkludente Zustimmung erfolgt bereits dadurch, dass der Kunde wissen musste, dass der Anbieter unter Einbeziehung der AGB den Vertrag abschießen wollte und dem nicht widersprochen hat.

Dieses Erfordernis schließt demnach die Vorgangsweise aus, die AGB erst bei Zusendung des ausgefertigten Vertrages oder gar bei Lieferung der Ware mitzusenden. Die Kenntnisnahme muss *vor* dem Vertragsschluss erfolgen.

---

[144] *(Riedler, 2010, S. 169 ff)*

[145] *(Riedler, 2010, S. 169)*

5.6.2 Geltungskontrolle

Die Geltungskontrolle befasst sich nicht mehr mit den AGB als Gesamtwerk sondern beleuchtet jede einzelne darin enthaltene Klausel.[146] Maßgeblich dafür ist der Inhalt des § 864a ABGB:

„Bestimmungen ungewöhnlichen Inhaltes in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern, die ein Vertragsteil verwendet hat, werden nicht Vertragsbestandteil, wenn sie dem anderen Teil nachteilig sind und er mit ihnen auch nach den Umständen, vor allem nach dem äußeren Erscheinungsbild der Urkunde, nicht zu rechnen brauchte; es sei denn, der eine Vertragsteil hat den anderen besonders darauf hingewiesen."

Darin sind vier Elemente enthalten, die einzeln herausgearbeitet werden müssen:[147]

- Eine Bestimmung ungewöhnlichen Inhaltes
- Nachteiligkeit für den Vertragspartner
- Überraschung
- Kein besonderer Hinweis auf die ungewöhnliche Klausel

Dabei liegt eine Bestimmung ungewöhnlichen Inhaltes dann vor, wenn sie üblicherweise in solchen Verträgen nicht enthalten ist (objektiv ungewöhnliche Bestimmung) oder wenn sie – obwohl im Allgemeinen durchaus üblich – für den konkreten Fall und diesen konkreten Vertragspartner aus Sicht des Aufstellers der AGB überraschend sein musste, sodass dieser nicht damit rechnen durfte, dass der Partner den AGB zustimmen würde.

Nachteilig ist die Vertragsbestimmung dann, wenn sie den Vertragspartner im Vergleich zum Verfasser der AGB schlechter stellt oder zu Lasten des Betroffenen vom dispositiven Recht abweicht. Dabei ist eine gröbliche Benachteiligung nicht erforderlich.

Der Überraschungseffekt ist dann gegeben, wenn die Klausel in den AGB derart versteckt ist, dass der Vertragspartner nicht mit ihnen rechnen musste. Dagegen sind ungewöhnliche Klauseln nicht als überraschend einzustufen, wenn sie durch ihre Stellung im Vertragstext, durch gesonderte Markierung (Farbe, Fettdruck, …) auffällig gemacht wurden, sodass der Partner mit Eintritt der ungewöhnlichen Klausel rechnen durfte.

---

[146] *(Riedler, 2010, S. 173)*

[147] *(Riedler, 2010, S. 174)*

Gleiches trifft zu, wenn der Aufsteller der AGB seinen Vertragspartner ausdrücklich auf diese Klauseln hingewiesen hat. Stimmt der Vertragspartner trotz des Hinweises der Klausel zu, dann wird sie auch – vorbehaltlich der nachfolgenden Inhaltskontrolle - zum Vertragsinhalt.

Wenn die Klausel allerdings den Tatbestand des §864a ABGB erfüllt, wenn also eines der vier obigen Elemente zutrifft, dann wird sie nicht Teil des Vertrages. Durch diese Nichtigkeit besteht auch keine Notwendigkeit der Anfechtung durch den Vertragspartner. Trotz der Nichtigkeit dieser Klausel gilt allerdings der Rest des geschlossenen Vertrages weiter.

5.6.3 Inhaltskontrolle

Bei der Inhaltskontrolle wird überprüft, ob der Inhalt jeder einzelnen Klausel sachlich nicht gerechtfertigte oder benachteiligende Inhalte zu Lasten des Vertragspartners des Verfassers hat. Die Prüfung umfasst einerseits den Bestand gegenüber dem § 879 Abs 3 ABGB (*Generalnorm*); andererseits wird auch die Prüfung gegen § 6 KSchG (*Spezialnorm für Verbrauchergeschäfte*) vorgenommen.[148]

5.6.3.1 Generalnorm

Der § 879 Abs 3 ABGB lautet wie folgt:

Eine in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern enthaltene Vertragsbestimmung, die nicht eine der beiderseitigen Hauptleistungen festlegt, ist jedenfalls nichtig, wenn sie unter Berücksichtigung aller Umstände des Falles einen Teil gröblich benachteiligt.

Dabei sind mit den Hauptleistungen im Kaufvertrag die Ware und der Preis, in Werkverträgen das zu erstellende Werk und der dafür zu entrichtende Preis und für andere Vertragstypen Entsprechendes gemeint.

Daher ist der Tatbestand von §879 Abs 3 ABGB dann erfüllt, wenn

- Eine Nebenbestimmung in den AGB oder Vertragsformblättern betroffen ist, und
- der Vertragsunterworfene gröblich benachteiligt wird.

[148] *(Riedler, 2010, S. 177)*

Mit vertraglichen Nebenbestimmungen können beispielsweise die Zeit und der Ort der Vertragserfüllung gemeint sein. Was eine gröbliche Benachteiligung darstellt, ist anhand der Umstände des Einzelfalles zu beurteilen. Dabei ist unter Berücksichtigung aller Umstände des Falles eine Gesamtbewertung vorzunehmen, wobei eine benachteiligende Regelung durch eine umso vorteilhaftere andere Regel durchaus ausgeglichen werden kann. Als Faustregel gilt: je deutlicher sich die Rechtspositionen von Aufsteller der AGB und Unterworfenen der AGB voneinander unterscheiden und je fragiler damit die Rechtsposition des Unterworfenen wird, desto eher kann auf eine gröbliche Benachteiligung geschlossen werden.

Die Rechtfolge eines Verstoßes einer Vertragsklausel gegen § 879 Abs 3 ABGB ist die Nichtigkeit der Klausel bei Weiterbestand des Restes des Vertrages.

5.6.3.2 Spezialnorm

Sowie das KschG[149] insgesamt gilt natürlich auch der §6 KSchG nur für Verbraucherverträge. Bei Anwendung dieser Art von Verträgen ist neben der Inhaltskontrolle gemäß der Generalnorm aus § 879 Abs 3 ABGB auch die Inhaltskontrolle nach § 6 KSchG durchzuführen.

Der §6 Abs 1 KSchG zählt in 15 Ziffern (Z1 bis Z15) abschließend diejenigen Vertragsbestimmungen auf, die für den Verbraucher jedenfalls nicht verbindlich sind. Diese Regelungen umfassen beispielsweise unangemessen lange Fristen (Z1), nicht zugegangene Erklärungen des Unternehmers an den Verbraucher, die vom Unternehmer als zugegangen definiert werden (Z3), die Einforderung einer Erklärung in einer strengeren Form als der Schriftform (Z4) oder Ausschluss von Leistungsverweigerungs- oder Zurückhaltungsrechten durch den Verbraucher (Z6 und 7).

IN §6 Abs 2 KSchG erfolgt eine Aufzählung der Bestimmungen, die für einen Verbraucher jedenfalls nicht verbindlich sind, außer wenn der Unternehmer nachweisen kann, dass er sie mit dem Verbraucher im Einzelnen ausgehandelt hat. Dabei reicht eine deutliche Hervorhebung und Erörterung im Vertragstext nicht aus, vielmehr muss jeder einzelnen Bestimmung für sich zugestimmt worden sein. Dies schließt wiederum eine Vorformulierung in AGB oder Vertragsformblättern aus. Beispiele der aufgezählten Tatbestände

[149] *Siehe §1 Abs 1 KSchG*

in Abs 2 leg. cit.[150] umfassen ein sachlich nicht gerechtfertigtes Rücktrittsrecht des Unternehmers (Z1) oder nicht zumutbare Leistungsänderungsrechte des Unternehmers (Z3).

Außerdem ist gemäß §6 Abs 3 KSchG eine in AGB oder Vertragsformblättern enthaltene Vertragsbestimmung unwirksam, wenn sie unklar formuliert ist.

Schließlich können nach §28 f KSchG von Interessensvertretungen (Bundeswirtschaftskammer, Bundesarbeiterkammer, ÖGB, und div.) Verbandsklagen erhoben werden, um die generelle Unterlassung strittiger Klauseln auf Dauer zu unterbinden.

5.6.4 Zusammenfassung

Zusammenfassend lässt sich festhalten, dass AGB, die schon an der Einbeziehungskontrolle scheitern, als Ganzes nicht zum Inhalt des Vertrages werden.
Werden die AGB nach bestandener Einbeziehungskontrolle Bestandteil des Vertrages, dann sind einzelne Klauseln, die der Geltungskontrolle des §864a ABGB widersprechen, vom Vertrag ausgenommen (*nichtig*) und der Rest des Vertrages bleibt gültig.
Jene Einzelbestimmungen, die der Inhaltskontrolle der §879 Abs 3 ABGB und §6 KSchG nicht standhalten, werden entweder als Ganze nichtig und damit nicht Vertragsteil oder teilweise nichtig und auf die Funktion einer „Restgeltung“ reduziert.

[150] *Legis citatae (lat.: Recht zitiert): In dem gerade zitierten Gesetz*

5.7 Die Begriffe Wurzelmangel und Leistungsstörung

5.7.1 Wurzelmangel

Mit Wurzelmangel bezeichnet man Mängel, die zum Zeitpunkt des Vertragsschlusses bestehen. In solchen Fällen stellt sich die Frage, ob überhaupt ein Vertrag zustande kommt. Ein Wurzelmangel besteht, wenn eine Vertragspartei gemäß § 865 ABGB aufgrund ihres Alters unfähig ist, ein Versprechen zu machen oder es anzunehmen.

5.7.2 Leistungsstörung

Vom Wurzelmangel abzugrenzen ist der Fall, bei dem es bei einem gültig geschlossenen Vertrag im Zuge der Abwicklung zu Störungen kommt. Beispielsweise könnte eine käuflich erworbene Sache zum vereinbarten Liefertermin nicht liefernd sein, oder der Empfänger der Sache insolvent, wodurch bei Lieferung keine Gegenleistung Zug um Zug erbracht werden kann.

5.7.3 Mögliche Rechtsfolgen

In beiden Fällen –Wurzelmangel ebenso wie Leistungsstörung – stellt sich die Frage nach den möglichen Rechtsfolgen für die vertragsschließenden Parteien.

