Blockchain und Smart Contracts

Die vertragsrechtlichen Implikationen einer neuen Technologie

Inauguraldissertation zur Erlangung der Würde eines Doctor iuris der Rechtswissenschaftlichen Fakultät der Universität Bern.

vorgelegt von

Eleonor Gyr

Die Fakultät hat diese Arbeit am 21. Februar 2019 auf Antrag der beiden Gutachterinnen, Prof. Dr. Susan Emmenegger und Prof. Dr. Mirjam Eggen, als Dissertation angenommen.

source: https://doi.org/10.24442/boristheses.1200 | downloaded: 4.7.2025

Urheberrechtlicher Hinweis

Dieses Dokument steht unter einer Lizenz der Creative Commons Namensnennung-Keine kommerzielle Nutzung-Keine Bearbeitung 2.5 Schweiz.
http://creativecommons.org/licenses/by-nc-nd/2.5/ch/

Sie dürfen:

dieses Werk vervielfältigen, verbreiten und öffentlich zugänglich machen.

Zu den folgenden Bedingungen:

Namensnennung. Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen (wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt).

Keine kommerzielle Nutzung. Dieses Werk darf nicht für kommerzielle Zwecke verwendet werden.

Keine Bearbeitung. Dieses Werk darf nicht bearbeitet oder in anderer Weise verändert werden.

Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter welche dieses Werk fällt, mitteilen.

Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.

Diese Lizenz lässt die Urheberpersönlichkeitsrechte nach Schweizer Recht unberührt. Eine ausführliche Fassung des Lizenzvertrags befindet sich unter http://creativecommons.org/licenses/by-nc-nd/2.5/ch/legalcode.de.

Das Originaldokument ist auf dem Webserver der Universitätsbibliothek Bern gespeichert.

.

Vorwort

Als ich im Jahr 2016 die Arbeit an der vorliegenden Dissertation aufnahm, waren die Begriffe «Blockchain» und «Smart Contracts» zwar bereits verbreitet; wissenschaftliche Auseinandersetzungen dazu waren jedoch – insbesondere im deutschsprachigen Raum – nur spärlich vorhanden. Die juristische Aufarbeitung eines technischen Themas ohne Rückgriffmöglichkeiten auf einen reichen Fundus an Literatur war einer der Knackpunkte aber auch die Hauptmotivation für die Ausarbeitung dieser Dissertation. Zwischenzeitlich findet auch in der Schweizer Literatur eine rege Auseinandersetzung zu den Themen Blockchain und Smart Contracts statt. Ich hoffe, dass die vorliegende Arbeit ihren Teil zu dem noch jungen Forschungsfeld beitragen kann.

Ich danke meiner Doktormutter Prof. Dr. Susan Emmenegger für die grosse Freiheit, die sie mir bei der Ausarbeitung der Arbeit gewährte. Prof. Dr. Mirjam Eggen danke ich für die Zweitbegutachtung und die anregenden Diskussionen zur Blockchain-Technologie während meiner Zeit als Assistentin am Zivilistischen Seminar der Uni Bern.

Von Herzen bedanke ich mich auch bei RA MLaw Corina Flückiger, M.A. Ramón Gander und M.A. Hans Martin Jörimann, die mich mit ermunterndem Zuspruch, kritischer Durchsicht und geduldigem Lektorat bei meinem Dissertationsvorhaben begleitet haben.

Manuskriptschluss der vorliegenden Arbeit war der 28. Juni 2018; Literatur, Materialien und Rechtsprechung sind nur bis zu diesem Zeitpunkt berücksichtigt.

Basel, im März 2019 Eleonor Gyr

Inhaltsübersicht

INHALTSÜBERSICHT ..... **IV**

INHALTSVERZEICHNIS ..... **VII**

ABKÜRZUNGSVERZEICHNIS ..... **XVII**

LITERATURVERZEICHNIS ..... **XXIII**

MATERIALIENVERZEICHNIS ..... **XLI**

WEITERE QUELLEN ..... **XLII**

EINLEITUNG **1**

1. TEIL: GRUNDLAGEN **3**

A. EINFÜHRUNG IN DIE BLOCKCHAIN-TECHNOLOGIE **4**

I. Historie und Begriff 5

II. Typologie 14

III. Vertrauen und die Blockchain 16

B. TECHNISCHE ASPEKTE DER BLOCKCHAIN-TECHNOLOGIE **22**

I. Funktionsweise einer Blockchain 22

II. Blockchain-Beispiele 29

C. VERTRAGLICHE ASPEKTE DER BLOCKCHAIN-TECHNOLOGIE **36**

I. Involvierte Parteien 36

II. Blockchain als Software 40

III. Blockchain als Plattform 60

IV. Fazit 84

2. TEIL: SMART CONTRACTS 85

A. EINFÜHRUNG SMART CONTRACTS 86

I. Historie und Begriff 86

II. Funktionsweise von Smart Contracts 99

III. Fazit 104

B. VERTRAGSABSCHLUSS UND SMART CONTRACTS 105

I. Vorfrage: Programmiersprache als Vertragssprache 106

II. Vertragsparteien: Rechts- und Geschäftsfähigkeit 110

III. Rechtsbindungswille und Willenserklärung: Antrag und Annahme .. 115

IV. Übereinstimmende Willenserklärung 135

V. Widerruf 138

VI. Inhalt des Vertrages 142

VII. Formvorschriften 148

VIII. Fazit 164

C. MANGELHAFTE WILLENSERKLÄRUNGEN 165

I. Irrtum 165

II. Täuschung und Furchterregung 170

III. Rechtsfolgen 172

IV. Fazit 176

D. LEISTUNGSSTÖRUNGEN 177

I. Leistungsunmöglichkeit 177

II. Positive Vertragsverletzung 184

III. Spätleistung 187

IV. Fazit 190

E. GEWÄHRLEISTUNG UND HAFTUNG 191

I. Fehler in der Software (Bug) 191

II. Fehlerhafte Anwendung des Smart Contract 199

III. Fazit 201

F. SMART CONTRACTS ALS HALTER VON VERMÖGENSWERTEN 202

I. Übertragung von Vermögenswerten 202

II. Funktion des Smart Contract 205

III. Fazit 211

3. TEIL: ZUSAMMENFASSUNG 212

I. Erkenntnisse 212

II. Würdigung 218

ANHANG: BEGRIFFE UND ERLÄUTERUNGEN I

Inhaltsverzeichnis

INHALTSÜBERSICHT ..... **IV**

INHALTSVERZEICHNIS ..... **VII**

ABKÜRZUNGSVERZEICHNIS ..... **XVII**

LITERATURVERZEICHNIS ..... **XXIII**

MATERIALIENVERZEICHNIS ..... **XLI**

WEITERE QUELLEN ..... **XLII**

EINLEITUNG **1**

1. TEIL: GRUNDLAGEN **3**

A. EINFÜHRUNG IN DIE BLOCKCHAIN-TECHNOLOGIE **4**

I. Historie und Begriff 5
1. Die Bitcoin-Blockchain 5
2. Neuere Entwicklungen 6
3. Definition 9
4. Merkmale 10
a) Dezentrales, verteiltes Netzwerk 10
b) Transaktionsregister 11
c) Unabänderbarkeit der registrierten Daten 12
d) Pseudoanonymität 12

II. Typologie 14
1. Öffentliche Blockchain 15
2. Private Blockchain 15
3. Mischformen 16

III. Vertrauen und die Blockchain 16
1. Vertrauen in der öffentlichen Blockchain 17
2. Vertrauen in der privaten Blockchain 19
3. Vertrauen im Schweizer Rechtssystem 19
4. Vertrauenslose Systeme im Schweizer Rechtssystem 20

5. Fazit 21

B. TECHNISCHE ASPEKTE DER BLOCKCHAIN-TECHNOLOGIE 22

I. Funktionsweise einer Blockchain 22
1. Transaktionsauslösung 23
2. Konsensverfahren 25
a) Öffentliche Blockchain 26
b) Private Blockchain 28
3. Blockbildung 28

II. Blockchain-Beispiele 29
1. Bitcoin-Blockchain 29
a) Zweck 30
b) Transaktionsmechanismus 30
2. Ethereum-Blockchain 31
a) Zweck 31
b) Transaktionsmechanismus 32
3. Hyperledger 32
a) Zweck 33
b) Transaktionsmechanismus 33
4. Corda 34
a) Zweck 34
b) Transaktionsmechanismus 34

C. VERTRAGLICHE ASPEKTE DER BLOCKCHAIN-TECHNOLOGIE 36

I. Involvierte Parteien 36
1. Softwareentwickler 37
2. Nutzer 37
3. Miner 38
4. Wallet-Anbieter 39

II. Blockchain als Software 40
1. Open-Source-Software 41
a) Begriff 42
b) OSS-Lizenzen 43

c) Abgrenzungen 45
d) Blockchain als Open-Source-Software 46
2. OSS-Lizenzvertrag 47
a) Vertragsparteien 47
b) Vertragsgegenstand 49
c) Zeitpunkt des Zustandekommens des OSS-Lizenzvertrages 49
d) Vertragstypologie 51
aa) Gefälligkeit 53
bb) Schenkung 54
cc) Leihe 56
dd) Einfacher Auftrag 56
ee) Zwischenfazit 57
e) Weitere Vertragsbestandteile 57
aa) Bedingung / Auflage 57
bb) Haftungs- und Gewährleistungsausschlüsse 58
3. Fazit 59

III. Blockchain als Plattform 60
1. P2P-Netzwerk 61
a) Begriff 61
b) Eigenschaften 62
2. Gesellschaftsrechtliche Aspekte eines P2P-Blockchain-Netzwerkes 63
a) Körperschaft 64
b) Personengesellschaft 64
c) Einfache Gesellschaft 65
aa) Zwei oder mehr Personen 65
bb) Vertragsmässige Verbindung 66
cc) Gemeinsamer Zweck mit gemeinsamen Mitteln 68
dd) Fehlende Identifizierbarkeit der Gesellschafter 69
d) Fazit 70
3. Vertragsverhältnis innerhalb des P2P-Netzwerkes 70
a) Vertragsverhältnis Nutzer – Miner 71
aa) Ethereum-Blockchain 72
bb) Bitcoin-Blockchain 73
b) Exkurs: Vertragsverhältnis Miner – Nutzer ausserhalb des Netzwerkes 74
aa) Stellvertretung 75
bb) Hilfsperson 76

c) Fazit 77
4. Zugang zum P2P-Blockchain-Netzwerk 78
a) Internet Service Provider 78
b) Internet-Provider-Haftung 79
c) Wallet-Anbieter als Provider? 81
d) Fazit 83
5. Fazit 83

IV. Fazit 84

2. TEIL: SMART CONTRACTS 85

A. EINFÜHRUNG SMART CONTRACTS 86

I. Historie und Begriff 86
1. Historie 86
2. Neuere Entwicklungen 87
3. Smart Contract von Ethereum 89
4. Definitionsansätze 90
a) Technische Ansätze 90
b) Juristische Ansätze 93
5. Eigene Definition von Smart Contracts 94
6. Merkmale 95
a) Autonomie/Eigenständigkeit 95
b) Unveränderbarkeit 96
c) Keine Interpretationsmöglichkeit 97
7. Exkurs: Elektronischer Agent 97
a) Begriff 98
b) Smart Contracts und elektronische Agenten 98

II. Funktionsweise von Smart Contracts 99
1. Allgemeines 99
2. Bezug zu Ereignissen ausserhalb der Blockchain 101
3. Übertragung von Vermögenswerten an den Smart Contract 102
4. Beispiele 102
a) Wohnungs- oder Automiete: Smarte Schlösser 102
b) Versicherung 103
c) Musik 103
d) Logistik 104

III. Fazit 104

B. VERTRAGSABSCHLUSS UND SMART CONTRACTS 105

I. Vorfrage: Programmiersprache als Vertragssprache 106
1. Formfreiheit und Stillschweigen 106
2. Programmiersprache 106
3. Unterschied Programmiersprache zu konventioneller Sprache 107
4. Programmiersprache als Vertragssprache 108
5. Fazit 109

II. Vertragsparteien: Rechts- und Geschäftsfähigkeit 110
1. Rechtsfähigkeit 110
2. Geschäftsfähigkeit 111
3. Rechts- und Geschäftsfähigkeit bei Smart Contracts 112
a) Öffentliche Blockchain 113
b) Private Blockchain 113
4. Fazit 114

III. Rechtsbindungswille und Willenserklärung: Antrag und Annahme .. 115
1. Rechtsbindungswille 116
a) Allgemeine Regeln 116
b) Im elektronischen Geschäftsverkehr 117
c) Bei Smart Contracts 117
aa) Fachkundige Personen 118
bb) Fachunkundige Personen 119
cc) Fachkundige und fachunkundige Personen 120
2. Adressatenkreis und Formvorschriften 121
a) Allgemeine Regeln 121
b) Im elektronischen Geschäftsverkehr 122
c) Bei Smart Contracts 123
3. Zugang der Willenserklärung und Frist 125
a) Allgemeine Regeln 125
b) Im elektronischen Geschäftsverkehr 126
c) Bei Smart Contracts 127
4. Zeitpunkt des Vertragsabschlusses 128
a) Allgemeine Regeln 128
b) Im elektronischen Geschäftsverkehr 128

c) Bei Smart Contracts 129
5. Zurechenbarkeit der Willenserklärung 130
a) Allgemeine Regeln 130
b) Im elektronischen Geschäftsverkehr 131
c) Bei Smart Contracts 131
6. Auslegung der Willenserklärung 132
a) Allgemeine Regeln 133
b) Im elektronischen Geschäftsverkehr 133
c) Bei Smart Contracts 133
7. Fazit 133

IV. Übereinstimmende Willenserklärung 135
1. Allgemeine Regeln 135
a) Natürlicher und normativer Konsens 135
b) Dissens 136
c) Wesentliche Vertragsbestandteile 136
2. Konsens im elektronischen Geschäftsverkehr 137
3. Konsens bei Smart Contracts 137

V. Widerruf 138
1. Allgemeine Regeln 138
2. Widerruf im elektronischen Geschäftsverkehr 140
3. Widerruf bei Smart Contracts 140

VI. Inhalt des Vertrages 142
1. Grundsatz der Inhaltsfreiheit 142
2. Inhaltsschranken 142
a) Sittenwidrigkeit 143
b) Unmöglichkeit 143
c) Widerrechtlichkeit 143
3. Inhaltsschranken im elektronischen Geschäftsverkehr und bei Smart Contracts 144
4. Rechtsfolgen 144
a) Nichtigkeit 144
b) Teilnichtigkeit 146
c) Nichtigkeit und Teilnichtigkeit im elektronischen Geschäftsverkehr 147
d) Nichtigkeit und Teilnichtigkeit bei Smart Contracts 147