5.7.3.1 Absolute Nichtigkeit

Ein absolut nichtiger Vertrag gilt als nicht geschlossen, und erwirkt auch keine Rechtskraft. Es wurde niemand zur Leistung einer Folgehandlung verpflichtet. Daher kann dieses Rechtsgeschäft auch nicht angefochten werden, es ist nicht existent.
Gründe für absolute Nichtigkeit sind beispielsweise[151]

- Parteiendissens
- Unzureichender Mindestinhalt
- Unbestimmbarkeit
- Unverständlichkeit
- Erkennbare fehlende Ernstlichkeit
- Scheingeschäft

[151] *(Riedler, 2010, S. 216)*

- Anfängliche Unmöglichkeit

5.7.3.2 Relative Nichtigkeit

Das Rechtsgeschäft bleibt vorerst gültig, solange sich die vom Gesetz geschützte Partei nicht auf die Nichtigkeit des Vertrages beruft. Allerdings hat der nicht geschützte Teil keine Möglichkeit, Nichtigkeit einzufordern. Er bleibt an das Rechtsgeschäft gebunden. Auch hier ist der Vertrag, sobald er für nichtig erklärt wurde, nicht mehr existent.[152]

5.7.3.3 Schwebende Unwirksamkeit

In den Zustand schwebender Unwirksamkeit gelangen Rechtsgeschäfte mit unmündig Minderjährigen.[153] Dabei ist die minderjährige Person nicht an den Vertrag gebunden, deren Geschäftspartner allerdings schon. Der gesetzliche Vertreter (meistens ein Elternteil) der unmündig minderjährigen Person kann allerdings den schwebend unwirksamen Vertrag durch seine Zustimmung in Kraft setzen. In dem Fall wird der Vertrag rückwirkend gültig. Erteilt der Elternteil keine Zustimmung, dann bleibt der Vertrag unwirksam. Der Geschäftspartner kann etwaig erbrachte Leistungen zurückfordern.

5.7.3.4 Anfechtbarkeit

Anfechtbar können Verträge werden, die zunächst gültig geschlossen werden, bei denen aber einer Person durch Fehlverhalten des Vertragspartners ein Gestaltungsrecht eingeräumt wird. Dieses Gestaltungsrecht erlaubt es der benachteiligten Person, durch einseitige Erklärung den Vertrag anzupassen oder aufzulösen. Die Vertragsanfechtung bewirkt die Rücksetzung in den Zustand vor dem Vertragsschluss. Beispiele für die Erlangung eines Gestaltungsrechtes treten bei Geschäften auf, die mittels List oder Drohung geschlossen wurden oder in denen ein Irrtum eine Rolle gespielt hat.[154]

---

[152] *(Riedler, 2010, S. 217)*

[153] *Siehe auch Kap. 5.5.1*

[154] *Siehe auch Kap. 5.9*

5.8 Hindernisse beim Vertragsschluss

Die Rechtswissenschaft kennt eine größere Anzahl an möglichen Hindernissen für den gültigen Abschluss eines Vertrages. Hinweise darauf gibt der §869 ABGB, darin der erste Satz:

„Die Einwilligung in einen Vertrag muss frei, ernstlich, bestimmt und verständlich erklärt sein."

Die *Bestimmtheit* ist eine Grundvoraussetzung für eine Willenserklärung, die ein Angebot im Rechtssinn darstellen soll. Damit dies zutrifft, müssen zumindest die essentialia negotii[155] enthalten sein. Für einen Kaufvertrag sind diese Mindestinhalte die Ware und der dafür zu entrichtende Preis.

Die *Verständlichkeit* einer Erklärung zielt auf die Frage ab, welcher Erklärungswert aus der Erklärung ableitbar ist.

Die *Ernsthaftigkeit* der Erklärung wird in den folgenden Punkten abgehandelt:

5.8.1 Mangelnde Ernsthaftigkeit

Eine Willenserklärung ist auf die Herbeiführung von Rechtsfolgen gerichtet.[156] Zielt die Erklärung allerdings nicht auf die Herbeiführung von Rechtsfolgen ab, sondern ist für einen objektiv-redlichen Erklärungsempfänger erkennbar nur zum Scherz abgegeben, dann liegt eine *Scherzerklärung* vor. Solche Erklärungen binden den Erklärenden nicht und sind ungültig. Allerdings binden solche Erklärungen, die aus der Sicht eines objektiv-redlichen Empfängers nicht als Scherz erkennbar sind, den Erklärenden sehr wohl. (Allerdings Erklärungsirrtum des Erklärenden)

5.8.2 Mentalreservation

Eine Mentalreservation oder ein sogenannter geheimer Vorbehalt liegt vor, wenn die Erklärende eine Erklärung abgibt, die nach ihrem mentalen[157] Vorbehalt nicht die Rechtsfolgen auslösen soll, die aus der Sicht eines objektiv-redlichen Dritten als gewollt erscheinen.[158] Der Erklärenden ist

---

[155] *Der notwendige Mindestinhalt für den jeweiligen Vertragstyp*

[156] *Siehe dazu auch die Def. in Kap. 5.1.3*

[157] *Inneren, geistigen Vorbehalt, der nicht nach außen kommuniziert wird*

[158] *(Riedler, 2010, S. 225)*

bewusst, dass der objektive Erklärungswert von ihrem inneren Willen abweicht.
Der Erklärungswert einer Willenserklärung ist nach der *Vertrauenstheorie* zu ermitteln.[159] Konnte ein objektiv-redlicher Erklärungsempfänger die fehlende Ernsthaftigkeit nicht erkennen, dann ist die Erklärung gültig, und der mentale Vorbehalt muss nicht beachtet werden. Erkennt allerdings die Erklärungsempfängerin, dass die Erklärende an ihre Erklärung nicht gebunden sein will, dann ist die Erklärung als ungültig zu sehen.[160]

5.8.3 Scheingeschäfte

Scheingeschäfte können als „doppelte Scherzerklärung" aufgefasst werden. Ein solches Scheingeschäft liegt dann vor, wenn beide Vertragsparteien übereinstimmend im gegenseitigen Einverständnis Erklärungen abgeben, die nicht die Rechtsfolgen auslösen sollen, die ein objektiv-redlicher Dritter als gewollt verstehen würde. Beide Parteien wollen also nicht an ihre Erklärungen gebunden sein.
Beispielsweise können die Parteien einen geringeren Kaufpreis für ein Grundstück notariell beglaubigen lassen, und den tatsächlichen Preis nicht dokumentieren, um die geforderten Abgaben niedriger zu halten. Solche Scheingeschäfte sind entsprechend § 916 Abs1 S 1 ABGB nichtig.[161]

5.8.3.1 Umgehungsgeschäft

Von Scheingeschäften ist das Umgehungsgeschäft abzugrenzen. Umgehungsgeschäfte verfolgen zumeist dasselbe Ziel wie Scheingeschäfte, nämlich die „Optimierung" von Abgabezahlungen. Unterschiedlich ist die Methode dazu. Während die Vertragsparteien an die Erklärungen eines Scheingeschäftes nicht gebunden sein wollen, liegt beim Umgehungsgeschäft ein Bildungswille gerade doch vor. Angestrebt wird allerdings eine andere Rechtsform, um der Rechtswidrigkeit des Scheingeschäftes zu entgehen.

Beispiele für Umgehungsgeschäfte beinhalten die Verwendung von „Strohmännern", um Verkaufsverbote an bestimmte Personengruppen zu umgehen. Ein anderes Beispiel betrifft den Abschluss eines Untermietvertrages, obwohl dem Mietrechtsgesetz entsprechend ein Hauptmietvertrag abzuschließen gewesen wäre.

---

[159] Siehe Kapitel 5.4.3 Konsens: Der Erklärungswert ist aus der Sicht eines objektiv-redlichen Dritten zu bestimmen

[160] Nach aktueller Rechtsprechung: Ob 36/82 SZ 56/11

[161] (Riedler, 2010, S. 227 ff)

5.8.4 Gesetzwidrigkeit

Gesetzwidrigkeit ist im § 879 Abs 1 ABGB geregelt:

„Ein Vertrag, der gegen ein gesetzliches Verbot oder gegen die guten Sitten verstößt, ist nichtig“[162]

Damit setzt der Gesetzgeber der Privatautonomie, insbesondere der freien Ausgestaltung des Vertragsinhaltes Grenzen. Gesetzwidrig sind Rechtsgeschäfte nur dann, wenn sie gegen zwingende Rechtsvorschriften verstoßen. Zulässig sind jedoch Rechtsgeschäfte, wenn sie dispositive Normen im Einverständnis der Vertragsparteien umgehen. [163]

5.8.5 Formvorschriften

Obwohl im Allgemeinem gemäß der Privatautonomie Verträge nach Parteienübereinkunft in beliebig vereinbarter Form (schriftlich, mündlich, durch Handschlag, etc.) geschlossen werden können, schreibt das österreichische Privatrecht doch in einigen Fällen eine bestimmte Form vor.

Beispielsweise erfordern Kauf-, Tausch-, Renten- und Darlehensverträge zwischen Ehegatten die Form eines Notariatsakts, also die Herstellung einer schriftlichen Urkunde im Beisein eines Notars mit der eigenhändigen Unterfertigung durch die Vertragsparteien.[164]

Die Anmeldung einer Eintragung ins Firmenbuch erfordert die notarielle Beglaubigung, also die Beurkundung durch einen Notar, dass die von ihm beglaubigte Unterschrift von einer bestimmten Person stammt. [165]

Gesetzliche Formvorschriften sind zwingendes Recht. Werden sie nicht eingehalten, so liegen gesetzeswidrige (unerlaubte) Rechtsgeschäfte vor.[166] Folgen dieser Gesetzeswidrigkeit reichen von absoluter Nichtigkeit des

---

[162] § 879 Abs 1 ABGB

[163] Fast alle Normen des öffentlichen Rechts sind als zwingendes Recht zu verstehen, da sie im Interesse der Allgemeinheit liegen, und deshalb nicht durch Parteienvereinbarung geändert werden dürfen.

[164] (Riedler, 2010, S. 259)

[165] § 11 UGB, (Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Unternehmensgesetzbuch, Fassung vom 13.09.2017)

[166] § 879 Abs 1 ABGB

Rechtsgeschäfts über relative Nichtigkeit eines Vertragsteiles bis zu zivilrechtlicher Unbeachtlichkeit bei verwaltungsrechtlichen Sanktionen. [167]

[167] *(Riedler, 2010, S. 262)*

5.9 Anfechtung von Verträgen

Das österreichische Zivilrecht bietet die Möglichkeit, einen schon gültig geschlossenen Vertrag aus verschiedenen Gründen anzufechten, wenn dafür eine Reihe von Voraussetzungen erfüllt wird. Neben der Anfechtung mit dem Ergebnis der gänzlichen oder teilweisen Aufhebung des Vertrages besteht auch die Möglichkeit der Abänderung des Vertrages und damit grundsätzlichen Beibehaltung des Vertragsschlusses.