VII. Formvorschriften 148
1. Grundsatz der Formfreiheit 148
2. Einfache Schriftlichkeit 149
a) Erklärungsinhalt in Schriftzeichen 150
aa) Erklärungsinhalt in Schriftzeichen im elektronischen Geschäftsverkehr 152
bb) Erklärungsinhalt in Schriftzeichen bei Smart Contracts 152
b) Erklärungsträger 153
aa) Erklärungsträger im elektronischen Geschäftsverkehr 154
bb) Erklärungsträger bei Smart Contracts 156
c) Unterschrift 157
aa) Unterschrift im elektronischen Geschäftsverkehr 158
bb) Unterschrift bei Smart Contracts 158
3. Qualifizierte Schriftlichkeit 159
4. Öffentliche Beurkundung 160
5. Formungültigkeit 160
a) Nichtigkeit und Teilnichtigkeit 161
aa) Allgemeine Regeln 161
bb) Nichtigkeit und Teilnichtigkeit bei Smart Contracts 162
b) Rückabwicklung und Konversion 162
6. Fazit 163

VIII. Fazit 164

C. MANGELHAFTE WILLENSERKLÄRUNGEN 165

I. Irrtum 165
1. Allgemeine Regeln 165
1. Irrtum im elektronischen Geschäfts-verkehr 167
a) Eingabe- und Bedienungsfehler 167
b) Übermittlungsfehler 168
2. Irrtum bei Smart Contracts 169
a) Fehlerhafte Willenserklärung beim Abschluss des Grundgeschäftes 169
b) Eingabe- und Bedienungsfehler 169
c) Übermittlungsfehler 170

II. Täuschung und Furchterregung 170

1. Täuschung 170
2. Furchterregung 171
3. Täuschung und Furchterregung im elektronischen ..... Geschäftsverkehr und bei Smart Contracts 172

III. Rechtsfolgen 172
1. Einseitige Unverbindlichkeit 172
2. Schadenersatzpflicht 174
3. Genehmigung 175
4. Rechtsfolgen im elektronischen Geschäftsverkehr und bei ..... Smart Contracts 175

IV. Fazit 176

D. LEISTUNGSSTÖRUNGEN 177

I. Leistungsunmöglichkeit 177
1. Ursprüngliche und nachträgliche Leistungsunmöglichkeit 178
2. Objektive und subjektive Leistungsunmöglichkeit 178
3. Unverschuldete Leistungsunmöglichkeit 180
4. Verschuldete Leistungsunmöglichkeit 181
5. Leistungsunmöglichkeit bei Smart Contracts 182
a) Ursprüngliche Unmöglichkeit 182
b) Nachträgliche Unmöglichkeit 183
c) Objektive und subjektive Leistungsunmöglichkeit 183
d) Unverschuldete und verschuldete Leistungsunmöglichkeit 183

II. Positive Vertragsverletzung 184
1. Allgemeine Regeln 184
2. Positive Vertragsverletzung bei Smart Contracts 186

III. Spätleistung 187
1. Allgemeine Regeln 187
2. Spätleistung bei Smart Contracts 189

IV. Fazit 190

E. GEWÄHRLEISTUNG UND HAFTUNG 191

I. Fehler in der Software (Bug) 191
1. Vertragliche Gewährleistung und Haftung 192
a) OSS-Lizenz 192
b) Übrige Softwareverträge 194
2. Deliktische Haftung 195
a) Verschuldenshaftung nach Art. 41 ff. OR 195
b) Geschäftsherrenhaftung 196
c) Produktehaftung 197

II. Fehlerhafte Anwendung des Smart Contract 199
1. Vertragliche Haftung 199
2. Deliktische Haftung 200

III. Fazit 201

F. SMART CONTRACTS ALS HALTER VON VERMÖGENSWERTEN 202

I. Übertragung von Vermögenswerten 202
1. Arten von Vermögenswerten 202
2. Übertragung an Smart Contract 203
3. Involvierte Parteien 205

II. Funktion des Smart Contract 205
1. Smart Contract als Fiduziar 205
a) Treuhandvertrag 205
b) Smart Contract als Fiduziar 206
c) Sicherungszession 207
aa) Sicherungszession mit Smart Contracts 207
bb) Forderungsübertragung mit Smart Contracts 208
2. Smart Contract als Aufbewahrer 209
a) Hinterlegungsvertrag 209
b) Smart Contract als Aufbewahrer 209
3. Smart Contract als Escrow-Agent 210
a) Escrow-Agreement 210
b) Smart Contract als Escrow-Agent 210

III. Fazit 211

3. TEIL: ZUSAMMENFASSUNG 212

I. Erkenntnisse 212

II. Würdigung 218

ANHANG: BEGRIFFE UND ERLÄUTERUNGEN I

1. Software, Computerprogramm, Algorithmus i
2. Hash ii
3. Hash-Bäume iii
4. Kryptografische Verschlüsselungsverfahren iii
   a) Symmetrische Verschlüsselung iv
   b) Asymmetrische Verschlüsselung iv
5. Digitale Signatur vi
   a) Allgemeines vi
   b) Elektronische Signatur gemäss ZertES vii
6. Virtuelle Währung / Kryptowährung ix
7. Token xi
8. ICO / TGE xiii
9. Hard Fork / Soft Fork xiii
10. DAOs / DAPs / DACs etc. xiv

Abkürzungsverzeichnis

a.A./A.A.	anderer Ansicht
ABl. EG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AJP	Aktuelle Juristische Praxis
API	Application Programming Interface
App(s)	Applikation(en)
AT	Allgemeiner Teil
Art.	Artikel
BAKOM	Bundesamt für Kommunikation
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (D)
BankG	Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 (SR 952.0)
BBl	Bundesblatt
betr.	betreffend
BGE	Amtliche Sammlung der Entscheide des Bundesgerichts
BGer	Bundesgericht
bspw.	beispielsweise
Bst.	Buchstabe
BV	Bundesverfassung
bzw.	beziehungsweise

ca.	circa
CHF	Schweizer Franken
CR	Computer und Recht
DAO	Dezentrale Autonome Organisation
DAPP	Dezentrale Applikation
d.h.	das heisst
DLT	Distributed Ledger Technologie
DuD	Datenschutz und Datensicherheit
E.	Erwägung
EÖBV	Verordnung über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen vom 8. Dezember 2017 (SR 211.435.1).
EFD	Eidgenössisches Finanzdepartement
ERC20	Ethereum Request for Comment 20
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
f. / ff.	folgende Seite(n)
FIDLEG	Bundesgesetz über die Finanzdienstleistungen (Finanzdienstleistungsgesetz) vom 15. Juni 2018 *(SR noch nicht bekannt)*
FinfraG	Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturgesetz) vom 19. Juni 2015 (SR 958.1)
FINMA	Eidgenössische Finanzmarktaufsicht

FINMA-RS	Rundschreiben der FINMA
Fn.	Fussnote
FS	Festschrift
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GNU-GPL	GNU General Public License
GNU-LGPL	GNU Lesser General Public License
h.L.	herrschende Lehre
Hrsg.	Herausgeber
http / https	Hyper Transfer Protocol / Hyper Transfer Protocol Secure
ICO	Initial Coin Offering
i.d.R.	in der Regel
InTeR	Zeitschrift zum Innovations- und Technikrecht
IoT	Internet of Things
IP	Internet Protokoll
IT	Information Technologie
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
KKG	Bundesgesetz über den Konsumkredit vom 23. März 2001 (SR 221.214.1)
Kt.	Kanton
lit.	litera
max.	maximal
min.	minimal

Mio.	Millionen
MIT	Massachusetts Institute of Technology
MM	Medienmitteilung
m.w.H.	mit weiteren Hinweisen
m.w.V.	mit weitern Verweisen
N.	Note
Nr.	Nummer
NZZ	Neue Zürcher Zeitung
o.ä.	oder ähnlich(e/er/s)
OR	Bundesgesetz betreffend die Ergänzung des Zivilgesetzbuches, Fünfter Teil: Obligationenrecht (SR 220)
OSS-Lizenz	Open-Source-Software-Lizenz
PoS	Proof of Stake
PoSp	Proof of Space
PoW	Proof of Work
PrHG	Bundesgesetz über die Produktehaftpflicht (Produktehaftpflichtgesetz) vom 18. Juni 1993 (SR 221.112.944).
P2P	Peer to Peer
resp.	respektive
RL	Richtlinie
SchlT	Schlusstitel
SLTA	Swiss Legal Tech Association
sog.	sogenannt(e/er/es)
SSRN	Social Science Research Network

SR	Ständerat
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht
TGE	Token Generating Event
THG	Bundesgesetz über die technischen Handelshindernisse vom 6. Oktober 1995 (SR 946.51)
u.a.	unter andere /anderen /anderem
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 9. Oktober 1992, SR 231.1
UIDG	Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010 (SR. 431.03)
UXTO	Unspent Transaction Output
vgl.	vergleiche
VO	Verordnung
WIPO	Word Intellectual Property Organization
www.	World Wide Web
z.B.	zum Beispiel
ZertES	Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur) vom 18. März 2016 (SR 943.03)
ZG	Zug
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210)

Ziff.	Ziffer
zit.	zitiert
ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (SR 272)

Literaturverzeichnis

Sämtliche Internet-Referenzen wurden zuletzt am 27. Juni 2018 eingesehen.

ADLER BENJAMIN, Rechtsfragen der Softwareüberlassung. Eine Untersuchung inbesondere der vielschichtigen Aspekte von sogenannten Weitergabeverboten, Münster 2014.

AEPPLI VIKTOR, Zürcher Kommentar zum Schweizerischen Zivilgesetzbuch, Obligationenrecht, Kommentar zur 1. und 2. Abteilung (Art.1-529 OR), Band Nr.V/1h/1, 3. Auflage, Zürich 1991.

AMSTUTZ MARC/MORIN ARIANE, Einleitung vor Art. 184 ff. OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529, 6. Auflage, Basel 2015,

ANTONOPOULOS ANDREAS M., Mastering Bitcoin. Unlock Digital Cryptocurrencies, Sebastopol 2017.

BACON LEE/BAZINAS GEORGE, "Smart Contracts": The Next Big Battleground?, in: Jusletter IT 18. Mai 2017.

BALSCHEIT PHILIPP, Konsumvertragsrecht und E-Commerce, Bern 2005.

BARRELET DENIS/EGLOFF WILLI, Art. 12 URG, in: Denis Barrelet und Willi Egloff (Hrsg.), Das neue Urheberrecht. Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, Bern 2008.

BAUSEN KRISTINA, Softwarepatente in den USA und Deutschland, Hamburg 2013.

BAYERN SHAWN/BURRI THOMAS/DALE GRANT THOMAS/HÄUSERMANN DANIEL M./MÖSLEIN FLORIAN/WILLIAMS RICHARD, Gesellschaftsrecht und autonome Systeme im Rechtsvergleich, in: AJP 2/2017, 192-203.

BERENTSEN ALEKSANDER/SCHÄR FABIAN, Bitcoin, Blockchain und Kryptoassets. Eine umfassende Einführung, Norderstedt 2017.

BERGER BERNHARD, Allgemeines Schuldrecht, Schweizerisches Obligationenrecht Allgemeiner Teil mit Einbezug des Deliktsrechts und Einführung in das Personen- und Sachenrecht, Bern 2018.

BERNET MARTIN, Art. 91 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

BOEHM FRANZISKA/PESCH PAULINA, Bitcoins: Rechtliche Herausforderung einer virtuellen Währung. Eine erste juristische Einordnung, in: MMR 2/2014, 75-79.

BOOG MARKUS, Art. 110 StGB, in: Marcel Alexander Niggli und Hans Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1-110 StGB und Jugendstrafgesetz, 3. Auflage, Basel 2013.

BRÄUTIGAM PETER, 1.Teil, A. E-Commerce 2.0, in: Peter Bräutigam und Daniel Rücker (Hrsg.), E-Commerce. Rechtshandbuch, München 2017.

BROWN RICHARD GENDAL/CARLYLE JAMES/GRIGG IAN/HEARN MIKE, Whitepaper Corda: An Introduction, 2016, abrufbar unter <https://docs.corda.net>.

BUCHER EUGEN, Schweizerisches Obligationenrecht, Allgemeiner Teil ohne Deliktsrecht, 2. neubearbeitete und erweiterete Auflage, Zürich 1988.

BURGWINKEL DANIEL, Blockchain Technology. Einführung für Business- und IT-Manager, Berlin/Boston 2016.

CHERPILLOD IVAN, Art. 2 URG, in: Barbara K. Müller und Reinhard Oertli (Hrsg.), Stämpflis Handkommentar, Urheberrechtsgesetz (URG), 2. Auflage, Bern 2012.

CHIAMPI OHLY DIANA D., SoftwareRecht: Von der Entwicklung zum Export. Probleme und Lösungen nach deutschem und amerikanischem Recht, 2. überarbeitete Auflage, Frankfurt a.M. 2013.

CHRISTIDIS KONSTANTINOS/DEVETSIKIOTIS MICHAEL, Blockchains and Smart Contracts for the Internet of Things, in: IEEE Access, Volume 4/2016, 2292-2303.

CLACK CHRISTOPHER D./BAKSHI VIKRAM A./BRAINE LEE, Smart Contract Templates: foundations, design landscape and research directions, 4. August 2016, abrufbar unter < https://arxiv.org>.

CREUTZ SEBASTIAN, Regeln virtueller Welten, Hamburg 2014.

DASSER FELIX, Art. 358 ZPO, in: Paul Oberhammer u.a. (Hrsg.), Kurzkommentar ZPO Schweizerische Zivilprozessordnung, Basel 2014.

DU PASQUIER SHELBY/POSKRIAKOV FEDOR, Art. 98 KAG, in: René Bösch u.a. (Hrsg.), Basler Kommentar, Kollektivanlagengesetz, 2. Auflage 2016.

DUNKEL JÜRG/EBERHART ANDREAS/FISCHER STEFAN/KLEINER CARSTEN/ KOSCHEL ARNE, System-Architekturen für verteilte Anwendungen, München 2008.

EBENHOCH PETER, Blockchain Compliance, in: Jusletter IT 22. Februar 2018.

EBENHOCH PETER/GANTER FELIX, Smart Contexts für Smart Contracs - Legal Programming für valide Blockchain-Verträge, in: Jusletter IT 22. Februar 2018.

ECKERT MARTIN, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, in: SJZ112/2016, 265-274.

- Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, in: SJZ 112/2016, 245-249.

EFFELSBERG WOLFGANG/STEINMETZ RALF/STRUFE THORSTEN, Benchmarking Peer-to-Peer Systems. Understanding Quality of Service in Large-Scale Distributed Systems, Berlin Heidelberg 2013.

EGGEN MIRJAM, Home Smart Home, in: AJP 9/2016, 1131-1140.

- Chain of Contracts. Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers, in: AJP 1/2017, 3-15.
- Was ist ein Token?, in: AJP 5/2018, 558-567.

EHRAT FELIX R./WIDMER MARKUS, Vorbemerkungen zu Art. 151-157 OR, Art. 151, 154 OR in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-520 OR, 6. Auflage, Basel 2015.

EICHNER MARK, Die Rechtsstellung von Treugebern und Begünstigten aus Trust und Treuhand unter besonderer Berücksichtigung des Haager Trust Übereinkommens und des Aussonderungsanspruchs, Basel 2007.

EISENHUT STEFAN, Escrow-Verhältnisse, das Escrow Agreement und ähnliche Sicherungsgeschäfte, Basel 2009.

ENGELHARDT CHRISTIAN, Die rechtliche Behandlung von Urheberrechtsverletzungen in P2P-Netzwerken nach US-amerikanischem und deutschem Recht, Frankfurt a.M. 2007.

EPINEY ASTRID, Art. 5 BV, in: Bernhard Waldmann u.a. (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015.

ESSEBIER JANA/BOURGEOIS JANIQUE, Die Regulierung von ICOs, in: AJP 5/2018, 568-579.

FANKHAUSER ROLAND, Art. 11, 12, 16, 17 und 18 ZGB, in: Thomas Geiser und Christina Fountoulakis (Hrsg.), Basler Kommentar, Zivilgesetzbuch I, Art. 1-456 ZGB, 6. Auflage, Basel 2018.

FELLMANN WALTER/MÜLLER KARIN, Berner Kommentar, Schweizerisches Zivilgesetzbuch, das Obligationenrecht, Die einzelnen Verhältnisse, Der einfache Auftrag, Art. 394-406 OR, Bern 2006.

FELLMANN WALTER, Produktehaftpflichtgesetz (PrHG), in: Heinrich Honsell u.a (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

FERCSIK SCHNYDER ORSOLYA, Internet-Access-Providing-Verträge mit geschäftlichen und privaten Endkuknden. Eine vertragsrechtliche Analyse nach dem schweizerischen Recht unter besonderer Berücksichtigung des Rechts der Europäischen Union, Zürich 2012.

FISCHER PETER/HOFER PETER, Lexikon der Informatik, 15. überarbeitete Auflage, Berlin 2011.

FISS OLAF, Die Haftung für fehlerhafte Software im Wettbewerb der Rechtsordnungen. Eine rechtsvergleichende Analyse, Frankfurt a.M. 2013.

FREI OLIVER, Der Abschluss von Konsumentenverträgen im Internet, Zürich 2001.

FRÖHLICH-BLEULER GIANNI, Open Source Compliance, in: Jusletter 12. November 2012.

- Softwareverträge, Bern 2014

FURRER ANDREAS, Die Einbettung von Smart Contracts in das schweizerische Privatrecht, in: Anwaltsrevue 3/2018, 103-115.

GANTER FELIX, "Code is Law" aber "is Code Law"?, in: Jusletter IT 22. Februar 2018.

GAUCH PETER/SCHLUEP WALTER R./SCHMID JÖRG/EMMENEGGER SUSAN, Schweizerisches Obligationenrecht Allgemeiner Teil, ohne ausservertragliches Haftpflichtrecht, 2 Bände, 10. Auflage, Zürich/Basel/Genf 2014.

GERHARDS JULIA, (Grund-) Recht auf Verschlüsselung?, Baden-Baden 2010.

GERVAIS ARTHUR, Vorteile und Probleme von Blockchains, in: digma 2017, 128-131.

GIRSBERGER DANIEL, Art. 358 ZPO, in: Karl Spühler u.a. (Hrsg.), Basler Kommentar Schweizerische Zivilprozessordnung (ZPO), 3. Auflage, Basel 2017.

GIRSBERGER DANIEL/HERRMANN JOHANNES LUKAS, Art. 164, 165 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

GISLER MICHAEL, Vertragsrechtliche Aspekte Elektronischer Märkte - nach Schweizerischem Obligationenrecht, Bamberg 1999.

GLARNER ANDREAS/MEYER STEPHAN D., Smart Contracts in Escrow-Verhältnissen, in: Jusletter 4. Dezember 2017.

GRAHAM-SIEGENTHALER BARBARA/FURRER ANDREAS, The Position of Blockchain Technology and Bitcoin in Swiss Law, in: Jusletter 8. Mai 2017.

GRÄNICHER DIETER, Art. 178 IPRG, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar Internationales Privatrecht, 3. Auflage, Basel 2013.

GRÜNEWALD SERAINA, Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen, in: Rolf H. Weber und Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 93-112.

GUILLOD OLIVIER/STEFFEN GABRIELLE, Art. 19 / 20 OR, in: Luc Thévenoz und Franz Werro (Hrsg.), Commentaire Romand, Code des obligations I, Art. 1-529 CO, 2. Auflage, Basel 2012.

GYR ELEONOR, Dezentrale Autonome Organisation DAO, in: Jusletter 4. Dezember 2017.

HANCOCK MATTHEW/VAIZEY ED, Distributed Ledger Technology: beyond block chain. A report by the UG Government Chief Scientific Adviser, 2016, abrufbar unter: <www.gov.uk>.

HANDSCHIN LUKAS, Die Abgrenzung zwischen der losen Zusammenarbeit und der einfachen Gesellschaft, in: Marc Amstutz (Hrsg.), Die vernetzte Wirtschaft. Netzwerke als Rechtsproblem, Zürich 2004, 107-120.

- Art. 530 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar Obligationenrecht II, Art. 530-946 OR inkl. Schlussbestimmungen, 5. Auflage, Basel 2016.

HAUSHEER HEINZ/AEBI-MÜLLER REGINA E., Art. 2 ZGB, in: Heinz Hausheer und Hans Peter Walter (Hrsg.), Berner Kommentar, Einleitung, Art. 1-9 ZGB Schweizerisches Zivilgesetzbuch, Einleitung und Personenrecht, Bern 2012.

HEARN MIKE, Whitepaper Corda: A distributed Ledger, Version 0.5, 2016, abrufbar unter: <https://docs.corda.net>.

HEROLD HELMUT/LURZ BRUNO/WOHLRAB JÜRGEN/HOPF MATTHIAS, Grundlagen der Informatik, 3. aktualisierte Auflage, Hallbergmoos 2017.

HESS HANS-JOACHIM, Stämpflis Handkommentar SHK, Produktehaftpflicht-gesetz (PrHG). Bundesgesetz über die Produktehaftpflicht vom 18. Juni 1993, 3. überarbeitete und ergänzte Auflage, Zürich 2016.

HESS MARTIN /WEISS VOIGT ALEXANDRA, E-Geld, E- und M-Payments gemäss Schweizer Recht, in: Clearit März 2014, 8-9.

HESS MARTIN/LIENHARD STEPHANIE, Übertragung von Vermögenswerten auf der Blockchain, in: Jusletter 4. Dezember 2017.

HILTY RETO M., Lizenzvertragsrecht. Systematisierung und Typisierung aus schutz- und schuldrechtlicher Sicht, Bern 2001.

- Softwarevertrag: Qualifikation im Lichte des gesetzlichen Gebrauchsrechts, in: Friedrich Harrer u.a. (Hrsg.), Besonderes Vertragsrecht - aktuelle Probleme. Festschrift für Heinrich Honsell zum 60. Geburtstag, Zürich/Basel/Genf 2001, 62-84.
- Die Rechtsnatur des Softwarevertrags, Erkenntnisse aus der Entscheidung des EuGH UsedSoft vs. Oracle, in: CR 10/2012, 625-637.

HOEREN THOMAS, Internetrecht, ein Grundriss, 3. Auflage, Berlin/Boston 2018.

HOFER SIBYLLE/HRUBESCH-MILLAUER STEPHANIE, Einleitungsartikel und Personenrecht, 2. Auflage, Bern 2012.

HONSELL HEINRICH, Art. 2 ZGB, in: Thomas Geiser und Christina Fountoulakis (Hrsg.), Basler Kommentar, Zivilgesetzbuch I, Art. 1-456 ZGB, 6. Auflage, Basel 2018.

- Art. 199 OR, in: Heinrich Honsell u. a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

HUGUENIN CLAIRE, Zum Verhältnis zwischen linguistischen Kommunikationsmodellen und Verträgen, in: Rolf Sethe u.a. (Hrsg.), Kommunikation, Festschrift für Rolf H. Weber zum 60. Geburstag, Bern 2011.

- Obligationenrecht. Allgemeiner und Besonderer Teil, 2. Auflage, Zürich 2014.

HUGUENIN CLAIRE/MEISE BARBARA, Art. 19/20 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

HUGUENIN CLAIRE/REITZE CHRISTOPHE PETER, 27, 54 ZGB, in: Thomas Geiser und Christina Fountoulakis (Hrsg.), Basler Kommentar, Zivilgesetzbuch I, Art. 1-456 ZGB, 6. Auflage, Basel 2018.

HÜRLIMANN-KAUP BETTINA, Die privatrechtliche Gefälligkeit und ihre Rechtsfolgen, Freiburg 1999.

HÜRLIMANN-KAUP BETTINA/SCHMID JÖRG, Einleitungsartikel des ZGB und Personenrecht, 3. ergänzte, verbesserte und nachgeführte Auflage, Zürich 2016.

ISLER MICHAEL, Datenschutz auf der Blockchain, in: Jusletter 4. Dezember 2017.

JACCARD GABRIEL, Smart Contract and the Role of Law, in: Jusletter IT 23. November 2017.

JAEGER TILL/METZGER AXEL, Open Source Software. Rechtliche Rahmenbedingungen der Freien Software, 4. Auflage, München 2016.

JUNG PETER, Art. 530 OR, in: Vito Roberto und Hans Rudolf Trüeb (Hrsg.), Handkommentar zum Schweizer Privatrecht, Personengesellschaften und Aktiengesellschaft, Vergütungsverordnung, 3. Auflage, Zürich 2016.

- Art. 625 OR, in: Lukas Handschin (Hrsg.), Zürcher Kommentar, Obligationenrecht, Art. 620-659b OR, die Aktiengesellschaft, Allgemeine Bestimmungen, Zürich 2016.

JUNG PETER/KUNZ PETER V./BÄRTSCHI HARALD, Gesellschaftsrecht, Zürich 2016.

KAULARTZ MARKUS, Die Blockchain Technologie, Hintergründe zur Distributed Ledger Technologie und zu Blockchains, in: CR 7/2016, 474-480.

Herausforderung bei der Gestaltung von Smart Contracts, in: InTer 4/16, 201-206.

KAULARTZ MARKUS/HECKMANN JÖRN, Smart Contracts - Anwendung der Blockchain Technologie, in: CR 9/2016, 618-624.

KERNEN ALEXANDER, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlung seines Kunden, in: Jusletter 4. März 2013.

KESSLER MARTIN A., Art. 41, 55 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art.1-529 OR, 6. Auflage, Basel 2015.

KIANICKA MICHAEL MARTIN, Die Agentenerklärung. Elektronische Willenserklärungen und künstliche Intelligenz als Anwendungsfall der Rechtsscheinshaftung, Zürich 2012.

KIENZLER ROMEO, Hyperledger - eine offene Blockchain Technologie, in: Daniel Burgwinkel (Hrsg.), Blockchain Technology. Einführung für Business- und IT Manager, Berlin/Boston 2016, 110-121.

KOCH FRANK A., Urheber- und kartellrechtliche Aspekte der Nutzung von Sopen-Source Software (I), in: CR 5/2000, 273-281.

- Urheber- und kartellrechtliche Aspekte der Nutzung von Open-Source-Software (II), in: CR 6/2000, 333-344

KOLLER THOMAS, Vorbemerkungen zu Art. 472-491, Art. 472 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR OR, 6. Auflage, Basel 2015.

KOLLER-TUMLER MARLIES, Art. 40a, 40b, 40c OR, in: Heinrich Hosell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

KOLVART MERIT/POOLA MARGUS/RULL ADDI, Smart Contracts, in: Tanel Kerikmäe und Addi Rull (Hrsg.), The Future of Law and eTechnologies, Cham 2016.

KRAMER ERNST A., Berner Kommentar, Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, Allgemeine Bestimmungen: Der Inhalt des Vertrages, Art. 19-22 OR, Bern 1991.

KRAMER ERNST A./SCHMIDLIN BRUNO, Berner Kommentar, Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, Allgemeine Bestimmungen: Die Entstehung durch Vertrag, Art. 1-18 OR, Bern 1986.

KRAMER ERNST A./PROBST THOMAS/PERRIG ROMAN, Schweizerisches Recht der Allgmeinen Geschäftsbedingungen, Bern 2016.

KRONBLAD CHARLOTTA/HAAPIO HELENA, Smart Contracts - Not so smart legal professionals?, in: Jusletter IT 22. Februar 2018.

KRYPZCYK VEIKKO/BOCHKOR OLENA, Programmieren für Einsteiger. Teil 1, Frankfurt a.M. 2015.

KÜTÜK-MARKENDORF MERIH ERDEM, Rechtliche Einordnung von Internetwährungen im deutschen Rechtssystem am Beispiel von Bitcoin, Frankfurt a.M. 2016.

LAUX CHRISTIAN/WIDMER JAN, Produkthaftung für Open-Source-Software?, in: Bernd Lutterbeck u.a. (Hrsg.), Open Source Jahrbuch 2007, Berlin 2007, 495-510.

LOHMANN MELINA F., Roboter als Wundertüten - eine zivilrechtliche Haftungsanalyse, in: AJP 2/2017, 152-162.

LUDEWIG JOCHEN/LICHTER HORST, Software Enegineering. Grundlagen, Menschen, Prozesse, Techniken, 3. korrigierte Auflage, Heidelberg 2013.

MARLY JOCHEN, Praxishandbuch Softwarerecht. Rechtsschutz und Vertragsgestaltung, 6. vollständig überarbeitete Auflage, München 2014.

MEIER-HAYOZ ARTHUR/FORSTMOSER PETER, Schweizerisches Gesellschaftsrecht mit Einbezug des künftigen Rechnungslegungsrechts und der Aktienrechtsreform, Bern 2012.

MEISSER LUZIUS, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Rolf H. Weber und Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 73-92.