In beiden Fällen möchte die anfechtende Partei ein *Gestaltungsrecht* erwirken, dass ihr die Möglichkeit gibt, durch einseitige Willenserklärung[168] den Vertrag abzuändern oder ganz aufzuheben.

Davon unberührt bleiben allerdings alle Anspruchsgrundlagen wie Schadensersatz oder Anspruch auf Rückabwicklung. Diese werden im ABGB getrennt geregelt.[169]

Nachfolgend werden die wichtigsten Gründe für eine Vertragsaufhebung oder Vertragsänderung beschrieben.

5.9.1 Irrtum

Mit Irrtum bezeichnet man eine falsche oder fehlende Vorstellung von der Wirklichkeit, also von Fakten, Vorgängen oder Zusammenhängen.[170]

In diesem Zusammenhang können drei Arten von Irrtümern unterschieden werden.

5.9.1.1 Erklärungsirrtum

Ein Erklärungsirrtum liegt dann vor, wenn die objektive Bedeutung der Erklärung des Irrenden von dessen inneren Willen abweicht. Die irrende Person erklärt also nach außen ein Vorhaben bestimmten Inhaltes, meint jedoch etwas anderes als nach außen erklärt wurde.
Werden bei der Analyse des Vorganges der äußere Erklärungswert mithilfe der Vertrauenstheorie und der innere Wille des Erklärenden verglichen und eine Divergenz zwischen beiden ermittelt, dann liegt ein Erklärungsirrtum vor.

---

[168] *d.h. ohne das eine Zustimmung der Gegenpartei vonnöten ist*

[169] *Den Schadensersatz regelt § 874 ABGB, den Anspruch auf Rückabwicklung §877 ABGB*

[170] *(Riedler, 2010, S. 271)*

Dazu zwei Bespiele:

1. Die Person K möchte schriftlich 3,5 Kilogramm einer Ware bestellen, vertippt sich allerdings und bestellt 35 kg. Hier weicht der äußere Erklärungswert mit 35 kg deutlich vom inneren Willen (3,5 kg) ab. Ein Erklärungsirrtum liegt vor.
2. Eine aus Westösterreich stammende Studentin möchte in einem Wiener Altbau eine Wohnung im ersten Stock mieten. Ihr innerer Wille ist es, einen Stock höher als das Erdgeschoß zu wohnen.
   Allerdings wird in Wiener Altbauten der nächst höher gelegene Stock als Mezzanin bezeichnet, und das in ihrer Erklärung als 1.Stock bezeichnete Geschoß liegt zwei Geschoße über dem Erdgeschoß. Auch hier liegt ein Erklärungsirrtum vor.[171]

5.9.1.2 Geschäftsirrtum

Im Fall des Geschäftsirrtums irrt die erklärende Person nicht über den Inhalt ihrer eigenen Erklärung sondern über einen tatsächlichen Umstand, der zum Vertragsinhalt geworden ist.

Lässt sich also herausarbeiten,

- über welchen Umstand sich die Person geirrt hat und
- welche Umstände durch Parteienkonsens Vertragsinhalt geworden sind,

dann liegt ein Geschäftsirrtum in dem Fall vor, wenn der Umstand, über den Irrtum besteht, auch Teil des Vertrages geworden ist.

Geschäftsirrtümer können in einen der folgenden Bereiche fallen:

1. Über die Natur des Geschäftes: A möchte von B ein Auto ausleihen und denkt dabei an unentgeltliche Leihe unter Freunden. B ist allerdings in einer Autovermietung beschäftigt und glaubt, dass es sich bei dem Geschäft um einen entgeltlichen Mietvertrag handelt.

2. Über den Vertragsgegenstand: A kauft ein als „antik“ bezeichnetes Möbelstück um 20000 Euro. Allerdings ist das Möbelstück zwar im viktorianischen Stil gehalten, allerdings erst vor kurzem in China

[171] *(Riedler, 2010, S. 272)*

erzeugt worden und nur 2000 Euro wert.

3. Über geschäftsrelevante Eigenschaften des Vertragsgegenstandes: Damit meint man Eigenschaften des Vertragsgegenstandes, die durch Parteienvereinbarung zum Vertragsinhalt geworden sind oder gewöhnlich beim betreffenden Gegenstand vorausgesetzt werden können. Als Beispiele sind der Kilometerstand[172] und Baujahr[173] eines Autos, oder die Größe einer Wohnung[174] anzuführen.
   Ein Geschäftsirrtum ist immer dann gegeben, wenn der Erklärende über Umstände irrt, über die der andere nach den geltenden Rechtsvorschriften aufklären hätte müssen.[175]

4. Über die Identität der Person des Vertragspartners oder über für das Geschäft wesentliche Eigenschaften dieser Person: insbesondere zielt hier das Gesetz auf den Irrtum über das Vorhandensein einer verwaltungsrechtlichen Befugnis zur Erbringen einer vereinbarten Leistung ab.[176] Wird z.B. ein Handwerker für eine Reparatur bestellt, der jedoch für diese Reparatur keine behördliche Konzession besitzt, dann liegt ein Irrtum über wesentliche Eigenschaften der Person des Vertragspartners vor.

5.9.1.3 Motivirrtum

Während sich der Geschäftsirrtum auf einen Umstand innerhalb des Vertragsinhaltes bezieht, bezieht sich der Motivirrtum auf einen Umstand außerhalb des Vertragsinhalts. Ähnlich wie beim Geschäftsirrtum wird bei der Analyse der Irrtums herausgearbeitet,

- über welchen Umstand sich die Person geirrt hat und
- welche Umstände durch Parteienkonsens Vertragsinhalt geworden sind.

Bezieht sich der Irrtum auf einen Umstand, der außerhalb des Vertragsinhalts liegt, dann liegt ein Motivirrtum vor.

---

[172] *7 Ob 171/70 JBl 1971, 258*

[173] *1 Ob 34/72 SZ 45/38*

[174] *5 Ob 573/80 Miet 32.096/28*

[175] *§ 871 Abs 2 ABGB*

[176] *§ 873 S 2 ABGB*

Der Motivirrtum ist bei entgeltlichen Geschäften[177] grundsätzlich unbeachtlich[178] und löst keine Rechtsfolgen aus, auch wenn das Motiv bei Vertragsschluss geäußert oder vom Vertragspartner erkannt wurde.

Beachtlich ist der Motivirrtum allerdings in folgenden Fällen:

- Bei List,
- bei Testamenten oder letztwilligen Verfügungen,
- bei unentgeltlichen Geschäften unter Lebenden, und
- wenn das Motiv zum Vertragsinhalt erhoben wird (da dann ein Geschäftsirrtum vorliegen würde)

Die Voraussetzungen für eine erfolgreiche Anfechtung oder Anpassung wegen Irrtums können in 4 Stufen unterteilt werden.

5.9.1.4 Beachtlichkeit des Irrtums

Als beachtliche Irrtümer gelten der Vertragsirrtum und der Geschäftsirrtum, während der Motivirrtum außer in den oben angeführten Fällen als unbeachtlich einzustufen ist.

5.9.1.5 Kausalität des Irrtums für den Vertragsschluss

Dazu muss die Frage beantwortet werden, ob der Vertrag vom Irrenden auch nach Kenntnis der wahren Sachlage (also ohne den Irrtum) in derselben konkreten Gestalt geschlossen worden wäre. Ist die Frage zu bejahen, dann war der Irrtum für den Vertragsschluss nicht kausal. [179]

5.9.1.6 Fehlendes Vertrauensschutzbedürfnis des Gegners

Grundsätzlich darf der Vertragspartner der irrenden Partei auf die Gültigkeit des geschlossenen Vertrages vertrauen. Der Gesetzgeber bietet insofern Schutz, als er die Möglichkeit bietet, die Umsetzung des Vertrages notfalls gerichtlich durchsetzen zu lassen.[180]

Allerdings gibt es Fälle, in denen die irrende Partei schutzwürdiger ist als seine Gegnerin. Tritt einer der drei in §871 Abs 1 ABGB angeführten Fälle

---

[177] z.B. Kaufvertrag, Mietvertrag, Leasing, Versicherungsvertrag

[178] Siehe Kap. 5.9.1.4

[179] (Riedler, 2010, S. 278)

[180] Pacta sunt servanda (lat.: Verträge sind einzuhalten) – gilt als allgemeiner, nicht festgeschriebener Rechtsgrundsatz

ein, so überwiegt das Interesse der Vertragsanfechtung oder Vertragsanpassung des Irrenden das Vertrauen seines Gegners auf den objektiven Erklärungswert des Vertrages.

„War ein Teil über den Inhalt der von ihm abgegebenen Erklärung in einem Irrtum befangen, der die Hauptsache oder eine wesentliche Beschaffenheit derselben betrifft, [..] so entsteht für ihn keine Verbindlichkeit, falls der Irrtum durch den anderen veranlaßt war, oder diesem aus den Umständen offenbar auffallen mußte oder noch rechtzeitig aufgeklärt wurde“ [181]

Für die Anwendbarkeit dieses Paragraphen sind also drei Dinge zu überprüfen:

1. Hat der Vertragspartner den Irrtum veranlasst?
   Der Vertragspartner hat den Irrtum veranlasst, wenn sein Verhalten nach der allgemeinen Lebenserfahrung geeignet ist, einen Irrtum hervorzurufen.[182] Man unterscheidet:
   a. Veranlassen durch aktives Tun: hier reichen (im Unterschied zur Anfechtbarkeit durch List)[183] Sorgfaltswidrigkeit oder Pflichtverletzung nicht.
   b. Veranlassen durch Unterlassen: kommt dann in Frage, wenn für den Unterlassenden eine Aufklärungspflicht bestanden hätte.

2. Hätte dem Gegner der Irrtum auffallen müssen?
   Offenbar auffallen muss der Irrtum[184], wenn er bei verkehrsüblicher Sorgfalt erkennbar gewesen wäre oder der Partner Verdacht hätte schöpfen müssen; wenn er also den Irrtum fahrlässig nicht entdeckt hat.[185]

3. Wurde der Irrtum noch rechtzeitig aufgeklärt?
   Der Irrtum ist dann rechtzeitig aufgeklärt, wenn der Gegner der irrenden Partei noch keine wirtschaftlichen Schritte im Vertrauen auf die Gültigkeit des Vertrages unternommen hat.

---

[181] *§ 871 Abs 1 ABGB*

[182] *Die Entscheidung in Bezug auf die allgemeine Lebenserfahrung, muss ein Gericht von Fall zu Fall individuell treffen.*

[183] *(Riedler, 2010, S. 279)*

[184] *z.B. die Verwechslung von Preisen für Kilogramm und Tonnen (7 Ob 671/78 SZ 51/144)*

[185] *(Riedler, 2010, S. 280)*

Trifft also einer dieser drei Punkte auf den Irrtum zu, so besteht weiterhin die Möglichkeit des Irrenden auf Auflösung oder Anpassung des Vertrages. Unterliegt jedoch der Gegner des Irrenden dem gleichen Irrtum wie der Irrende, so bleibt sein Schutzbedürfnis bestehen und eine Anfechtung wird nicht möglich.