MEYER STEPHAN D./SCHUPPLI BENEDIKT, Smart Contracts und deren Einordnung in das schweizerische Vertragsrecht, in: recht 2017, 204-224.

MIELKE BETTINA/WOLFF CHRISTINA, "Klar ist der Aether und doch von unergründlicher Tiefe" - Smart Contracts als interdisziplinäres Problem, in: Jusletter IT 22. Februar 2018.

MIK ELIZA, Smart contracts: Terminology, technical limitations and real world complexity, in: Law, Innovation and Technology 9(2)/2017, 269-300.

MORSCHER LUKAS/DORIGO LAURA, Software-Lizenzverträge, Erschöpfung bei Computerprogrammen und Gebrauchthandel mit Softwarelizenzen, in: Florian S. Jörg und Oliver Arter (Hrsg.), Internet-Recht und IT-Verträge, 8. Tagungsband, Bern 2009, 17-61.

MOUGAYAR WILLIAM, The Business Blochckain. Promise, Practice, and Application of the Next Internet Technology, Hoboken 2016.

NAKAMATO SATOSHI, Whitepaper Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, abrufbar unter: <https://bitcoin.org>.

PAAR CHRISTOF/PELZL JAN, Kryptografie verständlich. Ein Lehrbuch für Sudierende und Anwender, Berlin/Heidelberg 2016.

PABST RAFAEL, Blockchain-Technologie. Einführung in die Thematik Blockchain und die Blockchain-Managementsysteme anhand von Bitcoin, Ethereum und Hyperledger, abrufbar unter: <https://rafaelpabst.de/assets/bc_rpb.pdf>.

PESTALOZZI CHRISTOPH M./VOGT HANS-UELI, Art. 530, 543 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht II, Art. 530-964 OR inkl. Schlussbestimmungen, 5. Auflage, Basel 2016.

PLOOM TARMO, Blockchains - wichtige Fragen aus IT-Sicht, in: Daniel Burgwinkel (Hrsg.), Blockchain Technology, Einführung für Business und IT-Manager, Berlin/Boston 2016.

POLEDNA TOMAS/SCHLAURI SIMON/SCHWEIZER SAMUEL, Rechtliche Voraussetzungen der Nutzung von Open-Source-Software in der öffentlichen Verwaltung, insbesondere des Kantons Bern, Berlin/Bern 2017.

PRAZELLER MARKUS, Der Mitwirkungsbegriff in Art. 28 Abs. 1 ZGB bedarf einer Einschränkung, in: Medialex 2017, 45-50.

PROBST THOMAS, Der Lizenzvertrag: Grundlagen und Einzelfragen, in: Jusletter 2. September 2013.

REDEKER HELMUT, IT-Recht, 6. neubearbeitete Auflage, München 2017.

REETZ PETER, Die Sicherungszession von Foderungen unter bersonderer Berücksichtigung vollstreckungsrechtlicher Probleme, Zürich 2006.

- Die Sicherungszession: Aktuelle Rechtsfragen, in: Susan Emmenegger (Hrsg.), Kreditsicherheiten, Tagungsband Schweizerische Bankrechtstagung 2008, Basel 2008, 178-212.

REUTTER GERSTER CHRISTINA, Art. 29 URG, in: Barbara K. Müller und Reinhard Oertli (Hrsg.), Stämpflis Handkommentar, Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und verwandte Schutzrechte. Mit Ausblick auf das EU-Recht, deutsches Recht, Staatsverträge und die internationale Rechtsentwicklung, 2. Auflage, Bern 2012.

RIGAMONTI CYRILL P., Providerhaftung - auf dem Weg zum Urheber-verwaltungsrecht, in: sic! 2016, 117-134.

RIGAMONTI CYRILL P./WULLSCHLEGER MARC, Zur Teilnahme an Urheberrechtsverletzungen, in: sic! 2018, 47-56.

ROHN PATRICK, Zivilrechtliche Verantwortlichkeit der Internet Provider nach schweizerischem Recht, Zürich 2004.

ROON MICHA, Schlichtung und Blockchain, in: Anwaltsrevue 09/2016, 359-363.

ROWLAND DIANA/KOHL UTA/CHARLESWORTH ANDREW, Information Technology Law, 5. Auflage, Abingdon/New York 2017.

SANSONNETTI RICCARDO, Bitcoin: Virtuelle Währung mit Chancen und Risiken, in: Die Volkswirtschaft 9/2014, 44-46.

SCHALLER JEAN-MARC, Blockchain Serie, #1 Prolog: Smart Contracts ("Smart Codes"), Blockchain, Internet-of-Things ("IoT"), blogpost 32 (FinBlog), 2018, abrufbar unter: <www.finblog.ch>.

- Blockchain-Serie, #3 "Smart-Code"-Vertragsrecht, blogpost 34 (FinBlog), 2018, abrufbar unter: <www.finblog.ch>.

SCHÄRER HEINZ/MAURENBRECHER BENEDIKT, Art. 305 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

SCHMEH KLAUS, Kryptografie. Verfahren, Protokolle, Infrastrukturen, 6. Auflage, Heidelberg 2016.

SCHMID JÜRG, Art. 975 ZGB, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Zivilgesetzbuch II, Art. 457-977 ZGB und Art. 1-61 SchlT ZGB, 5. Auflage, Basel 2015.

SCHMIDLIN BRUNO, Berner Kommentar, Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, Allgemeine Bestimmungen, Mängel des Vertragsabschlusses, Art. 23-31 OR, 2. Auflage, Bern 2013.

SCHULIN HERMANN, Art. 66 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

SCHÜTZ JÜRG G., Personengesellschaftsrecht (Art. 530-619 OR), Bern 2015.

SCHWARZ CLAUDIA/KRUSPIG SABINE, Computerimplementierte Erfindungen - Patentschutz von Software?, Köln 2018.

SCHWENZER INGEBORG, Art. 11, 13, 16, 23, 26, 27, 31 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

- Schweizerisches Obligationenrecht Allgemeiner Teil, 7. Auflage, Bern 2016.

SESTER PETER, Open-Source-Software: Vertragsrecht, Haftungsrisiken und IPR-Fragen, in : CR 12/2000, 797-807.

SHIER CHARLES/MEHAR MUHAMMAD IZHAR/GIAMBATTISTA ALANA/GONG ELGAR/SANAYHIE RYAN/KIM HENRY/LASKOWSKI MAREK, Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack, in: SSRN 3014782, 2017, abrufbar unter: <https://ssrn.com/abstract=3014782>.

SIXT ELFRIEDE, Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie, Wiesbaden 2017.

STEINAUER PAUL-HENRI/FOUNTOULAKIS CHRISTINA, Droit des personnes physiques et de la protection de l'adulte, Bern 2014.

STEINMETZ RALF/WEHRLE KLAUS, Peer-to-Peer-Networking & -Computing, in: Informatik Spektrum 27/1 2004, 51-54.

STOMMEL SEBASTIAN, Blockchain-Ökosysteme. Identitäts- und Zugangsmanagement zur Blockchain und angedockten Ökosystemen, in: DuD 1/2017, 7-12.

SWAN MELANIE, Blockchain. Blueprint for a new economy, Sebastpol 2015.

SWANSON TIM, Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management, 2014, abrufbar unter: <www.ofnumbers.com/the-guide>.

SZABO NICK, Smart Contracts, 1994, abrufbar unter: <www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.

- The Idea of Smart Contracts, 1997, abrufbar unter: <www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>.
- Formalizing and Securing Relationships on Publi Networts, 1997, abrufbar unter: <http://journals.uic.edu/ojs/index.php/fm/article/view/548/469>.

TAPSCOTT DON/TAPSCOTT ALEX, Blockchain revolution. How the technology behind bitcoin is changing money, business, and the world, New York 2016.

THÉVENOZ LUC, Art. 97, 100, 107 OR, in: Luc Thévenoz und Franz Werro (Hrsg.), Commentaire Romand, Code des obliagtions I, Art. 1-529 CO, 2. Auflage, Basel 2012.

THOUVENIN FLORENT, Vergleichs- und Bewertungsdienste: eine Analyse aus Sicht des Wettbewerbsrechts (UWG), in: Rolf H. Weber und Florent Thouvenin (Hrsg.), Werbung - Online, Zürich 2017, 131-160.

THOUVENIN FLORENT/STILLER BURKHARD/HETTICH PETER/BOCEK THOMAS/REUTIMANN KENTO, Keine Netzsperren im Urheberrecht, in: sic! 2017, 701-722.

TOSOVIC VLADIMIR, Der DAO-Hack - und die Konsequenzen für die Blockchain, in: Daniel Burgwinkel (Hrsg.), Blockchain Technology. Einführung für Business- und IT-Manager, Berlin/Boston 2016, 159-165.

VIGNA PAUL/CASEY MICHAEL J., The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order, New York 2015.

VOGT NEDIM PETER/VOGT ANNAIG L., Art. 239 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.

VONZUN RETO, Rechtsnatur und Haftung der Personengesellschaft, Basel 2000.

WEBER ROLF H., Berner Kommentar, Schweizerisches Zivilgesetzbuch, das Obligationenrecht, Allgemeine Bestimmungen, die Folgen der Nichterfüllung, Art. 97-109, Bern 2000.

- Freie Software - Befreiung vom Vertragstypenkonzept?, in: Friedrich Harrer u.a. (Hrsg.), Besonderes Vertragsrecht - aktuelle Probleme. Festschrift für Heinrich Honsell zum 60. Geburtstag, Zürich 2002, 41-57.
- Open Source Software: Vertragsgestaltung, Zürich 2003.
- E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Auflage, Zürich 2010.
- Art. 394 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, 6. Auflage, Basel 2015.
- Blockchain als rechtliche Herausforderung, in: Jusletter 18. Mai 2017.
- Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts, in: Jusletter 4. Dezember 2017.

WEBER ROLF H./JÖHRI YVONNE, Vertragsabschluss im Internet, in: Rolf H. Weber u.a. (Hrsg.), Geschäftsplattform Internet. Rechtliche und praktische Aspekte, Zürich 2000.

WEBER ROLF H./WAGNER ALEXANDER F., Corporate Governance auf der Blockchain, in: SZW 1/2017, 59-70.

WEBER ROLF H./WEBER ROMANA, Internet of Things. Legal Perspectives, Zürich 2009.

WERRO FRANZ, Introduction Art. 41-61, in: Luc Thévenoz und Franz Werro (Hrsg.), Commentaire Romand, Code des obligations I, Art. 1-529 CO, 2. Auflage, Basel 2012.

WIDMER MICHAEL, Der Softwarepflegevertrag, Zürich 2000.

WIDMER MIKE J., Open Source Software - urheberrechliche Aspekte freier Software, Bern 2003.

WIEGAND WOLFGANG, Art. 97, 98, 100, 101, 102, 107, 119 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art.1-529 OR, 6. Auflage, Basel 2015.

XOUDIS JULIA, Art. 13 OR, in: Luc Thévenoz und Franz Werro (Hrsg.), Commentaire Romand, Code des obliagtions I, Art. 1-529 CO, 2. Auflage, Basel 2012,

ZELLWEGER-GUTKNECHT CORINNE, Digitale Landeswährung - Ein Überblick. Elektronisch gebuchte und staatlich gedeckte Einlagen als Zahlungsmittel, in: Jusletter 31. Oktober 2016.

ZELLWEGER-GUTKNECHT CORINNE/BUCHER EUGEN, Art. 1, 4, 5, 7, 8, 9, 10 OR, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Obligationenrecht I, Art.1-529 OR, 6. Auflage, Basel 2015.

Materialienverzeichnis

BAFIN, Merkblatt zu Initial Coin Offering: Hinweisschreiben zur Einordnung als Finanzinstrumente vom 20. Februar 2018, abrufbar unter: <www.bafin.de>, Merkblätter.

BOTSCHAFT zur Totalrevision des Bundesgesetzes über die elektronische Signatur (ZertES) vom 15. Januar 2014, BBl 2014, S. 1001-1038.

BUNDESRAT, Bericht zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, abrufbar unter: <www.news.admin.ch>.

- Bericht über die zivilrechtliche Verantwortlichkeit von Providern vom 15. Dezember 2015, abrufbar unter: <www.ejpd.admin.ch>.

EUROPÄISCHE UNION, Richtlinie 2000/31/EG vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt («Richtlinie über den elektronischen Geschäftsverkehr»), ABl. EG Nr. L 178 vom 17. Juli 2000.

FINMA, Wegleitung für Unterstellunganfragen betreffend Initial Coin Offerings (ICOs) vom 16. Februar 2018, abrufbar unter: <www.finma.ch>, *Dokumente*.

Weitere Quellen

COMUNE DI CHIASSO, Comunicato Stampa (Medienmitteilung) vom 7. September 2017, abrufbar unter: <www.chiasso.ch>.

KANTON ZUG, Medienmitteilung der Volkswirtschaftsdirektion vom 2. November 2017, abrufbar unter: <www.zg.ch>.

SWISS INTERNET INDUSTRY ASSOCIATION SIMSA, Code of Conduct Hosting, 2013, abrufbar unter: <www.simsa.ch>.

SWISS LEGAL TECH ASSOCIATION SLTA, Data, Blockchain and Smart Contracts - Proposal for a robust and forward-looking Swiss ecosystem, 2018, abrufbar unter: <www.swisslegaltech.ch>.

WHITEPAPER ETHEREUM, A Next-Generation Smart Contract and Decentralized Application Platform, abrufbar unter: <https://github.com>, *Ethereum Whitepaper*.

WHITEPAPER HYPERLEDGER, Hyperledger Architecture, Volume 1, abrufbar unter: <www.hyperledger.org>.

Einleitung

Thema

Die sog. *Blockchain-Technologie* ist gegenwärtig kaum mehr aus der Medienberichterstattung wegzudenken; es kann sogar von einem regelrechten *Hype* gesprochen werden, der an die Ursprungszeiten des Internet erinnert. Dabei handelt es sich keineswegs um ein neues Phänomen: Die Vorläufer der heutigen Blockchain entstanden schon in den 90er Jahren. Die heute bekannte Ausgestaltung findet ihren Ursprung in der Bitcoin-Blockchain, die fast ausschliesslich als Plattform für die Schaffung von und den Handel mit Kryptowährungen eingesetzt wurde. Zwischenzeitlich sind zahlreiche weitere Anwendungsfelder erschlossen worden und die Technologie erfährt eine stete Weiterentwicklung. Mit Hilfe einer Blockchain können Vermögenswerte geschaffen und verschoben, Handel betrieben und Unternehmens-finanzierungen getätigt werden. Die rege Nutzung der Technologie wirft zahlreiche Fragen auf, welche auch das Recht beschlagen. 1

Die vorliegende Arbeit befasst sich mit einer privatrechtlichen Sicht auf die Blockchain-Technologie. Ihr Kern ist eine Auslegordnung derselben, mit einem besonderen Fokus auf *Smart Contracts* und deren Einordnung in das allgemeine Vertragsrecht. Auf weitere (zentrale) diskussionswürdige Punkte wie bspw. prozessuale Fragen, den Datenschutz oder konkursrechtliche Probleme wird vorliegend nicht eingegangen. Auch nicht behandelt wird die Einbettung von Dateneigentum in unsere Rechtsordnung. 2

Fragestellung

Im Zentrum der Arbeit steht die Frage, ob Smart Contracts als Verträge im Sinne des Obligationenrechts qualifiziert werden können und falls ja, ob die bestehenden gesetzlichen Grundlagen für diese Art von Vertrag ausreichende Handhabe bieten. 3

Vorgehen

Um die vorgenannte Frage zu beantworten, wird in einem ersten Teil die Blockchain-Technologie vorerst allgemein, dann aus technischer Sicht und anschliessend mit einer ersten vertragsrechtlichen Einordnung erläutert. Im zweiten Teil wird der Smart Contract untersucht und geprüft, ob die 4

allgemeinen Grundsätze zur Entstehung eines vertraglichen Verhältnisses auch auf Smart Contracts angewendet werden können. Abschliessend folgt eine Zusammenfassung der wichtigsten Erkenntnisse sowie eine Würdigung.

5 Die vorliegende Arbeit nähert sich dem Thema Blockchain und Smart Contracts auf einer generell-abstrakten Ebene, was nicht zuletzt darauf zurückzuführen ist, dass die Technologie noch verhältnismässig jung ist und noch kein Anwendungsfall einer gerichtlichen Auseinandersetzung bedurfte.

1. Teil: Grundlagen

Im ersten Teil der vorliegenden Arbeit wird in drei Kapiteln eine schrittweise Annäherung an die Blockchain-Technologie vorgenommen. Der erste Schritt besteht aus einer allgemeinen Einführung in die Technologie, die einen ersten Überblick verschaffen soll. Im darauf folgenden Kapitel wird die grundlegende Funktionsweise der Technologie dargelegt. Im dritten und letzten Abschnitt werden sodann die vertragsrechtlichen Aspekte der Blockchain-Technologie erörtert; dies betrifft einerseits die Blockchain als *Open-Source-Software* und andererseits die Blockchain als Plattform. Diese ersten vertragsrechtlichen Einschätzungen dienen als Grundlage für weitere Ausführungen im zweiten Teil, der sich ausschliesslich mit Smart Contracts beschäftigt. 6

A. Einführung in die Blockchain-Technologie

7 Die Blockchain-Technologie wurde im Detail erstmals im Zusammenhang mit der *Bitcoin*-Blockchain im Jahre 2008 beschrieben. Nachdem sie ein paar Jahre lang ein Mauerblümchendasein fristete und ausserhalb der IT-Branche kaum Beachtung fand, verhalf ihr die zunehmende Popularität von Bitcoin in den letzten Jahren zu mehr Bekanntheit.[1] Aber auch die Technologie hinter der Kryptowährung, die Blockchain-Technologie, ist zwischenzeitlich ins Bewusstsein der breiten Öffentlichkeit gerückt. Sie wird in einem hohen Tempo weiterentwickelt und Blockchain-Plattformen und Anwendungen, die auf der Technologie aufbauen, schiessen derzeit wie Pilze aus dem Boden.

8 Es lässt sich zwar nicht leugnen, dass sich aus den rasch voranschreitenden Weiterentwicklungen Vorteile für den Nutzer ergeben, doch ist ein regelrechter Wahn um die Technologie ausgebrochen, der bisweilen skurrile Blüten treibt. Es entstehen betrügerische Systeme, die bspw. mit Scheinkryptowährungen Anleger anlocken und mit ihren Aktivitäten Aufsichtsbehörden wie die Eidgenössische Finanzmarktaufsicht (FINMA) in Atem halten.[2] Findige Unternehmen machen sich die Blockchain-Euphorie zu Nutze: So ist der Aktienkurs von Long Island Iced Tea Ltd. um 500% in die Höhe geschnellt, nachdem die Geschäftsleitung beschlossen hatte, das Wort „Blockchain“ als Gag in den Firmennamen zu integrieren („Long Blockchain Ltd.“).[3]

9 Im folgenden Einführungsteil wird zunächst auf die Entstehungsgeschichte und den Begriff der Blockchain eingegangen, gefolgt von einer Auslegeordnung zwecks Konkretisierung der unterschiedlichen Merkmale der Technologie und

---

1 Der Begriff *Bitcoin* wird einerseits für die Einheit der Kryptowährung benutzt, andererseits aber auch für das Netzwerk (Plattform) und das Protokoll, vgl. ANTONOPOULOS, Mastering Bitcoin, 2; BERENTSEN/SCHÄR, Kryptoassets, 40.

2 Vgl. www.finma.ch/de/news/2017/09/20170919-mm-coin-anbieter/.

3 Vgl. www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/long-island-iced-tea-500-prozent-plus-durch-namensaenderung-in-long-blockchain/20767496.html.

einer Typologisierung. Abschliessend wird auf den Vertrauensaspekt eingegangen, der in der Blockchain-Technologie eine zentrale Rolle einnimmt.

I. Historie und Begriff

Nachfolgend wird zuerst auf die Bitcoin-Blockchain, die Pionierin unter den Blockchain-Plattformen, und sodann auf neuere Entwicklungen eingegangen. Da die Technologie und ihre Anwendungsmöglichkeiten sich in einem rasanten Tempo weiterentwickeln, kann in dieser Übersicht nicht jede Neuerung berücksichtigt werden. 10

1. Die Bitcoin-Blockchain

Das technische Konzept der Blockchain, das heute verbreitet Anwendung findet und als Grundlage für Weiterentwicklungen dient, tauchte erstmals im Jahr 2008 im Bitcoin-Whitepaper[4] von SATOSHI NAKAMATO[5] auf, in dem die Funktionsweise der Bitcoin-Blockchain im Detail erläutert wird. 11

Immer wenn sich eine neue, vielversprechende Technologie durchsetzt, stellt sich die Frage, welche Neuerung oder welcher Nutzen durch diese Technologie zu erwarten ist, resp. für welche Problematik sie eine Lösung bietet. Im Hinblick auf die Bitcoin-Blockchain kann die Antwort wie folgt lauten: Für die Abwicklung von Geschäften, ob im virtuellen Raum oder im „realen Leben“, ist heute meist eine zwischengeschaltete, vertrauenswürdige Instanz erforderlich. Wer beispielsweise eine Geldüberweisung tätigen will, vertraut seiner Bank als Intermediär. Die Bank verwaltet Kundengelder und waltet gleichzeitig als vertrauenswürdige Instanz, die überprüft, ob ein Betrag nicht bereits ausgegeben wurde. Vertrauenswürdige Instanzen generieren allerdings 12

---

4 Ein Whitepaper wird in der Regel bei Informatikprojekten erstellt. Das jeweilige Projekt wird mit Worten und Auszügen aus dem Code beschrieben.

5 SATOSHI NAKAMATO ist ein Pseudonym – es ist bis heute nicht bekannt, wer sich hinter diesem Namen verbirgt.

Aufwand und verursachen Kosten für die Nutzer.[6] Mit dem Bitcoin-Whitepaper stellte NAKAMATO nun erstmals ein System vor, das zwischenparteiliche Transaktionen ohne Intermediär – weder in der Form einer Abwicklungsplattform noch einer Vertrauensinstanz – ermöglicht.[7] Es wird mithin argumentiert, die Intention hinter der Bitcoin-Blockchain sei es, den (technologischen) Grundstein für einen intermediärsfreien Wirtschaftskreislauf zu legen, da sie ohne Individuum oder Unternehmen auskommt, das die Verantwortung für das System trägt oder seine Funktionalität sicherstellt. Es handelt sich um ein kompliziertes, mehrschichtiges System, in dem die Teilnehmer einander hierarchisch gleichgestellt sind und das so ausgelegt ist, dass betrügerisches Verhalten keinen Vorteil bringt.[8]

13 Die Bitcoin-Blockchain wurde primär für Transaktionen mit der Kryptowährung Bitcoin entwickelt. Weitere Anwendungsmöglichkeiten (z.B. das Mitsenden einer Zusatzinformation nebst der Kryptowährung) sind aufgrund der technischen Ausgestaltung nur in sehr beschränktem Mass möglich.

2. Neuere Entwicklungen

14 Seitdem vor rund zehn Jahren die Grundlagen der Bitcoin-Blockchain im erwähnten Whitepaper veröffentlicht wurden, hat sich viel getan. Insbesondere ist eine Entwicklung hin zu Business-Blockchain-Lösungen zu beobachten, die sich von der Grundidee, auf Intermediäre zu verzichten und ein vertrauensloses Netzwerk (N 24, 39 ff.) aufzubauen, mitunter weit entfernen. Es gibt zwischenzeitlich Blockchain-Plattformen, die im Vergleich zur Bitcoin-Blockchain eine grössere Speicherkapazität aufweisen und somit auch die Integration von weiteren Anwendungen zulassen, wie dies bspw. bei der Ethereum-Blockchain möglich ist.

---

6 Vgl. TAPSCOTT/TAPSCOTT, Blockchain Revolution, 3 ff.

7 NAKAMATO, Bitcoin Whitepaper, 1.

8 Vgl. BERENTSEN/SCHÄR, Kryptoassets, 71.

Aus den Entwicklungen der letzten Jahre haben sich zwei Grundströmungen herauskristallisiert. Einerseits gibt es die öffentlichen Blockchain-Plattformen, die an den Grundidealen des intermediärsfreien, öffentlichen und transparenten Netzwerks festhalten. Doch auch hier ist zu beobachten, dass die Nutzer mehrheitlich von Profitstreben geleitet sind und die Blockchain-Technologie nicht einzig und alleine idealistische Zwecke verfolgt. So herrscht bspw. in der Bitcoin-Community seit längerer Zeit Uneinigkeit über die künftige Ausrichtung und Weiterentwicklung der Plattform. Einerseits sind die Grössenbeschränkung pro Block sowie die Transaktionskadenz Gegenstand der Diskussionen, andererseits wird auch die Rolle der sog. *Miner*[9] (vgl. nachfolgend N 101 ff.), also derjenigen Teilnehmer, die mit ihrer Rechenleistung Transaktionen validieren, kontrovers diskutiert.[10] Der Zwist hat sich in mehreren Spaltungen der Plattform manifestiert; zwischenzeitlich wurde bspw. Bitcoin durch Bitcoin-Cash und Bitcoin-Gold (diese wiederum durch weitere Bitcoin-Abspaltungen wie bspw. Bitcoin Diamond) ergänzt.[11] Ob die Abspaltungen monetären Interessen geschuldet sind oder tatsächlich ideeller Natur sind, ist umstritten.[12] 15

Parallel zur originären Blockchain-Community gibt es eine starke Bewegung, die blockchainbasierte Anwendungen und Plattformen schafft, die auf Unternehmen zugeschnitten sind. So verzichten diese bspw. auf 16

---

9 Als ein Miner wird ein Teilnehmer einer Blockchain bezeichnet, der seine Rechenleistung für das Konsensverfahren zur Verfügung stellt und dafür vergütet wird (vgl. N 61 ff., 179, 181).

10 Zum Validierungsprozess vgl. nachfolgendes Kapitel B.I.2., N 61 ff.

11 Vgl. zu den *Forks* der Bitcoin-Blockchain vgl. www.nzz.ch/finanzen/bitcoin-rekord-aber-abspaltungen-verunsichern-die-investoren-ld.1325385.

12 Der Kurs von Bitcoin-Cash ist nach der Spaltung kontinuierlich gestiegen; die Kryptowährung hat sich zwischenzeitlich etabliert. Da jeder Bitcoin-Besitzer automatisch auch Bitcoin-Cash-Besitzer wurde, haben viele Teilnehmer von der Spaltung profitiert. Die kurz darauffolgende Spaltung in Bitcoin-Gold wurde daher eher mit Profitstreben als mit Idealismus (Wiederherstellung der Dezentralität durch Vermeidung von Miningpools, vgl. https://bitcoingold.org) in Verbindung gebracht. Selbiges gilt für jede weitere (Ab-) Spaltung, wie bspw. die Spaltung in Bitcoin Diamond.

Pseudoanonymität (vgl. N 28 ff.) und volle Transparenz und ermöglichen die Einhaltung von regulatorischen Vorgaben. Namhafte Software- und Computerhersteller wie bspw. *IBM* oder *Microsoft* haben in jüngster Vergangenheit Blockchain-Plattformen und -Applikationen als Unternehmenslösungen entwickelt. Auch in der Schweiz ist eine ähnliche Entwicklung zu beobachten: *Swisscom* hat spezifisch für Unternehmen eine Blockchain-Plattform und Anwendungen dafür geschaffen und bietet sich als zentraler Blockchain-Dienstleister an.[13]

17 Der Fokus liegt sowohl bei den öffentlichen als auch geschlossenen Plattformen und Anwendungen nicht mehr nur auf Kryptowährungen: Der Einsatz der Technologie schliesst u.a. auch Verträge (Smart Contracts, vgl. N 211 ff.), Unternehmensfinanzierungen (sog. *Initial Coin Offerings ICO*, vgl. Anhang, N 35 ff.) oder die Abbildung und administrative Vereinfachung von komplexen Abläufen, wie bspw. in der Logistik, mit ein.

18 Selbst die bei der Blockchain-Technologie ursprünglich im Fokus stehenden Finanzintermediäre, die dank der Technologie überflüssig werden sollen, investieren grosse Beträge in die Weiterentwicklung der Technologie. So haben Schweizer Banken[14] federführend an der Schaffung des *Utility Settlement Coin (USC)* mitgewirkt, der den Interbanken-Zahlungsverkehr sowie das *Clearing* und *Settlement* einfacher und kostengünstiger gestalten soll.