5.9.1.7 Wesentlichkeit des Irrtums

Ein Irrtum ist wesentlich, wenn das Geschäft ohne den Irrtum nicht geschlossen worden wäre. Dagegen ist ein Irrtum unwesentlich, wenn der Vertrag bei Kenntnis der wahren Sachlage auch, aber mit anderem Inhalt geschlossen worden wäre.[186]

Es ist von der Frage der Wesentlichkeit des Irrtums abhängig, ob dem Irrenden, falls die vorher genannten Bedingungen der Beachtlichkeit, Kausalität und dem fehlenden Vertrauensschutzbedürfnis des Gegners, zutreffen, ein Gestaltungsrecht zur Anfechtung[187] oder zur Anpassung[188] des Vertrages zukommt.

5.9.1.8 Anfechtung des Vertrages

Ist der Irrtum als wesentlich zu charakterisieren, dann erhält der Irrende das Gestaltungsrecht, den Vertrag anzufechten. Die Anfechtung hebt den Vertrag mit dinglicher ex-tunc-Wirkung auf.[189]

Aufhebung mit dinglicher Wirkung meint, dass die Aufhebung auch auf den sachenrechtlichen Teil zurückwirkt. Sollte also ein Ziel des Vertrages ein Übertrag des Eigentums einer Sache (eines „Dinges“, z.B. bei Kaufvertrag über ein Auto) gewesen sein, dann geht auch das Eigentum an der Sache an den vorigen Eigentümer zurück. Der Eigentumsübertrag wird rückwirkend ungültig, wie wenn der Vertrag nie geschlossen worden wäre. Dies ist auch die Bedeutung des Ausdruckes ex-tunc-Wirkung: die Aufhebung bewirkt, dass der Zustand vor dem Vertragsschluss eintritt, als wenn der Vertrag nie geschlossen worden wäre.

---

[186] *Wäre der Vertrag mit demselben Inhalt geschlossen, dann war der Irrtum nicht kausal*

[187] *Gemäß § 871 ABGB*

[188] *Gemäß § 872 ABGB*

[189] *(Riedler, 2010, S. 283)*

5.9.1.9 Anpassung des Vertrages

Sollte der Irrtum für beide Parteien unwesentlich, oder für den Irrenden zwar wesentlich, aber für dessen Vertragspartner unwesentlich gewesen sein, dann kann der Irrende auch eine Anpassung des Vertrages beanspruchen.

Dabei ist der tatsächliche Wille der Parteien maßgeblich. Es ist daher festzustellen, mit welchem Inhalt der Vertrag bei Kenntnis der wahren Sachlage geschlossen worden wäre. Für den Fall, dass der Vertragsschluss bei einem geminderten Preis zustande gekommen wäre, kommt folgende Berechnungsformel zur Anwendung:

$$geminderter\ Preis = \frac{vereinbarter\ Preis * Wert\ der\ mangelhaften\ Ware}{Wert\ der\ mangelfreien\ Ware} \quad 190$$

Sollte der Irrtum für beide Parteien als unwesentlich zu klassifizieren sein, dann kommt nur eine Anpassung in Frage, wenn sich die Parteien auf einen neuen Inhalt einigen können. Andernfalls kommt auch in diesem Fall nur eine Anfechtung und Aufhebung des Vertrages in Frage.

5.9.1.10 Schadenersatzpflicht

Wurde die irrende Partei fahrlässig in die Irre geführt, ein Anspruch des Irrenden auf Ersatz des Schadens. Ihm müssen alle Schäden ersetzt werden, die er nicht erlitten hätte, wenn er nicht auf die Gültigkeit der Erklärung vertraut hätte.[191]

5.9.2 List

List ist eine vorsätzliche, rechtswidrige Irreführung einer vertragsschließenden Partei durch die Gegenpartei oder durch jemanden, der dieser Gegenpartei zurechenbar ist.

Wird eine Partei vor oder bei dem Vertragsschluss listig in die Irre geführt, dann kommt trotzdem ein gültiger Vertrag zustande. Der getäuschten Partei steht aber das Gestaltungsrecht zu, den Vertrag wegen List anzufechten oder anzupassen.

---

[190] *(Riedler, 2010, S. 285)*

[191] *(Riedler, 2010, S. 287)*

Dazu § 870 ABGB:

„Wer von dem anderen Teile durch List [..][192] zu einem Vertrage veranlaßt worden, ist ihn zu halten nicht gebunden."

Obwohl § 870 explizit nur von Verträgen spricht, kommen analoge Regelungen auch für einseitig empfangsbedürftige Willenserklärungen zur Geltung, sodass auch Kündigungen oder Erklärungen zu einem Rücktritt angefochten werden können. Dies ist auch in § 876 verankert:

„Die vorstehenden Bestimmungen (§§ 869 bis 875) finden entsprechende Anwendung auf sonstige Willenserklärungen, welche einer anderen Person gegenüber abgegeben wurden."

Ähnlich wie beim Tatbestand des Irrtums gibt es auch hier mehrere Prüfschritte, mit denen festgestellt werden soll, ob der Tatbestand der List erfüllt ist.

5.9.2.1 Bestehen eines Irrtums beim Getäuschten

Die vertragsschließende Partei wird Vorspiegelung falscher oder Entstellung wahrer Tatsachen in einen Irrtum geführt oder durch Unterdrückung wahrer Tatsachen in ihrem Irrtum belassen oder bestärkt.[193] Dabei ist die Unterscheidung zwischen Geschäfts-, Erklärungs- oder Motivirrtum unerheblich, da bei List jede Art von Irrtum beachtlich ist.[194]

5.9.2.2 Kausalität der listigen Irreführung

Die listige Irreführung war kausal für den Vertragsabschluss, wenn der Vertrag vom Getäuschten ohne Vorliegen eines Irrtums nicht oder nicht in dieser konkreten Form geschlossen worden wäre. Damit wird auch festgelegt, dass die Irreführung vor oder bei dem Vertragsschluss vorliegen muss und nicht erst bei der Vertragserfüllung auftreten darf.

---

[192] Der Inhalt des ausgelassenen Teiles des §870 bezieht sich auf den Tatbestand der Drohung

[193] (Riedler, 2010, S. 290)

[194] Ausnahme: wird der Irrtum durch einen echten Dritten laut § 875 ABGB herbeigeführt, und die Täuschung dem Vertragspartner des Getäuschten nicht bekannt war, dann ist der Motivirrtum unbeachtlich.

5.9.2.3 Rechtswidrigkeit der Irreführung

Man unterscheidet bei den Handlungen, die zum Irrtum führen zwischen aktivem Tun und passivem Unterlassen:

1. Irrtumserregung durch Tun: dies stellt dann eine rechtswidrige Handlung dar, wenn sich die handelnde Person objektiv sorgfaltswidrig verhalten hat, und nicht, wie sich ein ordnungsgemäßer, rechtstreuer Mensch verhalten hätte.
   Beispiel: Bietet ein Händler seine Ware über dem vom Hersteller unverbindlich empfohlenen Richtpreis als „Sonderangebot" an dann liegt eine rechtswidrig irreführende Handlung vor.[195]

2. Irrtumserregung durch Unterlassen: dies stellt eine rechtswidrige Irreführung dann dar, wenn der Irreführende die Aufklärungspflichten verletzt hat. Die Aufklärungspflichten ergeben sich aus dem Gesetz, dem Vertrag oder der Übung des redlichen Verkehrs.

5.9.2.4 Vorsatz des Täuschenden

Vorsatz des Täuschenden liegt vor, wenn er den Getäuschten *wissentlich* und *willentlich* überlistet hat.
Die wissentliche Täuschung kann einerseits dadurch erfolgen, dass der Täuschende die Kenntnis von der Unrichtigkeit der Umstände hat, oder andererseits dadurch, dass er die Richtigkeit der Umstände gegenüber dem Getäuschten versichert, obwohl der Täuschende dies nicht zweifelsfrei weiß.
Die willentliche Täuschung liegt vor, wenn der Täuschende die Irreführung des Getäuschten beabsichtigt hat.

5.9.2.5 Täuschung durch den Vertragspartner

Eine notwendige Voraussetzung für das Erlangen eines Gestaltungsrechtes (auf Vertragsauflösung oder Vertragsanpassung) ist, dass die Täuschung durch den jeweiligen Vertragspartner (oder einer ihm zuzuordnenden dritten Person)[196] erfolgt ist.

---

[195] *(Riedler, 2010, S. 292)*

[196] *z.B. eine Person, die den Auftrag zur Täuschung erhält*

Dieses Gestaltungsrecht ist aber auch erlangbar, wenn die Täuschung durch eine dritte Person erfolgt ist, die dem Vertragspartner nicht zuzuordnen ist,[197] und

- Der Vertragspartner des Getäuschten an der Täuschungshandlung des Dritten mitgewirkt hat, oder
- der Vertragspartner von der Täuschungshandlung des Dritten wissen musste, oder
- die Täuschung dem Vertragspartner gegenüber rechtzeitig aufgeklärt worden ist. [198]

5.9.2.6 Anfechtung oder Anpassung des Vertrages

Grundsätzlich ist eine Willenserklärung, auch dann gültig, wenn sie unter dem Einfluss einer Täuschung entstanden ist, und der Vertrag ist demnach auch gültig. Ergibt eine Analyse der Vertragsschlusshandlungen, dass die oben in den Abschnitten 5.9.2.1 bis 5.9.2.5 aufgezählten Punkte zutreffen, dann kommt dem Getäuschten das Gestaltungsrecht der Vertragsanfechtung zu. Die Anfechtung beseitigt den Vertrag mit dinglicher ex-tunc-Wirkung. [199]

Der Getäuschte hat auch die Möglichkeit, eine Vertragsanpassung nach § 872 ABGB vorzunehmen, wenn er der Vertrag auch ohne Täuschung, aber mit anderem Inhalt abgeschlossen hätte.