19 Nicht nur Unternehmen sind an der Blockchain-Technologie interessiert. Auch Staaten und Behörden sind daran, die Technologie ihren Interessen anzupassen. So hat beispielsweise Venezuela einen sog. *Petro-Token (PTR)* ausgegeben, der mit Erdöl abgesichert ist und dem Land so aus der Schuldenkrise helfen soll.[15] Wiederum andere Länder sind daran, ihre Grundbücher mit Hilfe dieser Technologie vertrauenswürdiger und manipulationssicher auszugestalten.[16]

---

13 Swisscom-Blockchain, vgl. https://blockchain.swisscom.com/.

14 U.a. *UBS* und *Credit Suisse*.

15 Vgl. www.elpetro.gob.ve.

16 Z.B. Georgien, das bereits sein Grundbuch auf Blockchain umgestellt hat, oder Schweden, das noch in der Pilotphase steckt, vgl. https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-

3. Definition

Aufgrund dieser dynamischen Entwicklung ist heute nicht klar zu umreissen, was eine Blockchain ausmacht und wie sie zu definieren ist. Da die Bitcoin-Blockchain die erste ihrer Art war und einen hohen Bekanntheitsgrad aufweist, wird sie oft pars pro toto stellvertretend für alle Blockchains erwähnt. Auch in der vorliegenden Arbeit wird als Ausgangsbeispiel häufig die Bitcoin-Blockchain herangezogen. Sie ist einerseits die Pionierin unter den Blockchains, andererseits weist sie dank ihrer knapp zehnjährigen Laufzeit auch eine gewisse Beständigkeit auf und ist damit auch Gegenstand von wissenschaftlichen Auseinandersetzungen geworden. Grundlegend für das Verständnis ist aber, dass Blockchains nicht mit Kryptowährungen gleichzusetzen sind. Kryptowährungen sind lediglich ein Anwendungsfall der Technologie.[17] 20

Der Begriff *Blockchain* wird je nach Kontext unterschiedlich verstanden und eingesetzt; *Blockchain* kommt also gewissermassen die Rolle eines Sammelbegriffes zu. Es empfiehlt sich für ein differenziertes Verständnis, die Blockchain gemäss ihren Funktionen zu differenzieren.[18] Zu unterscheiden ist grundsätzlich zwischen der Blockchain als technisches Konzept, der Blockchain als Software und der Blockchain als Plattform.[19] Das technische Konzept meint die Technologie an sich. Unter Blockchain als Software ist einerseits der Quellcode für die Blockchain-Plattformen zu verstehen, worunter auch die verschiedenen Softwarecodes subsumiert werden, die auch für weitergehende Anwendungsmöglichkeiten (z.B. Smart Contracts [N 211 ff.] oder verschiedene Formen von Token [N 30 ff.]) einsetzbar sind.[20] Schliesslich kann die Blockchain als Plattform generell als die Infrastruktur bezeichnet werden, die durch das Netzwerk (N 24) betrieben wird. 21

---

to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#7e19589b4dcd.

17 Vgl. KAULARTZ, Blockchain Technologie, 474.

18 Vgl. BURGWINKEL, Blockchain Technology, 3 ff.

19 Ausführlich BURGWINKEL, Blockchain Technology, 5.

20 Vgl. BURGWINKEL, Blockchain Technology, 9 f.

22 Vereinfacht und definierend kann eine Blockchain als Datenbank, als eine Aneinanderreihung von Datensätzen bezeichnet werden, die in Blöcken zusammengefasst und sequentiell miteinander verknüpft werden,[21] basierend auf einem dezentralen, verteilten Netzwerk.[22]

4. Merkmale

23 Die Blockchain-Technologie unterscheidet sich durch das Zusammenspiel von technischen und funktionellen Merkmalen von anderen, bereits bestehenden Technologien. Als besondere Merkmale gelten das dezentrale, verteilte Netzwerk, das Transaktionsregister (die Datenbank), die Unveränderbarkeit der registrierten Daten sowie die Pseudoanonymität der Teilnehmer.

a) Dezentrales, verteiltes Netzwerk

24 Ein zentrales Element einer Blockchain ist das Netzwerk.[23] Es handelt sich um ein *Peer-to-Peer* (*Person-to-Person*, *P2P*)-Netzwerk[24] mit einer verteilten und dezentralen Architektur. Dezentral bedeutet hier, dass das Netzwerk von Teilnehmern, die ihre Rechenleistung und Speicherkapazität zur Verfügung stellen, betrieben wird.[25] Gleichzeitig sind die einzelnen Knotenpunkte des Netzwerkes (*Nodes*) untereinander vernetzt, wobei die Teilnehmer untereinander gleichgestellt sind.[26] Durch ihre verteilte Struktur sind dezentrale Netzwerke besonders gut gegen Angriffe und Ausfälle geschützt, da jeder

---

21 BERENTSEN/SCHÄR, Kryptoassets, 199; BURGWINKEL, Blockchain Technology, 5 f.; GERVAIS, Blockchains, 128; SWAN, Blockchain, X (Preface).

22 Vgl. WEBER, Blockchain, N 1.

23 Vgl. ANTONOPOULOS, Mastering Bitcoin, 139; HANCOCK/VAIZEY, Distributed Ledger, 17; KAULARTZ, Blockchain Technologie, 475.

24 Ausführlich zu P2P-Netzwerken: DUNKEL U.A., System-Architekturen, 141 ff.

25 MOUGAYAR, Business Blockchain, 6.

26 BERENTSEN/SCHÄR, Kryptoassets, 95; ENGELHARDT, Urheberrechtsverletzungen, 25 f.; vgl. MEYER/SCHUPPLI, Smart Contracts, 206.

Teilnehmer ersetzbar ist, ohne dass es zu Datenverlusten kommt.[27] Änderungen am System sind grundsätzlich nur mit einer Teilnehmermehrheit durchführbar, eine Aktualisierung kann nur durch die Betreiber der Knotenpunkte (Teilnehmer) selbst vorgenommen werden.[28]

b) Transaktionsregister

25 Die Blockchain speichert Transaktionsdaten, d.h. sie zeichnet auf, wem was zu welchem Zeitpunkt gehört; sie ist – wie bereits angedeutet – ein Transaktionsregister.[29] Welche Art von Daten im Einzelfall gespeichert wird, ist dabei irrelevant.

26 Häufig taucht in der Beschreibung der Technologie die Bezeichnung *Distributed Ledger* auf. Eine prägnante deutsche Übersetzung des Begriffes ist derzeit nicht in Gebrauch. Wörtlich übersetzt bedeutet Distributed Ledger etwa *verteiltes Kontobuch*, oder in einer eher deskriptiven Deutung, *dezentrales Transaktionsregister*.[30] Der Ledger ist ein (IT-basiertes) System, in dem die Bewegungen (egal ob monetärer Art oder nicht) aufgezeichnet werden. So stellt beispielsweise ein bankinternes System, das Aufzeichnungen über Kontobewegungen führt, ebenfalls ein Ledger dar.[31] Je nach Autor werden die Begriffe *Blockchain* und *Distributed Ledger* synonym verwendet[32] oder die Blockchain als eine Unterart der Distributed Ledger-Technologie verstanden.[33] Vereinzelt wird auch der Begriff *Kryptoledger* benutzt,[34] wobei die kryptografische Verschlüsselungstechnik, ein wesentliches Merkmal der Blockchain, hervorgehoben wird. In der vorliegenden Arbeit wird Blockchain als eine Anwendung (Unterart) der Distributed-Ledger-Technologie

---

27 BERENTSEN/SCHÄR, Kryptoassets, 96.

28 Für das Bitcoin-Netzwerk vgl. ANTONOPOULOS, Mastering Bitcoin, 139 ff.; BERENTSEN/SCHÄR, Kryptoassets, 194.

29 ANTONOPOULOS, Mastering Bitcoin, 161; HESS/LIENHARD, Übertragung von Vermögenswerten, N 1.

30 iso-20022.ch, www.iso-20022.ch/lexikon/distributed-ledger-technology/.

31 HANCOCK/VAIZEY, Distributed Ledger, 33 ff.

32 SWANSON, Great Chain, 16 ff.

33 EGGEN, Chain of Contracts, 5.

34 SWANSON, Great Chain, 16.

verstanden. Nachfolgend wird ausschliesslich der Begriff *Blockchain* verwendet.

c) Unabänderbarkeit der registrierten Daten

27 Aufgrund der kryptografischen Verschlüsselungstechnik und der verteilten und dezentralen Struktur ist es (bis zum heutigen Zeitpunkt) nicht möglich, einmal gespeicherte Daten nachträglich abzuändern oder zu löschen.[35] Eine „Änderung“ von Informationen muss durch eine neue Transaktion erfolgen. Die einzelnen Blöcke sind sequentiell verkettet, was die zeitliche Reihenfolge und auch die Integrität der gesamten Daten sicherstellt.[36] Die gespeicherten Daten sind für die Teilnehmer des Netzwerks aufgrund der öffentlichen Zugänglichkeit jederzeit nachvollziehbar. Es kann also zu jeder Zeit nachgeprüft werden, zu welchem Zeitpunkt welche Transaktion auf der entsprechenden Blockchain gespeichert wurde.[37]

d) Pseudoanonymität

28 Da der Nutzer einer öffentlichen Blockchain nicht seinen realen Namen offenlegen muss,[38] könnte auf ein auf Anonymität beruhendes System geschlossen werden. Es ist jedoch vielmehr von einer Pseudoanonymität auszugehen: Jedem Teilnehmer einer Blockchain wird eine Pseudoidentität in Form einer Adresse zugewiesen.[39] Diese besteht aus einer Abfolge von Buchstaben und Zahlen.[40] Je nach Netzwerk werden Adressen pro Transaktion oder laufend vergeben.[41] Werden die Adressen nicht bei jeder Transaktion

---

35 Vgl. HESS/LIENHARD, Übertragung von Vermögenswerten, N 4.

36 BURGWINKEL, Blockchain Technology, 5 f.; MOUGAYAR, Business Blockchain, 5 ff.

37 ANTONOPOULOS, Mastering Bitcoin, 111 ff.; BURGWINKEL, Blockchain Technology, 21 Tab.7.

38 Vgl. SIXT, Transaktionssysteme, 33.

39 SIXT, Transaktionssysteme, 33.

40 KAULARTZ, Blockchain Technologie, 475.

41 SIXT, Transaktionssysteme, 33; für die Adressen in der Bitcoin-Blockchain vgl. ausführlich ANTONOPOULOS, Mastering Bitcoin, 64 ff.; BERENTSEN/SCHÄR, Kryptoassets, 126 ff.

gewechselt, besteht die Gefahr, dass Transaktionsmuster eruiert werden können und daraus auf die Identität einer Person geschlossen werden kann.[42]

29 Bei öffentlichen Blockchains, wie bspw. der Bitcoin- oder Ethereum-Blockchain, müssen sich die Teilnehmer grundsätzlich nicht identifizieren, um am Netzwerk teilzunehmen. Die durch das System zugewiesene Identität lässt für sich alleine keine Rückschlüsse auf die wahre Identität eines Nutzers zu.[43] Es steht den Teilnehmern jedoch frei, bei einem allfälligen Handel untereinander mehr Informationen oder gar einen Identitätsnachweis zu verlangen.[44] Bei privaten Blockchains steht die Frage nach Anonymität oder Pseudoanonymität nicht im Vordergrund, da dieser Aspekt gerade durch einen geschlossenen Teilnehmerkreis verhindert werden kann, resp. verhindert werden möchte (vgl. N 35).

30 Oft geschieht im Zusammenhang mit der Blockchain eine Identifizierung beim „Eintritt“ in die virtuelle Welt, bspw. mit dem Erwerb einer Kryptowährung bei einer entsprechenden Börse oder einem Händler oder beim „Austritt“, wenn Kryptowährung gegen Fiat-Währung[45] getauscht wird.[46] Der Kauf und Verkauf von virtuellen Währungen untersteht den Geldwäschereibestimmungen, d.h. die Käufer oder Verkäufer von Kryptowährungen werden von den Händlern

---

42 BERENTSEN/SCHÄR, Kryptoassets, 129; SIXT, Transaktionssysteme, 33.

43 BOEHM/PESCH, Bitcoins, 76; ISLER, Datenschutz auf der Blockchain, N 4; KAULARTZ, Blockchain Technologie, 479.

44 Vgl. SIXT, Transaktionssysteme, 155.

45 Als Fiat-Geld oder Fiat-Währung werden diejenigen Währungen bezeichnet, die von einer Zentralbank ausgegeben werden und als offizielles Zahlungsmittel anerkannt sind, bspw. Schweizer Franken, Euro oder Dollar.

46 Um eine Identifizierung zu umgehen, bestehen auch hier spezialisierte Dienste, die einen Wechsel in eine Fiat-Währung via eine Drittperson anbieten, z.B. https://localbitcoins.com/ (Person in der Nähe wechselt Bitcoins in Fiat-Währung und übergibt diese in Bargeld an den Auftraggeber).

oder Börsen identifiziert.[47] Daraus schliesst sich, dass, sobald eine Verbindung zwischen der realen und der virtuellen Welt besteht (z.B. A wechselt seine Bitcoins in Schweizer Franken), eine Identifizierung unumgänglich ist. Es ist mit technischem Know-how auch möglich, über zugewiesene (Blockchain-) Adressen Rückschlüsse auf die verwendeten Geräte, IP-Adressen, Mailadressen oder gar die Identität zu ziehen.[48] Davor bieten auch sog. Mixer-Dienste, die bspw. Bitcoin-Nutzern helfen sollen, ihre wahre Identität zu verschleiern, nicht abschliessende Sicherheit.[49]

31 Insgesamt kann festgehalten werden, dass eine Pseudoanonymität besteht, die nicht mit „echter" Anonymität verwechselt werden darf. Global betrachtet sind Rückschlüsse auf die Identität der Nutzer auch bei öffentlichen Blockchains möglich.

II. Typologie

32 Wie bereits eingangs erwähnt, können zwei Arten von Blockchains unterschieden werden: öffentliche, jedermann zugängliche Blockchains und private Blockchains, bei denen der Teilnehmerkreis geschlossen ist.[50] Zu beachten ist ausserdem, dass Mischformen oder Kombinationen von öffentlichen und geschlossenen Systemen existieren.

---

47 BUNDESRAT, virtuelle Währungen, 15; GRÜNEWALD, Währungs- und geldschwäschereirechtliche Fragen, 105 ff; SIXT, Transaktionssysteme, 33.

48 ISLER, Datenschutz auf der Blockchain, N 4; SIXT, Transaktionssysteme, 155; vgl. Untersuchung von Wissenschaftlern der Universität Luxemburg, die eine Methode zur Eruierung von IP-Adressen untersuchten, von welcher aus Bitcoin-Transaktionen generiert wurden: https://arxiv.org/pdf/1405.7418.pdf.

49 SIXT, Transaktionssysteme, 156.

50 Vgl. HANCOCK/VAIZEY, Distributed Ledger, 18.

1. Öffentliche Blockchain

Eine offene oder öffentliche (*public*) Blockchain zeichnet sich dadurch aus, dass sie einer unbestimmten, nicht vordefinierten Anzahl von Teilnehmern offensteht. Hin und wieder wird diese Art von Blockchain auch *Unpermissioned Ledger* genannt. Diese wird weder von einer verantwortlichen Person noch einem Unternehmen erstellt oder geleitet und die Teilnehmer sind untereinander grundsätzlich gleichgestellt.[51] 33

Ein solches Blockchain-Netzwerk kann nicht zensuriert und nur sehr schwer manipuliert werden, da jeder Teilnehmer jederzeit neue Transaktionen ausführen kann und sämtliche Informationen verteilt, dezentral und laufend synchronisiert gespeichert werden (vgl. nachfolgend N 53 ff.).[52] Beispiele für diese Art von Blockchain sind die Bitcoin-Blockchain und das Ethereum-Netzwerk. 34

2. Private Blockchain

Eine private oder geschlossene Blockchain ist, wie der Name schon sagt, nicht öffentlich und steht nur einer bestimmten Teilnehmergruppe zur Verfügung. Je nach Ausgestaltung ist innerhalb dieser Gruppe jeder Teilnehmer gleichberechtigt oder eine Instanz (z.B. eine Auswahl von Teilnehmern) steuert die Blockchain und sorgt für deren Integrität. Teilweise wird auch von Konsortiums-Blockchain gesprochen, wenn ein bestimmter Teilnehmerkreis eine Blockchain betreibt, der sich bereits vertraut. Eine geschlossene Blockchain, die von einer vordefinierten Teilnehmergruppe kontrolliert wird, ähnelt stark den heute bestehenden Systemen – der Unterschied liegt wohl einzig in der verwendeten Technologie. 35

36

[51] Vgl. SIXT, Transaktionssysteme, 31.

[52] HANCOCK/VAIZEY, Distributed Ledger, 17.

Blockchain-Puristen oder *Kryptoanarchisten*[53] würden hier einwenden, dass einzig eine öffentliche Blockchain eine „echte“ Blockchain sei, da es schon lange vor NAKAMATOS Bitcoin-Whitepaper verteilte Netzwerksysteme für geschlossene Teilnehmerkreise gab und bei geschlossenen Systemen gerade die vorherrschenden Merkmale der Blockchain-Technologie (Dezentralität und Verzicht auf Vertrauen in Gegenparteien) fehlen. Auf diese Diskussion wird aber in der vorliegenden Arbeit nicht eingegangen und auch die private Blockchain als Blockchain interpretiert und in die Betrachtungen einbezogen.

3. Mischformen

37 Es sind Mischformen mit Elementen öffentlicher und privater Blockchains oder Systeme bekannt, die je nach Funktionalität zwischen einer geschlossenen und einer öffentlichen Plattform hin- und herpendeln oder beide Systeme in eine Anwendung integriert haben. So gibt es bspw. Plattformen, die zwar jedermann zugänglich sind, die aber von einer bestimmten Teilnehmergruppe kontrolliert werden.[54] Diese Kontroll-Gruppe ist entweder vorbestimmt oder wird in einem Validierungsprozess durch die Teilnehmer eingesetzt; sie ist für die Integrität der Blockchain besorgt.[55]

III. Vertrauen und die Blockchain

38 Als treibendes Element und eigentliche konzeptionelle Innovation der Blockchain-Technologie ist der Vertrauensaspekt zu erwähnen: Mit der

---

53 Kryptoanarchisten nennt man die Generation von Anarchisten, die die Staatsmacht mit Hilfe der Technologie auszuhebeln versuchen. Die Bitcoin-Blockchain wurde u.a. auch mit diesem Grundgedanken entwickelt.

54 HANCOCK/VAIZEY, Distributed Ledger, 17.

55 Ein Beispiel für diese Art von Blockchain ist Ripple, ein globales Zahlungsausgleichssystem; vgl. HANCOCK/VAIZEY, Distributed Ledger, 19 (Abbildung).

Blockchain wurde ein System geschaffen, das ohne das Vertrauen der Parteien auskommt (*Trustless System*).

39 Grundidee der öffentlichen Blockchain ist die Überwindung des Vertrauensaspektes, der im täglichen Wirtschaftsleben eine zentrale Rolle einnimmt. Wir gehen Verträge mit Parteien ein, von denen wir annehmen, dass sie das Vereinbarte einhalten werden. Dies beruht auf der Reputation einer Partei, der staatlichen Überwachung oder der persönlichen Bekanntschaft. Auch im Schweizer Recht spielt der Vertrauensaspekt eine zentrale Rolle. Man denke bspw. an den Grundsatz von Treu und Glauben, der für die gesamte Rechtsordnung gilt (vgl. Art. 5 Abs. 3 BV, vgl. nachfolgend N 47).[56]

40 Durch die technische Möglichkeit, Daten unveränderbar, dezentral und verteilt zu speichern, muss bei einer Blockchain keiner Gegenpartei mehr vertraut werden, sondern einzig und allein der Technologie. Es findet also eine Verlagerung der Vertrauensrolle von etablierten Unternehmen und Institutionen hin zu einer Technologie und damit ein Paradigmenwechsel statt.[57]

41 Bei einer genaueren Betrachtung der Technologie und ihrer Anwendungsfälle ist jedoch zu beobachten, dass bekannte Intermediäre, wie bspw. Banken, zwar nicht mehr benötigt werden, aber dafür neue Intermediäre (z.B. *Wallet-Anbieter*, vgl. N 44) erforderlich werden, um die Technologie für die breite Masse nutzbar zu machen.

1. Vertrauen in der öffentlichen Blockchain

42 Durch den Wegfall des Vertrauensaspektes erhoffen sich die Nutzer von offenen Blockchains intermediärsfreie P2P-Anwendungen. Für die idealistisch geprägten Nutzer einer öffentlichen Blockchain ist die Blockchain ohne dieses basisdemokratische Element bedeutungslos. Aber auch weniger idealistischen

---

56 Vgl. EPINEY, BSK BV, Art. 5 N 1 ff.; HONSELL, BSK ZGB I, Art. 2 N 4.

57 Zum Vertrauensaspekt MOUGAYAR, Business Blockchain, 29 ff.; SWANSON, Great Chain, 16 f.; TAPSCOTT/TAPSCOTT, Blockchain Revolution, 3 ff.

Nutzern wird der Wegfall von Intermediären nur schon aus Kostengründen entgegenkommen.

43 Bei einer öffentlichen Blockchain wird das Vertrauen durch die unzähligen Betreiber der Rechnerknoten begründet. Durch sie wird gewährleistet, dass das System nicht von einem einzigen Markteilnehmer abhängig ist. Es ist jedoch zu beobachten, dass sich durch die (teilweise) Konzentration von Minern (*Mining-Farmen* etc.), wie beispielsweise bei der Bitcoin-Blockchain, dieses basisdemokratisch verteilte Vertrauen nun doch wieder vermehrt auf einige zentrale Akteure konzentriert, die für das Netzwerk unabdingbar sind.

44 Der Vertrauensaspekt erleidet bei öffentlichen Blockchains noch eine weitere Schwächung: Um eine öffentliche Blockchain wie bspw. Bitcoin oder Ethereum für die Allgemeinheit zugänglich zu machen, sind wiederum Intermediäre notwendig. Will ein Nutzer nicht die gesamte Blockchain bei sich abspeichern, ist er bspw. auf einen sog. Wallet-Anbieter (N 104 ff.) angewiesen, der für ihn die *Private Keys* aufbewahrt und den Zugang zur Blockchain sicherstellt.[58] Faktisch sind also die bekannten Intermediäre weggefallen und lediglich durch andere ersetzt worden. So wird bspw. nicht mehr einer Bank vertraut, dass sie Geld oder andere Vermögenswerte sicher aufbewahrt, sondern es werden die erworbenen Vermögenswerte (z.B. Kryptowährung) einem Wallet-Anbieter anvertraut (der in den meisten Jurisdiktionen keiner Aufsicht untersteht[59]). Dies widerspricht eigentlich dem Leitmotiv vieler Blockchain-Plattform-Nutzer, die eine Blockchain gerade aufgrund des Wegfalls von Intermediären nutzen. Durch das Aufkommen neuer Intermediäre, welche die Technologie für die breite Masse nutzbar machen, wird der zentrale Aspekt der Blockchain-Technologie, ein vertrauensloses System zu etablieren, gewissermassen ad absurdum geführt.

58 Vgl. Kapitel C.III.4., N 198 ff.

59 Für die Schweiz siehe FINMA, Wegleitung ICO, 7.

2. Vertrauen in der privaten Blockchain

Eine private Blockchain wird durch ein in der Grösse begrenztes Netzwerk oder einen Anbieter betrieben. Es kann sich dabei um ein Konsortium handeln, dessen Teilnehmer das Netzwerk nach den gemeinsam definierten Regeln betreiben. Hier stützt sich das Vertrauen auf die geschlossene Gemeinschaft, mit deren Teilnehmern die private Blockchain initiiert wurde. Wird eine Plattform benutzt, die von einem Anbieter betrieben und unterhalten wird, dann kann nicht mehr von einem Trustless System gesprochen werden, da einem einzigen Marktakteur – dem Betreiber der Plattform – vertraut wird. 45

3. Vertrauen im Schweizer Rechtssystem

Das Vertrauen spielt auch im Recht eine sehr zentrale Rolle. Einerseits sorgt der Staat durch die Schaffung von Aufsichtsrecht und der daraus resultierenden Beaufsichtigung von Unternehmen oder Berufsgruppen dafür, dass Bürger oder Marktteilnehmer gewissen Institutionen und Berufsgruppen vertrauen können. Das betrifft bspw. Banken, Pharmaunternehmen oder einige regulierte Berufe wie bspw. Ärzte oder Rechtsanwälte. 46

Vertrauen ist auch ein zentraler Aspekt des Privatrechts. Grundstein des Schweizerischen Privatrechts ist der Grundsatz von Treu und Glauben (Art. 2 ZGB).[60] Ausfluss des Prinzips von Treu und Glauben ist das Vertrauensprinzip bei der Auslegung von Willenserklärungen.[61] So werden bei unbewiesenem übereinstimmendem Willen der Vertragsparteien die Willenserklärungen nach dem Vertrauensprinzip ausgelegt. Demnach ist eine Willenserklärung so zu verstehen, wie sie vom Empfänger gemäss Wortlaut, im Zusammenhang und nach den gesamten Umständen in guten Treuen verstanden werden durfte und 47

60 Ausführlich HONSELL, BSK ZGB I, Art. 2 N 13 ff.

61 BERGER, Allgemeines Schuldrecht, N 708; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 211; HONSELL, BSK ZGB I, Art. 2 N 13; SCHWENZER, OR AT, N 27.41.

musste.[62] Bei Vertragsschluss spielt das Vertrauen in die Person der Gegenseite eine wichtige Rolle. Einer Vertragspartei „mit gutem Namen“ wird eher vertraut als mit einer Person, die gänzlich unbekannt ist oder deren Ruf nicht frei von Zweifeln bezüglich Integrität und/oder Bonität ist.

4. Vertrauenslose Systeme im Schweizer Rechtssystem

48 Systeme wie eine Blockchain können gewisse Aufgaben, die heute der Staat übernimmt, erleichtern oder situativ auch erschweren. So kann es sein, dass heute beaufsichtigte Intermediäre, insbesondere im Finanzmarktbereich, wegfallen und gegebenenfalls durch ein vertrauensloses System, wie bspw. eine öffentliche Blockchain, ersetzt werden. Wie jedoch bereits ausgeführt, kommen dafür neue Akteure auf den Markt, die je nach Tätigkeit zur Wahrung der Marktintegrität und des Schweizer Wirtschaftssystem zu beaufsichtigen sind.

49 Ob ein vertrauensloses System auch Auswirkungen auf die Grundprinzipien des Vertragsrechtes haben kann, ist aus heutiger Sicht schwer abzuschätzen; dies nicht zuletzt auch deshalb, weil die Technologie einer steten Entwicklung unterworfen ist und es noch nicht viele Anwendungsfälle gibt. Auch ist hervorzuheben, dass der Vertrauensaspekt im Privatrecht zwei Seiten hat. Auf der einen Seite dient das Vertrauensprinzip der Auslegung von Verträgen. Durch die Automatisierung von Verträgen mit Hilfe der Blockchain-Technologie (Smart Contracts, N 214 ff.) findet zwar eine Verfestigung des Grundsatzes *pacta sunt servanda* statt, doch können Willenserklärungen durch die technologischen Bedingungen nicht so abgebildet werden, dass sie keinerlei Auslegung mehr bedürfen (vgl. N 326 ff.). Auf der anderen Seite bedarf es im Vertragsrecht auch des Vertrauens in die Integrität der Vertragspartei. Die Blockchain-Technologie kann diesen Aspekt des Vertrauens teilweise überflüssig machen, da bspw. das Vertrauen in die

[62] BGE 138 III 659 E. 4.2.1 S. 666; 132 III E. 4 S. 28; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 207.

Einhaltung von Verträgen aufgrund der technologischen Möglichkeiten nicht mehr in allen Fällen nötig ist.[63]

5. Fazit

Zusammenfassend können aus heutiger Sicht zwei Facetten der Auswirkungen der Technologie auf den Vertrauensaspekt im Privatrecht – abgesehen davon, dass sie höchst unklar sind – hervorgehoben werden. Einerseits können die technologischen Möglichkeiten das Vertrauen in die Integrität und Verlässlichkeit der Vertragspartei überflüssig machen; andererseits kann die Technologie aber Willenserklärungen nicht so zweifelsfrei abbilden, dass das Vertrauensprinzip für die Auslegung von Verträgen nicht mehr zur Anwendung gelangen müsste. 50

[63] Ausführlich dazu 2. Teil Smart Contracts, N 211 ff.

B. Technische Aspekte der Blockchain-Technologie

51 Mit den nachfolgenden Ausführungen wird die Intention verfolgt, die Blockchain-Technologie in einer verständlichen Sprache zu erklären, und so den Grundstein für den zweiten Teil (Smart Contracts) zu legen. Der technisch versierte Leser muss an dieser Stelle um Nachsicht gebeten werden, da die Ausführungen die Technologie nicht in technischer Detailtiefe ausloten; dies ist für das Verständnis der vorliegenden Arbeit aber auch nicht notwendig.

52 Nachfolgend wird zuerst auf die grundlegende Funktionsweise einer Blockchain eingegangen. Danach werden als Veranschaulichungsbeispiele vier Blockchain-Plattformen vorgestellt.