Auffallend ist dabei die nachteilige Stellung des Täuschenden: Durch das eingeräumte Gestaltungsrecht kann der Getäuschte den Vertrag nach seinem Gutdünken anpassen, ohne dass dem Täuschenden ein Mitspracherecht zukäme. Der Täuschende kann der Anpassung nur insoweit widersprechen, als durch die Anpassung sonst sachlich gerechtfertigte, wesentliche Interessen auf seiner Seite beeinträchtigt würden. [200]

---

[197] *Man spricht vom* „echten Dritten“

[198] *(Riedler, 2010, S. 295)*

[199] *Siehe 5.9.1.8*

[200] *(Riedler, 2010, S. 296)*

Ein Verzicht auf das Recht auf Anfechtung oder Anpassung wird dem Getäuschten nicht zugesprochen, da ein derartiger Verzicht gegen die guten Sitten verstoßen würde. [201]

Dieses Recht auf Anfechtung oder Anpassung verjährt nach 30 Jahren,[202] innerhalb dieser Zeitspanne kann es gerichtlich geltend gemacht werden. [203]

5.9.3 Drohung

Vergleichbar mit den im Falle einer listigen Täuschung in Gange gebrachten Mechanismen sind auch die, die im Falle einer Drohung eingesetzten Analysetechniken.

Maßgeblich wird wie schon im Fall der List der § 870 ABGB:

„Wer von einem anderen Teile durch List oder durch ungerechte gegründete Furcht zu einem Vertrage veranlaßt worden, ist ihn zu halten nicht verbunden.“

Wenn also eine Vertragspartei vor oder bei Abgabe seiner Erklärung bedroht wurde, dem kommt ein Gestaltungsrecht zur Auflösung oder Anpassung des Vertrages (der wiederum gültig geschlossen wurde) zu.

Vergleichbar mit der Vorgehensweise bei listiger Täuschung wird auch hier in mehreren Stufen festgestellt, ob eine Drohung vorliegt, sie kausal für den Vertragsschluss war, durch wen sie ausgesprochen wurde, ob eine Furcht bestanden hat und ob die Drohung dadurch rechtswidrig wurde.

Detaillierter soll an dieser Stelle darauf allerdings nicht eingegangen werden.

---

[201] *§ 879 ABGB*

[202] *§ 1478 ABGB*

[203] *Interessant ist dabei die juristische Denkweise: Ein Getäuschter kann zwar nicht auf sein Gestaltungsrecht verzichten, aber er kann solange darauf verzichten, es auszuüben, bis es verjährt ist.*

5.10 Verbraucherverträge

Einen Spezialfall des Vertrages stellt der sogenannte Verbrauchervertrag dar. Verbraucherverträge sind Rechtsgeschäfte zwischen einem Unternehmer gemäß §1 UGB[204] und einem Vertragspartner, der nicht unter die Definition des §1 UGB fällt und entsprechend als Verbraucher bezeichnet wird. Der §1 UGB definiert sowohl den Begriff des Unternehmers als auch den des Unternehmens:

„Ein Unternehmer ist, wer ein Unternehmen betreibt." [205]

und

„Ein Unternehmen ist jede auf Dauer angelegte Organisation selbständiger wirtschaftlicher Tätigkeit, mag sie auch nicht auf Gewinn gerichtet sein." [206]

Vergleichbare Formulierungen finden sich auch im ersten Abschnitt des Konsumentenschutzgesetzes, das dem Verbraucher maßgebliche Rechte als Partei im Verbrauchervertrag einräumt.[207]

Gemäß §2 UGB sind auch *„Aktiengesellschaften, Gesellschaften mit beschränkter Haftung, Erwerbs- und Wirtschaftsgenossenschaften, Versicherungsvereine auf Gegenseitigkeit, Sparkassen, Europäische wirtschaftliche Interessensvereinigungen, Europäische Gesellschaften und Europäische Genossenschaften"* Unternehmer.

Damit ein Verbrauchervertrag entsteht, muss allerdings §1 UGB (oder §2 UGB) zur Anwendung kommen, der Unternehmer muss also als solcher im Rahmen seiner Geschäftstätigkeit auftreten und nicht als Privatperson, die beispielsweise von einer anderen Privatperson Gebrauchtwaren ersteigert.

Bei Verbraucherverträgen findet besonders das erste Hauptstück des Konsumentenschutzgesetzes[208] Anwendung. Diese verdrängen als

---

[204] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Unternehmensgesetzbuch, Fassung vom 13.09.2017)*

[205] *§1 Abs 1 UGB*

[206] *§1 Abs 2 UGB*

[207] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Konsumentenschutzgesetz, Fassung vom 13.09.2017)*

speziellere Norm auch Parallelbestimmungen des ABGB. Das Konsumentenschutzgesetz enthält wesentliche Regelungen zum Schutz des Verbrauchers.

Nach §3 KSchG hat die Verbraucherin eine Frist von einer Woche zum Rücktritt vom Vertrag, so dieser nicht innerhalb der Geschäftsräume des Unternehmens, auf Messen oder Marktständen geschlossen wurde. Gleiches gilt für Geschäftsabschlüsse auf Werbefahrten, Ausflugsfahrten und Ähnlichem.
Allerdings wird dieses Rücktrittsrecht nicht wirksam, wenn die Verbraucherin die geschäftliche Verbindung mit dem Unternehmer selbst angebahnt hat, dem Vertragsschluss keine Besprechungen zwischen den am Geschäft Beteiligten vorangegangen sind, oder bei Verträgen, die außerhalb der Geschäftsräume geschlossen wurden, wenn die Leistungen sofort zu erbringen waren und das Entgelt 25 Euro nicht übersteigt.[209]

Weitere Aspekte des KSchG finden sich im Kapitel über Fernabsatz.[210]

---

[208] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Konsumentenschutzgesetz, Fassung vom 13.09.2017)*

[209] *Wird das Unternehmen seiner Natur nach ohne Geschäftsrum betrieben, dann darf das Entgelt bis zu 50 Euro betragen.*

[210] *5.11*

5.11 Fernabsatz[211]

Ausgangspunkt für die den Fernabsatz betreffenden Rechtsvorschriften ist die Fernabsatzrichtlinie[212] der Europäischen Union, deren Umsetzung in Österreich mit dem 1.1.2001 in Kraft trat. Die Umsetzung umfasste Änderungen im Konsumentenschutzgesetz, im Bundesgesetz gegen unlauteren Wettbewerb und Produkthaftungsgesetz.

Im Konsumentenschutzgesetz wurden die §§ 5a bis 5j samt Überschrift eingefügt:[213]

„Vertragsabschlüsse im Fernabsatz“

Die §§ 5a und 5b regeln die Anwendungsbereiche des Gesetzesabschnittes. Demnach gelten die §§ 5c bis 5i für Verträge, die unter ausschließlicher Verwendung eines oder mehrerer Fernkommunikationsmittel geschlossen werden, sofern sich der Unternehmer eines für den Fernabsatz organisierten Vertriebs- oder Dienstleistungssystems bedient.[214]

Dabei meint der Begriff *Fernkommunikationsmittel* die Kommunikationsmittel, die zum Abschluss eines Vertrages ohne gleichzeitige körperliche Anwesenheit der Parteien verwendet werden können. Beispiele dafür sind neben Katalogen und Pressewerbungen auch alle Arten von elektronischen Kommunikationsmittel: Ferngespräche mit Personen oder Automaten, Bildtelefon, Teleshopping oder elektronische Post.[215]

Nicht anzuwenden sind §§ 5c bis 5i auf Verträge über Finanzdienstleistungen (Wertpapierdienstleistungen, Versicherungen, Bankdienstleistungen, Dienstleistungen im Zusammenhang mit Termin- und Optionsgeschäften), den Bau und Verkauf von Immobilien, Verträgen unter Verwendung von Warenautomaten oder in automatisierten Verkaufsräumen und Versteigerungen.[216]

---

[211] *(Riedler, 2010, S. 155)*

[212] *Richtlinie 97/7/EG über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz*

[213] *(Fernabsatz-Gesetz)*

[214] *§ 5a Abs 1 KSchG*

[215] *§ 5a Abs 2 KSchG*

[216] *§ 5b KSchG*

In § 5c werden die Informationen aufgezählt die dem Konsumenten zur Verfügung gestellt werden müssen. Dazu gehören auch die Information über das Bestehen eines Rücktrittsrechtes. Diese Informationen müssen dem Konsumenten klar und verständlich in einer dem verwendeten Kommunikationsmittel angepassten Art und Weise übermittelt werden.
Davon ausgenommen sind allerdings regelmäßige Hauslieferungen und Dienstleistungen in den Bereichen Unterbringung, Beförderung, Lieferung von Speisen und Getränken, wenn sich der Unternehmer zu einer Lieferung zu einer festgelegten Zeit verpflichtet.[217]
Ein Teil der angeführten Informationen sind dem Verbraucher auch schriftlich oder auf einem für ihn verfügbaren Datenträger zu übermitteln.[218]

Gemäß § 5e KSchG kann der Verbraucher von einem im Fernabsatz geschlossenen Vertrag bis zum Ablauf einer im KSchG definierten Frist von sieben Tagen[219] zurücktreten. Dabei ist das Absenden einer Rücktrittserklärung innerhalb dieser Frist ausreichend.

Der § 5f beschreibt die Ausnahmen vom Rücktrittsrecht, die beispielsweise bei Waren, die direkt nach Kundenspezifikationen hergestellt wurden, Audio-, Videoaufzeichnungen und Software, sofern das Siegel gebrochen wurde, Wett- und Lotteriedienstleistungen und Hauslieferungen oder Freizeit-Dienstleistungen.

Die Folgeparagraphen (§ 5g - 5j) befassen sich mit dem Modus des Rücktritts, Lieferfristen, und Bindungen im Fall von Gewinnzusagen, und werden hier nicht weiter behandelt.

---

[217] § 5c Abs 4 KSchG

[218] § 5d Abs 2 KSchG

[219] Hier zählt der Samstag nicht als Werktag

5.12 E-Commerce[220]

Das E-Commerce-Gesetz (ECG) ist die Umsetzung der e-Commerce-Richtlinie der Europäischen Union vom 8.6.2000[221] und ist mit 1.1.2002 in Kraft getreten.

Die §§ 9 – 12 ECG im 4. Abschnitt enthalten Sondervorschriften über Informationspflichten eines Dienstanbieters, die Abgabe einer Vertragserklärung, Vertragsbestimmungen und Geschäftsbedingungen und den Zugang elektronischer Erklärungen.[222]

Dem Benutzer sind angemessene technische Mittel zur Verfügung zu stellen, mit denen dieser Eingabefehler vor Abgabe seiner Willenserklärung erkennen und korrigieren kann. Ihm ist der Zugang seiner elektronischen Vertragserklärung unverzüglich zu bestätigen. Der Bestätigung gilt (ebenso wie die Vertragserklärung) als zugegangen, wenn sie unter gewöhnlichen Umständen abgerufen werden können. Diese Verpflichtungen fallen unter zwingendes Recht, können also nicht abbedungen[223] werden.

---

[220] *(Riedler, 2010, S. 157)*

[221] *EC-RL, Richtlinie 2000/32/EG*

[222] *(Riedler, 2010, S. 157)*

[223] *Durch Zahlung eines Geldbetrags außer Kraft gesetzt werden*

5.13 Zusammenfassung

Ein großer Teil des österreichischen Privatrechtes beschäftigt sich mit verschiedenen Aspekten rund um Verträge. Es beschreibt das Zustandekommen eines Vertrages durch übereinstimmende Willenserklärungen, die den Wunsch, eine rechtlich belastbare Bindung einzugehen und dies dem Adressaten der Erklärung auch kundtun zu wollen, enthalten.

Eine Voraussetzung dafür, dass eine Person überhaupt einen Vertrag eingehen darf, ist ihre Geschäftsfähigkeit. Diese ist sowohl vom Alter der Person als auch von ihrer mentalen Tauglichkeit abhängig.

Die Gültigkeit des Vertrages hängt aber an weiteren Bedingungen. So ist der innere Wille der Vertragspartner zu erforschen, und mit dem objektiven Erklärungswert ihrer Willenserklärungen abzustimmen. Besteht der begründete Verdacht, das trotz offensichtlicher Bindungswünsche in der Willenserklärung der innere Wille einer oder beider Parteien dem Wunsch, einen Vertrag zu den vereinbarten Bedingungen oder überhaupt abzuschließen, widerspricht, dann kommt unter Umständen auch kein Vertrag zustande.

Auch wenn ein Vertrag gültig geschlossen wurde, kann es sein, dass eine Vertragspartei, wenn sie geirrt hat oder getäuscht wurde, die Möglichkeit erhält, den Vertag abzuändern oder ganz aufzulösen.

Zu überprüfen bleibt außerdem noch, ob Vereinbarungen getroffen wurden, die den gesetzlichen Grundlagen des Verbraucherschutzes und dem Schutz vor gesetzes- oder sittenwidrigen Vertragsklauseln widersprechen, und somit ungültig werden.

Diese Vorschriften in ihrer gesamten Breite müssen auch für auf elektronischem Weg über Fernkommunikationsmittel geschlossene Verträge gelten. Damit müssen sie auch Gültigkeit für jedes rechtliche Gebilde haben, sobald es sich als Vertrag bezeichnen möchte oder als solcher wirken möchte.

6 Analyse

6.1 Aspekte des Vertragscodes

In einfacher Beschreibung ist ein Smart Contract eine Software, die eine Abfolge von Prozessschritten automatisch ausführt, sobald gewisse vorgegebene Voraussetzungen erfüllt sind. Diese Voraussetzungen beinhalten auch eine Bereitschaft und übereinstimmende Zielsetzung externer Akteure, seien sie natürliche oder juristische Personen oder andere vorgeschaltete Netzwerkknoten. Dabei erzeugt oder verändert diese Software Daten, die in der Blockchain abgelegt sind oder dort abgelegt werden.

Diese übereinstimmende Zielsetzung und die Bereitschaft, diese Ziele zu umzusetzen, lassen sich in Juristensprache auch als übereinstimmende Willenserklärungen interpretieren. Diese übereinstimmenden Willenserklärungen rücken dieses Softwarekonstrukt in die Nähe eines Vertrages. In anderen Worten sind Smart Contracts eine Abfolge von Handlungsanordnungen, die diese Vertragsbestimmungen durch den Code der Software abbilden.[224]

Als Beispiel kann man sich eine Fluglinie vorstellen, die ihren Kunden einen Smart Contract anbietet, der im Fall einer Verspätung oder eines Ausfalles automatisch eine Entschädigung ausbezahlt.[225] Im globalen Wettbewerb der Fluglinien um Fluggäste kann daraus ein gewinnbringender Wettbewerbsvorteil entstehen.

Es drängt sich die Frage auf, wie damit umgegangen werden soll, falls Fluggast und Fluglinie über die Dauer der Verspätung geteilter Meinung sind oder die Verspätung nach Meinung der Fluglinie unvermeidbar war. Hier könnten zusätzliche Mechanismen implementiert werden, um auf diese Arten von Leistungsstörungen entsprechend zu reagieren.

Die wichtigere Frage ist: hat man es in diesem Fall schon mit einem Vertrag zu tun?

---

[224] *(Buchleitner & Rabl, 2017, S. 6)*

[225] *(Blocher, 2016, S. 618)*

6.1.1 The Code is the Law ?

Gerne wird der Satz „The code is the law“ zitiert [226]. Damit will man suggerieren, dass der Smart Contract, wenn er nur smart genug aufgesetzt worden ist, er hinreichend als Vertragstext tauglich ist. Mit den propagierten Eigenschaften der Unanhaltbarkeit, Unveränderlichkeit und Unwiderlegbarkeit würden Anwälte und Gerichte von selbst arbeitslos werden, da es ja in solchen Verträgen nichts mehr nachzuverhandeln gäbe.

Als es allerdings im Juni 2016 aufgrund eines Fehlers im Code der auf der Ethereum-Plattform laufenden Applikation „The DAO“ zu einem virtuellem Einbruch kam, der einen Schaden in der Größenordnung von 50 Millionen $ verursachte, entschloss sich das Entwicklerteam zu einem Relaunch mit korrigiertem Code.

Nach einer Abstimmung unter den Teilnehmern wurde dieser Plan in die Tat umgesetzt, woraufhin einer der Mitgründer der DAO-Anwendung sich zu der Aussage hinreißen ließ: *„Wir haben unseren obersten Gerichtshof gefunden – die Community.“*[227]

In einer innovativen IT-Kultur, die weitgehend amerikanisch dominiert ist, kann diese Sichtweise teilweise durch das Amerikanische Vertragsrecht erklärt werden. So beschreibt Dolinar[228] die Grundhaltung des amerikanischen Rechtssystems folgendermaßen:

*The dominant position in American law is the so-called “*objective theory*”. This means that one has to look at the external manifestations made by each of the parties rather than to their subjective intentions.*

(Die dominierende Stellung im amerikanischen Recht ist die sogenannte „objektive Theorie". Das bedeutet, dass man die äußeren Manifestationen der einzelnen Parteien und nicht ihre subjektiven Intentionen betrachten muss.)[229]

Beispielgebend dafür ist der Fall Lucy vs. Zehmer[230], der als Lehrstück für Studentinnen und Studenten der Rechtswissenschaften an amerikanischen Universitäten im ersten Jahr dient. Dieser Rechtsstreit beschäftigt sich mit

---

[226] *z.B. (Lessig, 2000)*

[227] *(Kaulartz & Heckmann, 2016)*

[228] *(Dolinar, 2010, S. 142)*

[229] *Übersetzung unter Zuhilfenahme von https://www.deepl.com/translator*

[230] *196 Va 493, 84 S.E.2d 516 (1954)*

Spaßerklärungen, und wie weit die Vertragspartner auf den Inhalt der Erklärung, die unter Alkoholeinfluss abgegeben wurde, vertrauen darf.

Der Fall behandelt den Verkauf von Zehmers Farm an O.W.Lucy zum Preis von 50.000 $. Nach Konsum von Unmengen an Alkohol wurde der Verkauf schriftlich festgehalten und von Zehmers Frau bezeugt. Am nächsten Tag beteuerten sowohl Zehmer als auch seine Frau, die Erklärung im Spaß abgegeben zu haben und verlangten die Anullierung des Vertrages.

Das oberste Berufungsgericht des Staates Virginia entschied pro Lucy,
Es berief sich dabei auch auf den Fall First Nat. Bank v. Roanoke Oil Co.[231] :

In the field of contracts, as generally elsewhere, „We must look to the outward expression of a person as manifesting his intention rather than to his secret and unexpressed intention. The law imputes to a person an intention corresponding to the reasonable meaning of his words and acts.

(Im Bereich der Verträge, wie allgemein andernorts auch, müssen wir *das Ausgesprochene* eines Menschen als Manifestation seiner Intention betrachten, nicht seine geheime und unausgesprochene Intention. Das Gesetz unterstellt einer Person eine Absicht, die der vernünftigen Bedeutung ihrer Worte und Handlungen entspricht.)[232]

Die beiden englischsprachigen Zitate bringen zum Ausdruck, dass die Bedeutung einer Erklärung stärker von ihrem objektiven Erklärungswert abhängt als von der inneren nicht zum Ausdruck gebrachten Absicht.
Dies steht im Gegensatz zur Sichtweise, die auch das österreichische Zivilrecht vertritt, in der der innere Wille einer Erklärung stärker wirkt als der objektive Erklärungswert.

Fraglich bleibt, ob im angloamerikanischen Rechtsraum ein Smart Contract allein durch seine Verschriftlichung schon als Vertrag angesehen werden kann.

6.1.2 Der Code als Vertragsformblatt ?

Vertragsparteien steht es grundsätzlich frei, ihre Vereinbarungen auch in Form einer Programmiersprache schriftlich festzuhalten. Dies fällt umso

---

[231] *169 Va 99, 114, 192 S.E. 764, 770*

[232] *Übersetzung unter Zuhilfenahme von https://www.deepl.com/translator*

leichter, je klarer sie sich auf die Sprache und die darin verwendeten Elemente (die Softwarearchitektur) einigen können. In der Praxis wird es – vor allem im Massenmarkt auf absehbare Zeit wohl kaum genügend gut ausgebildete Menschen geben, die einen Vertragsquelltext lesen, verstehen und interpretieren können. Daher entsteht das Problem: Der Nutzer muss sich an einen für ihn nicht verständlichen Text binden, so er an der Dienstleistung Nutzen ziehen möchte.

Verstärkt wird diese Problematik durch die Tatsache, dass die Blockchain systemimmanent verteilt auf idealerweise allen Endgeräten parallel läuft. Jedes Endgerät hat also eine Kopie des Codes gespeichert und hat diese auch in Betrieb.

Fasst man den Code als den Vertragstext auf, dann entsteht durch die vielfache Verteilung des Codes eine Situation, wie sie von einem Vertragsformblatt bekannt ist.[233] Ein Anbieter verteilt an jeden seiner Kunden einen vorgefertigten Vertrag, der in einer Programmiersprache geschrieben ist. Ob jeder Kunde den Vertragstext verstehen kann, muss in Zweifel gezogen werden.

Nun ist aber gemäß §6 Abs 3 KSchG eine in AGB oder Vertragsformblättern enthaltene Vertragsbestimmung unwirksam, wenn sie unklar formuliert ist. [234] diese Rechtsvorschrift ist allerdings nur für Verbraucherverträge, also für Verträge zwischen einem Unternehmer und einem Verbraucher gültig.

Unternehmer ist laut §1 UGB jemand, der eine regelmäßige selbständige wirtschaftliche Tätigkeit ausübt, auch wenn sie nicht auf Gewinn ausgerichtet ist. Ein Anbieter von Diensten für einen potentiellen Weltmarkt (sofern es sich um eine öffentliche Blockchain als Basis für den Dienst handelt) muss also als Unternehmer im Sinn des KSchG gesehen werden. Damit wird der §6 des KSchG schlagend, woraus man wiederum für eine große Anzahl von smarten Contracts schließen muss:

Wenn der Code als der Vertrag gesehen wird, dann ist er unwirksam! Wenn man also nicht akzeptieren will, dass sich eine große Menge an Anbietern und Verbrauchern im vertragsfreien Raum bewegen, dann folgt daraus: Der Code kann nicht der Vertrag sein.

---

[233] Im deutschen Bürgerlichen Gesetzbuch (BGB) findet sich Vergleichbares: siehe (Heckmann & Kaulartz, 2016, S. 139)

[234] Genaueres in Kap. 5.10

6.1.3 Der Code als Verkaufsautomat

Stellt man sich einen Kaffeeautomaten in einem Stockwerk einer Firma vor, der den bevorzugten Kaffee jeder in dem Stockwerk arbeitenden Person kennt, und durch Sensoren erkennt, wenn sich die jeweilige Person der Kaffeeküche nähert und dann automatisch den programmierten Kaffee zubereitet und die Kosten danach automatisch vom Gehaltskonto der Person abbucht.

Für diese Funktionen wird keine Blockchain benötigt, trotzdem ist der Code, der in diesem Automaten läuft, als Smart Contract interpretierbar. Der Automat verfügt über ein „oracle", also eine Schnittstelle, die auf externe Signale (die Person, die sich der Kaffeeküche nähert) reagiert und entsprechend Prozessschritte einleitet, die dann zum Verkauf eines Bechers Kaffee gegen den vorher abgestimmten Geldbetrag als Entgelt führt. Angebot und Annahme als übereinstimmende Willenserklärungen müssen zum Zeitpunkt der Registrierung und Freischaltung des Kontos für die Abbuchung des Kaffeepreises in Einklang gebracht werden. Der Handel wird durch Betreten der Kaffeeküche als Willensbetätigung ausgelöst.

Der Code kann also in einigen Fällen als Teil des Verkaufsautomaten gesehen werden, und ist in der beschriebenen Form noch nicht besonders „smart". Denkbar sind aber auch komplexere Szenarien, die die Möglichkeit der Rückabwicklung einbeziehen, für den Fall dass beispielsweise Milch aus ist und der Kaffee deshalb nicht den Qualitätsvorstellungen des Kunden entspricht. Mit der einprogrammierten Möglichkeit der „automatischen Anfechtung" des geschlossenen Vertrages wegen Leistungsstörung erfüllt der Smart Contract zumindest das Versprechen, sich diverse Arten eines Rechtsstreites durch die Automatik einzusparen.

Allerdings ist der Code für sich genommen aufgrund mangelnder Hardware gewiss kein solcher Verkaufsautomat. In dem beschriebenen Fall ist der Code ein Mittel der Vertragserfüllung und der Leistungsausführung.[235]

6.1.4 Elektronische Verträge laut ECG

Verträge, die mithilfe von elektronischen Hilfsmitteln wie der Blockchain oder auf einer Blockchain-Plattform laufenden Programmcodes geschlossen werden, werden in den meisten Fällen als elektronische Verträge betrachtet werden müssen, insbesondere dann, wenn ein Geschäftsabschluss ohne

[235] *(Heckmann & Kaulartz, 2016, S. 140)*

Verhandlung in einem Geschäftslokal sondern rein im „virtuellen Raum“ erreicht wird. Somit fallen diese Verträge unter das E-Commerce-Gesetz (ECG).[236]

Gemäß E-Commerce-Gesetz haben Diensteanbieter umfangreichen Informationspflichten über Rücktrittsmöglichkeiten vom Vertragsschluss nachzukommen. Die Einhaltung dieser Informationspflichten ist entscheidend für das gültige Zustandekommen des Vertrages. Unklar ist allerdings, wer in einem peer-to-peer-Netzwerk ohne zentrale Dienstleistungsinstanz überhaupt als Diensteanbieter gesehen werden kann.[237] Hier wird in gewissen Fällen sogar eine Nachschärfung durch die Gesetzgebung notwendig werden.

[236] *(Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für E-Commerce-Gesetz)*

[237] *(Buchleitner & Rabl, 2017, S. 12)*

6.2 Mögliche Gründe für die Ungültigkeit des Smart Contract

6.2.1 Mündigkeit

Es ist grundsätzlich einfach, sich auf seinem Mobiltelefon oder Tablet die nötige Software zu installieren um in die Welt der Smart Contracts einzutreten. Ebenso einfach dürfte es in vielen Fällen sein, sein Wallet zu füllen und damit am kommerziellen Geschäftsleben teilzunehmen.

Allerdings gestattet das österreichische Privatrecht Personen unter 18 Jahren nur unter gewissen Voraussetzungen die Teilnahme am Geschäftsleben.[238] Fraglich ist, ob diese Schranken als Hinderungsgrund in den Smart Contract eingebaut werden, zumal das Coding mit einer hohen Wahrscheinlichkeit nicht in Österreich erfolgen wird.

Das österreichische Recht sieht jedoch als Sicherheitsnetz vor, von Minderjährigen abgeschlossene Verträge nicht als gültig anzuerkennen. Die technische Auflösung und Rückabwicklung der Verträge muss naturgemäß die Angelegenheit des internationalen Rechts werden.

6.2.2 Benachteiligende Bestandteile im Vertrag

Benachteiligende Klauseln in Vertragsformblättern werden in den § 864a ABGB[239] , § 879 Abs 3 ABGB[240] und im § 6 KSchG[241] behandelt. Allen drei Normen ist gemeinsam, dass ein Zutreffen den Vertragsteil für ungültig erklärt.

Würde in einem smarten Versicherungsvertrag Auszahlungen nur unter bestimmten unüblichen Bedingungen erfolgen, die für den Versicherungsnehmer benachteiligend wirken, dann stellt sich wiederum die Frage der Rückabwicklung oder Nachbesserung des Vertrages.

---

[238] *Siehe Kap. 5.5.1*

[239] *Siehe Kap. 5.6.2, Geltungskontrolle*

[240] *Siehe Kap. 5.6.3.1, Generalnorm der Inhaltskontrolle*

[241] *Siehe Kap. 5.6.3.2, Spezialnorm der Inhaltskontrolle*

6.2.3 Verletzung der Informationspflichten

Informationspflichten, die Unternehmer gegenüber Verbrauchern zu leisten haben, werden im § 5c KSchG aufgezählt. Werden diese Informationspflichten vernachlässigt, dann steht dem Konsumenten nach § 5d Abs 3 KSchG eine auf drei Monate verlängerte Rücktrittsfrist vom Vertrag zu. Grundsätzlich ist der Vertrag aber weiterhin gültig.

6.2.4 Unklare Formulierungen

Dieser Fall wurde im Kapitel 6.1.2 für Verbraucherverträge beschrieben. Demnach ist gemäß §6 Abs 3 KSchG eine in den AGB oder Vertragsformblättern enthaltene Vertragsbestimmung unwirksam, wenn sie unklar formuliert ist, was für einen codierten Vertrag zutreffen dürfte.

6.3 Rücktritt vom Vertrag und Vertragsauflösung

6.3.1 Rücktritt

Was bedeutet Rücktritt von einem Vertrag für die Einträge einer unveränderlichen Blockchain? Mit einer Rücknahme der Dienstleistung und Rücküberweisung der Gegenleistung, sofern diese Schritte technisch (und physikalisch: z.B. Rücksendung einer Ware) durchführbar sind, sollte dem Anspruch des Rücktrittes genüge getan sein.

6.3.2 Anfechtung

Wie ist allerdings ein Vertrag zu sehen, der aufgrund einer der in Kapitel 5.9 beschriebenen Störungen angefochten wird? Nutzt man sein Gestaltungsrecht mit dem Zweck der Vertragsauflösung, will man den Zustand vor dem Vertragsschluss erreichen. Der Vertrag soll also nicht mehr existieren.

Dabei stellt sich die Frage, wie ein vertragsloser Zustand erreicht wird, wenn dieser Vertrag schon unlöschbar in der Blockchain verankert wurde. Ob der Eintrag einer „Gegendarstellung“ in die Blockchain reicht, wird wohl umfassend diskutiert und vielleicht auch gesetzlich verankert werden müssen.

6.3.3 Nichtiger Vertrag

Ein absolut nichtiger Vertrag gilt als nicht geschlossen, und erwirkt auch keine Rechtskraft. Es wurde niemand zur Leistung einer Folgehandlung verpflichtet. Daher kann dieses Rechtsgeschäft auch nicht angefochten werden, es ist nicht existent.

Unklar bleibt auch in diesem Fall, wie eine Rücksetzung in den Stand vor dem Vertragsschluss zu erfolgen hat, da der Vertragsschluss ja schon in der Blockchain unveränderlich gespeichert wurde und kaum mehr als nicht existent betrachtet werden kann. Hier könnte es notwendig werden dass die Gesetzgebung oder die Rechtsprechung verbindliche Regeln einführen.

6.4 Schlussfolgerung

Grundsätzlich kann durch den übereinstimmenden Willen zweier Partner im peer-to-peer-Verband ein rechtsgültiger Vertrag zustande kommen. Dabei ist aber der Code des Smart Contract nicht als der Vertragstext zu lesen. Der Smart Contract ist kein Vertrag im Rechtssinne.[242] Den Inhalt des Vertrages bestimmen vielmehr die vor der automatischen Abwicklung implizit abgestimmten Mindestinhalte.

Problematisch ist die Rechtsgültigkeit des Vertrages immer dann zu sehen, wenn besondere Informationspflichten nicht eingehalten werden. Wie im Fall zu verfahren ist, in dem der offensichtlich ungültige, trotzdem unanhaltbar automatisch laufende Vertrag an der Ausführung gehindert werden kann, ohne alle anderen parallel in der Blockchain laufenden Smart Contracts negativ zu beeinflussen, ist noch unklar.

Ebenso unklar ist das Verfahren, nach dem ungültige oder angefochtene Verträge aus dem System entfernt werden können, um die Vertragspartner in den vorigen Stand zu setzen, zumal eine Grundeigenschaft der Blockchain die ist, nichts zu vergessen. (Unwiderlegbarkeit der Daten[243]).

Und ebenso ist unklar, wie auf gesetzlich vorgeschriebene Rücktrittsrechte von Konsumenten eingegangen werden soll. Hier kann die Leistungsphase erst dann beginnen, wenn die Rücktrittsfristen verstrichen sind. Dies widerspricht aber dem Grundgedanken des E-Commerce, eine erworbene Ware in seiner Anwendungsumgebung (beim Kunden zu Hause) zu testen, da man sich nicht in den Verkaufsräumen mit der Funktionalität befassen kann.

Es bleibt abzuwarten, wie schnell und wie weit sich die neue Technologie des Smart Contract ausbreiten wird. Es ist allerdings davon auszugehen, dass in einigen der angesprochenen Bereiche, insbesondere im Konsumentenschutz, bei Vertragsrücktritten und Anfechtungen der Gesetzgeber Regelungen finden muss, um Technologie und Recht zueinander zu führen.

---

[242] *(Heckmann & Kaulartz, 2016, S. 140)*

[243] *Vergleiche dazu Abschnitt 3.3.6*

7 Verzeichnis der Abbildungen

8 Literaturverzeichnis

Anderson, R. (2008). *Security Engineering.* Wiley.

Aschwanden, E. (10. 05 2016). *Stadt Zug wird weltweit zum Bitcoin-Pionier*. Abgerufen am 15. 10 2017 von Neue Zürcher Zeitung AG: https://www.nzz.ch/schweiz/crypto-valley-zukunftsmodell-oder-marketing-gag-ld.22911

Back, A. (01. 08 2002). *Hashcash - a denial of service counter-measure.* Abgerufen am 30. 09 2017 von http://www.hashcash.org/papers/hashcash.pdf

Bitcoin Wiki. (14. 04 2010). Abgerufen am 28. 09 2017 von https://en.bitcoin.it/wiki/Main_Page

bitcoin.stackexchange.com. (kein Datum). Abgerufen am 05. 10 2017 von https://bitcoin.stackexchange.com/questions/4301/what-is-an-unspent-output: https://bitcoin.stackexchange.com/questions/4301/what-is-an-unspent-output2017

Blocher, W. (2016). The next big thing: Blockchain - Bitcoin - Smart Contracts. *Anwaltsblätter 8+9/2016*, (S. 612-618).

Blockchain overall size. (kein Datum). Abgerufen am 30. 10 2017 von Blockchain.info: https://blockchain.info/de/charts/blocks-size

Brandau, C. (10. 01 2017). *Schwedisches Grundbuchamt wird Blockchain Testphase einleiten*. Abgerufen am 15. 10 2017 von Coinwelt: http://coinwelt.de/2017/01/schwedisches-grundbuchamt-wird-blockchain-testphase-im-maerz-einleiten/

Brooklyn Microgrid 101. (kein Datum). Abgerufen am 15. 10 2017 von Brooklyn Microgrid: https://www.brooklyn.energy/bmg-101

Buchleitner, C., & Rabl, T. (01 2017). Smart Contracts - Revolution oder alter Wein im digitalen Schlauch? *Ecolex Fachzeitschrift für Wirtschaftsrecht*, S. 4-10.

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Allgemeines bürgerliches Gesetzbuch, Fassung vom 13.09.2017. (1811/2017). Abgerufen am 13. 09 2017 von http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer= 10001622

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Bundes-Verfassungsgesetz. (kein Datum). Abgerufen am 26. 10 2017 von Bundeskanzleramt: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000138

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für E-Commerce-Gesetz. (kein Datum). Abgerufen am 15. 10 2017 von Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für E-Commerce-Gesetz: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001703

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Fern- und Auswärtsgeschäfte-Gesetz, Fassung vom 09.10.2017. (kein Datum). Abgerufen am 09. 10 2017 von ris.bka.gv.at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008847

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Konsumentenschutzgesetz, Fassung vom 13.09.2017. (kein Datum). Abgerufen am 13. 09 2017 von https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer =10002462

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Notariatsaktsgesetz, Fassung vom 13.09.2017. (1871/2017). Abgerufen am 13. 09 2017 von https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer =10001679

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Unternehmensgesetzbuch, Fassung vom 13.09.2017. (kein Datum). Abgerufen am 13. 09 2017 von https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer =10001702

Buterin, V. (2013). *A next generation smart contract & decentralized application platform.* Abgerufen am 15. 10 2017 von EthereumWhitePaper.pdf: https://github.com/ethereum/wiki/wiki/White-Paper

Bydlinski, P. (2007). *Bürgerliches Recht Band I Allgemeiner Teil.* Wien: Springer-Verlag.

Bydlinski, P. (2010). *Grundzüge des Privatrechts für Ausbildung und Praxis.* Wien: Manzsche Verlags- und Universitätsbuchhandlung.

CMS-Broschüre-Fin-Tech-eng.pdf. (2017). Abgerufen am 12. 10 2017 von CMS in Germany - International Law Firm: https://cms.law/en/content/download/308272/7780745/version/1/file/PR-Blockchain-18-07-2017-en.pdf

Condliffe, J. (09. 03 2017). *Blockchain für die Schiffslogistik*. Abgerufen am 03. 05 2017 von https://www.heise.de/tr/artikel/Blockchain-fuer-die-Schiffslogistik-3646857.html

Dapp, M. M., Balta, D., & Krcmar, H. (2017). *Blockchain - Disruption der öffentlichen Verwaltung.* Konrad Adenauer Stiftung.

Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. *Peer-to-Peer Computing (P2P), Thirteenth International Conference on IEEE.*

Diedrich, H. (2016). *Ethereum.* Wildfire Publishing.

Distributed-Ledger-Technologien im Zahlungsverkehrund in der Wertpapierabwicklung. (09 2017). Abgerufen am 09. 10 2017 von Deutsche Bundesbank: https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Monatsberichtsaufsaetze/2017/2017_09_distributed_ledger_technologien.pdf?__blob=publicationFile

Dolinar, H. (2010). *Legal English.* Linz: Johannes Kepler Universität Linz Multimediale Studienmaterialien GmbH.

Electronic Signatures v. Digital Signatures. (06. 12 2017). Abgerufen am 15. 10 2017 von eSign Genie:

https://www.esigngenie.com/blog/electronic-signatures-vs-digital-signatures/

Faust, F. (2016). *Digitale Wirtschaft - Analoges Recht.* Abgerufen am 10. 10 2017 von Gutachten A zum Deutschen Juristentag: http://static1.1.sqspcdn.com/static/f/1376130/26847040/1455040340113/Faust+Digitale+Wirtschaft+-+Analoges+Recht+Gutachten+fur+den+71.+DJT.PDF?token=73St8IVwwV4tYnJQSVMQJmH3F8c%3D

Fernabsatz-Gesetz. (kein Datum). Abgerufen am 09. 10 2017 von Internet4jurists: http://www.internet4jurists.at/gesetze/bg_fernabsatz01.htm

Finley, K. (18. 06 2016). *Wired.com : A 450 Mio Hack Showed That the DAO Was All to Human*. Abgerufen am 09. 10 2017 von Wired.com: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

Giese, D., Kops, M., Wagenknecht, S., de Boer, D., & Preuss, M. (2016). *Die Blockchain Bibel.* Kleve: Mark Preuss.

Gord, M. (26. 04 2016). *Smart Contracts Described By Nick Szabo 20 Years Ago Now Becoming Reality*. Abgerufen am 30. 04 2017 von https://bitcoinmagazine.com/: https://bitcoinmagazine.com/articles/smart-contractsdescribed-by-nick-szabo-years-ago-now-becoming-reality-1461693751/

Grau, C. (20. 06 2016). *Schweden integriert Blockchain beim Grundbuchamt*. Abgerufen am 15. 10 2017 von Netzwoche: http://www.netzwoche.ch/news/2016-06-20/schweden-integriert-blockchain-beim-grundbuchamt

Heckmann, D., & Kaulartz, D. (11. 11 2016). Selbsterfüllende Verträge. *c't magazin für computertechnik*, S. 138.

Kaulartz, M., & Heckmann, J. (13. 10 2016). *DAO Hack: Wenn sich der Smart Contract als "Dumb" erweist.* Abgerufen am 09. 10 2017 von CMSHS-bloggt: https://www.cmshs-bloggt.de/tmc/it-recht/dao-hack-wenn-der-smart-contract-sich-als-dumb-contract-erweist/

Koziol, H., & Welser, R. (2001). *Grundriss des bürgerlichen Rechts, Band II: Schuldrecht Allgemeiner Teil, Schuldrecht Besonderer Teil, Erbrecht.* Wien: Manzsche Verlags- und Universitätsbuchhandlung.

Leisinger, C. (10. 05 2016). *Zukunftsmodell oder Marketing-Gag?* Abgerufen am 15. 10 2017 von Neue Zürcher Zeitung AG: https://www.nzz.ch/finanzen/devisen-und-rohstoffe/devisen/bitcoin-ld.40204

Lessig, L. (01 2000). *Code is Law.* Abgerufen am 09. 10 2017 von havardmagazine.com: http://havardmagazine.com/2000/01/code-is-law.html

Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography.* CRC Press.

Merkle, R. C. (05. 01 1982). *Method of providing digital signatures*. Abgerufen am 30. 10 2017 von Google.com/patents: http://google.com/patents/US4309569

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Abgerufen am 12. 09 2017 von http://www.bitcoin.org/bitcoin.pdf

Omni Layer - Open-source,fully decentralized asset platform on the Bitcoin Blockchain. (kein Datum). Abgerufen am 30. 09 2017 von http://www.omnilayer.org/

Proof of Stake FAQ. (kein Datum). Abgerufen am 30. 10 2017 von Github: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

Public-Key-Verschlüsselungsverfahren. (kein Datum). Abgerufen am 15. 10 2017 von Wikipedia: https://de.wikipedia.org/wiki/Public-Key-Verschl%C3%BCsselungsverfahren

Raval, S. (2016). *Decentralized Applications.* O'Reilly.

Riedler, A. (2010). *Zivilrecht I Allgemeiner Teil.* Wien: Manzsche Verlags- und Universitätsbuchhandlung.

Szabo, N. (1997). The Idea of Smart Contracts.

Tapscott, D., & Tapscott, A. (2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World.* Penguin Books.

Urheberrechtsgesetz. (kein Datum). Abgerufen am 15. 10 2016 von Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Urheberrechtsgesetz: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001848

von Perfall, D., Hillebrand, T., Smole, E., Lay, L., & Charlet, M. (2016). *Blockchain - Chance für Energieverbraucher?* Düsseldorf: Verbraucherzentrale NRW.

Wagenknecht, S. (07. 07 2017). *Schweden nutzt jetzt offiziell die Blockchain für Grundbucheintragungen*. Abgerufen am 15. 10 2017 von BTC-ECHO: https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragungen/

Welzel, C., Eckert, K.-P., Kirstein, F., & Jacumeit, V. (2017). *Mythos Blockchain: Herausforderung für den öffentlichen Sektor.* Berlin: Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme.

Wood, G. (07. 08 2017). *Ethereum: A secure decentralized generalized transaction ledger.* Abgerufen am 13. 09 2017 von Ethereum Yellow Paper - GitHub Pages: https://ethereum.github.io/yellowpaper.pdf

Zhao, Z., & Chan, T.-H. (2016). How to Vote Privately Using Bitcoin. *Information and Communications Security, Bd. 9543*, S. 82-96.