I. Funktionsweise einer Blockchain

53 In der Folge wird in den Grundzügen dargelegt, wie eine Blockchain funktioniert. Es gilt das Prinzip, dass mit Hilfe der Blockchain festgehalten, überprüft und nachgewiesen werden kann, wer zu welchem Zeitpunkt welche Transaktion durchgeführt hat. Wie bereits ausgeführt, ist die Blockchain eine Aneinanderreihung von Datensätzen, in der die Daten in Blöcken zusammengefasst und sequentiell miteinander verknüpft werden.[64]

54 Grundsätzlich kann eine Blockchain lediglich als Register, in dem Datensätze (z.B. Patent, Vertrag, Diplom) abgespeichert werden,[65] oder als Infrastruktur für einfache oder kompliziertere Transaktionen zwischen zwei oder mehreren

---

64 BERENTSEN/SCHÄR, Kryptoassets, 199; BURGWINKEL, Blockchain Technology, 5 f.; GERVAIS, Blockchains, 128; SWAN, Blockchain, X (Preface).

65 So gibt bspw. das Center for Innovative Finance (CIF) der Universität Basel blockchainbasierte Kurszertifikate aus, um diese einerseits fälschungssicher auszugestalten und für Dritte (z.B. Arbeitgeber) einfach online überprüfbar zu machen. Eine Demoversion ist abrufbar unter https://cif.unibas.ch/de/eventsprojekte/zertifikate/.

Parteien genutzt werden (z.B. Übertragung von Vermögenswerten, Vertragsabwicklung).[66] Bei beiden Verwendungszwecken wird die Speicherung durch einen Transaktionsmechanismus und ein Konsensverfahren vorgenommen. In der Ausgestaltung dieser beiden Verfahren können sich dort Unterschiede ergeben, wo eine Blockchain aufgrund einer eingeschränkten Funktionalität oder eines eingeschränkten Zweckes oder Benutzerkreises einen vereinfachten Mechanismus vorsieht.[67]

55 Es gibt unzählige Varianten und Ausgestaltungen von Blockchains und die Entwicklung schreitet unaufhaltsam voran. Die nachfolgenden Erläuterungen sind daher sehr vereinfacht gehalten und als Grundmechanismen zu verstehen. Als Orientierungshilfe dient hier die Bitcoin-Blockchain. Dabei wird zuerst erläutert, wie der Transaktionsmechanismus in den Grundzügen funktioniert und anschliessend auf die Bedeutung des Konsensverfahrens eingegangen.

1. Transaktionsauslösung

56 Jeder Teilnehmer des Blockchain-Netzwerkes verfügt über ein kryptografisches Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel (*Public* und *Private Key*, N 57).[68] Aus dem öffentlichen Schlüssel wird zudem eine Adresse generiert, mit der bspw. Kryptowährungen oder andere *Token* entgegengenommen werden können.[69]

57 Der private Schlüssel dient als Signatur; diejenige Person, welche eine Transaktion auslösen möchte, unterschreibt mit diesem Schlüssel die

---

66 Z.B. die Übertragung von Kryptowährungen auf der Bitcoin- oder Ethereum-Blockchain.

67 Z.B. eingeschränkter Konsensmechanismus bei einer Blockchain, die ausschliesslich als Register für die Integritätsnachweise von Dokumenten dient.

68 Vgl. ANTONOPOULOS, Mastering Bitcoin, 63; BERENTSEN/SCHÄR, Kryptoassets, 119; STOMMEL, Blockchain-Ökosysteme, 10.

69 ANTONOPOULOS, Mastering Bitcoin, 65; BERENTSEN/SCHÄR, Kryptoassets, 126 f.; STOMMEL, Blockchain-Ökosysteme, 10.

gewünschte Transaktion.[70] Die Signatur belegt, dass die Speicherung oder die Übertragung eines Wertes tatsächlich von der Person X ausgelöst wurde. Der öffentliche Schlüssel dient zur Validierung (im Sinne von Authentifizierung des Inhabers des Private Keys) dieser Transaktion.[71] Es kann also mit Hilfe des öffentlichen Schlüssels überprüft werden, ob Partei X tatsächlich die entsprechende Transaktion mit ihrem privaten Schlüssel signiert hat.[72]

58 Die gewünschte Transaktion wird durch den Nutzer signiert und dann in einem Transaktionspool (auch *Memory Pool* oder *Memopool*) zwischengespeichert, um anschliessend durch einen Miner validiert zu werden (vgl. nachfolgend Konsensverfahren N 61 ff.).[73]

59 Beispiel 1: Anna hat eine Erfindung gemacht und möchte ihr Patent in der Blockchain abspeichern. Dazu generiert sie aus dem Dokument (Patent) einen *Hash-Wert* (Anhang, N 5 ff.) und speichert diesen auf der Blockchain. Sie signiert ihren Datensatz mit ihrem privaten Schlüssel.[74]

60 Beispiel 2: Anna möchte Empfänger Bert eine Einheit einer Kryptowährung übertragen. Dazu sendet sie die Einheit an die Adresse von Bert, die aus dem öffentlichen Schlüssel von Bert generiert wurde. Anna unterschreibt die Transaktion mit ihrem privaten Schlüssel. Bert kann mit Hilfe des öffentlichen Schlüssels von Anna überprüfen, ob die Transaktion auch wirklich von ihr stammt.

---

70 VIGNA/CASEY, Cryptocurrency, 125 ff.

71 SWANSON, Great Chain, 17 f.

72 Vgl. ANTONOPOULOS, Mastering Bitcoin, 57, 60; BERENTSEN/SCHÄR, Kryptoassets, 55.

73 ANTONOPOULOS, Mastering Bitcoin, 192.

74 Es besteht auch die Möglichkeit, dass der komplette Datensatz auf der Blockchain gespeichert werden kann; es kommt auf die Speicherkapazität der jeweiligen Blockchain an. Vgl. BURGWINKEL, Blockchain Technology, 13 f.

2. Konsensverfahren

61 Eine kryptografische Signatur kann die Authentizität und die Integrität der Daten sicherstellen, nicht aber verhindern, dass ein Wert mehrfach übertragen wird.[75] Auch regelt die kryptografische Verschlüsselung nicht, in welcher Reihenfolge Transaktionen in die Blockchain aufgenommen werden, damit sämtliche Knotenpunkte über den gleichen Datensatz verfügen. Diese beiden Probleme (Mehrfachübertragung und Chronologie der Transaktionen) werden durch das sog. Konsensverfahren gelöst.

62 Mit dem Konsensverfahren einigen sich die Nutzer grundsätzlich auf eine Chronologie der Transaktionen und stellen diese Transaktionshistorie mit einem bestimmten Verfahren, z.B. einer zusätzlichen Aufgabenstellung sicher.[76] Das Konsensverfahren muss zudem so ausgestaltet sein, dass betrügerisches Verhalten nicht lohnenswert ist und sich die Teilnehmer aus Eigeninteressen an die Regeln halten.[77]

63 In Beispiel 1 kann dieser zusätzliche Prüfschritt entfallen, da Anna keinen Wert überträgt.

64 In Beispiel 2 würde in einem ersten Schritt überprüft, ob Anna tatsächlich über eine Einheit der Kryptowährung verfügen kann und ob sie diese Einheit nicht bereits einer anderen Person, z.B. Carl, übertragen hat. In einem zweiten Schritt würde die zusätzliche Aufgabe gelöst, die die Chronologie der Transaktionen sicherstellt.

---

75 Die Signatur belegt, dass der Wert tatsächlich übertragen/überschrieben wurde, jedoch kann eine digitale Signatur nicht verhindern, dass ein Wert gleichzeitig mehrfach übertragen wird; vgl. ANTONOPOULOS, Mastering Bitcoin, 2 f.; MEISSER, Kryptowährungen, 81; SCHMEH, Kryptografie, 781.

76 Vgl. BERENTSEN/SCHÄR, Kryptoassets, 206; SIXT, Transaktionssysteme, 43.

77 BERENTSEN/SCHÄR, Kryptoassets, 206.

a) Öffentliche Blockchain

65 Sind sich die Teilnehmer einer Blockchain gänzlich unbekannt, wie dies bei öffentlichen Blockchains die Regel ist, werden sog. vertrauenslose Konsensalgorithmen eingesetzt.[78] Solche Konsensverfahren sind beispielsweise *Proof of Work* (*PoW*, N 66 ff.), *Proof of Stake* (*PoS*)[79] oder *Proof of Space* (*PoSp*)[80].[81] Nachfolgend wird für öffentliche Blockchains stellvertretend das PoW-Verfahren erläutert, welches bei der Bitcoin-Blockchain und derzeit auch noch bei der Ethereum-Blockchain angewandt wird.[82]

66 Das PoW-Verfahren soll nicht nur die Mehrfachübertragung eines Wertes verhindern, sondern auch die Transaktionshistorie sicherstellen; es wird zusätzlich zur Validierung der Signatur[83] eingesetzt.

---

78 KIENZLER, Hyperledger, 114.

79 Bei Proof of Stake wird die Validierung nach Stimmgewicht eines Nutzers innerhalb der Blockchain vorgenommen. Das Stimmgewicht stützt sich dabei auf die Anzahl der Währungseinheiten, die ein Teilnehmer besitzt oder nach einem vordefinierten Verteilschlüssel der Stimmen, vgl. WEBER/WAGNER, Corporate Governance, 62.

80 Proof of Space, auch *Proof of Capacity*, genannt, ist ein Konsensverfahren, das sich nach der zur Verfügung gestellten Speicherkapazität richtet (im Gegensatz zur Proof of Work, das sich an der Rechenleistung orientiert).

81 Vgl. WEBER, Blockchain, N 3 f.; WEBER/WAGNER, Corporate Governance, 62.

82 Die Ethereum-Blockchain will in Zukunft auf ein anders Konsensprotokoll wie bspw. Proof of Stake setzen.

83 Die Bitcoin-Blockchain arbeitet mit asymmetrischen Schlüsseln, auf elliptischen Kurven beruhenden ECDSA-Algorithmus: vgl. ANTONOPOULOS, Mastering Bitcoin, 63 ff.; SCHMEH, Kryptografie, 781; SIXT, Transaktionssysteme, 37.

67 Grundsätzlich wird beim PoW[84] eine Rechenaufgabe gestellt, die zwar aufwendig zu lösen, aber einfach zu überprüfen ist.[85] Die Lösung der Aufgabe erfolgt mittels der sog. *Brute-Force-Methode* (auch Exhaustionsmethode genannt); das heisst, es wird solange nach der Lösung gesucht, bis sie gefunden ist.[86] Das Lösen der Aufgabe benötigt viel Rechenleistung, welche durch einen Teil der Teilnehmer des Netzwerkes übernommen wird. Bei der Bitcoin- und Ethereum-Blockchain übernehmen Miner diese Aufgabe und werden mit einer vordefinierten Anzahl Bitcoins, resp. einer Transaktionsgebühr dafür entlohnt.[87] Erst wenn diese Aufgabe gelöst ist, kann die Transaktion zur Blockhain hinzugefügt werden.[88]

68 In der Praxis arbeiten viele Miner gleichzeitig an der Validierung derselben Transaktion. Dabei gilt das Prinzip, dass derjenige Miner die Vergütung erhält, der die Rechenaufgabe zuerst gelöst hat. Es wird an mehreren verschiedenen Transaktionen gleichzeitig gearbeitet. Dies kann zu einer Bildung von mehreren Ästen der Kette führen. Der Konsensalgorithmus gibt jedoch vor, dass nur die längste aller Ketten die gültige ist.[89]

69 Überträgt Anna den Wert, den sie bereits Bert versprochen hat, zweimal, das heisst gleichzeitig auch an Carl, so wird nur diejenige Transaktion in die Blockchain aufgenommen, die zuerst „gemint“ wurde. Um sicher zu gehen, dass eine Information in einer Blockchain stabil ist, das heisst, als gültige Transaktion in die Blockchain aufgenommen wurde, wird bei der Bitcoin-Blockchain angeraten, mind. sechs Folge-Blöcke abzuwarten.[90]

---

84 Ausführlich zum PoW-Algorithmus ANTONOPOULOS, Mastering Bitcoin, 191 ff. PoW wird auch anderweitig eingesetzt, z.B. für Spam-Schutz, siehe für weitere Beispiele SCHMEH, Kryptografie, 289 f.

85 SWANSON, Great Chain, 17 ff. Zur mathematischen Rechenaufgabe siehe SCHMEH, Kryptografie, 289 ff.

86 BERENTSEN/SCHÄR, Kryptoassets, 61; GERHARDS, Verschlüsselung, 34; SCHMEH, Kryptografie, 289 f.

87 SCHMEH, Kryptografie, 781; VIGNA/CASEY, Cryptocurrency, 126 ff.

88 Vgl. MEISSER, Kryptowährungen, 86 f.; SIXT, Transaktionssysteme, 31 f.

89 BERENTSEN/SCHÄR, Kryptoassets, 216.

90 ANTONOPOULOS, Mastering Bitcoin, xxiv (unter "confirmations"); SIXT, Transaktionssysteme, 43.

b) Private Blockchain

70 Bei privaten Blockchains kann das Konsensverfahren weniger aufwendig ausgestaltet werden, da sich die Teilnehmer entweder bereits kennen oder die gegenseitige Identifizierung sicherstellen können.[91]

3. Blockbildung

71 Die durch das Mining validierten Transaktionen werden in einem Block zusammengefasst und an die bestehende Blockchain gekoppelt. Blocks sind also Informationspakete, die aus mindestens einer Transaktion bestehen.[92] Je nach Blockchain unterscheidet sich die Anzahl der enthaltenen Transaktionen eines Blockes. Bei der Bitcoin-Blockchain wird nur alle zehn Minuten ein neuer Block zur Kette hinzugefügt, wobei die Blockgrösse auf derzeit 1MB limitiert ist (das entspricht ca. 1978 Transaktionen bei einer Transaktionsgrösse von 500 Bytes).[93] Bei der Ethereum-Blockchain ist keine Grössenlimitierung der einzelnen Blöcke vorgesehen: die Anzahl der Transaktionen wird dynamisch durch die Berechnung des Gas-Wertes (vgl. N 178) angepasst.[94]

72 Ein Block der Blockchain setzt sich grundsätzlich aus einer *Kopfzeile* (*Block Header*) und dem *Körper* (*Block Body*) zusammen. In der Kopfzeile werden je nach Blockchain unterschiedliche Informationen gespeichert. In der Bitcoin-Blockchain bspw. werden im Block Header vier Datensätze untergebracht: die Referenz zum vorhergehenden Block, womit der Block mit dem vorhergehenden verbunden ist; der Hash-Wert (Anhang, N 5 ff.) aller bisherigen Transaktionen; ein Zeitstempel sowie die Problemlösung der Rechenaufgabe, die für die Aufnahme in die Blockchain gelöst werden musste (vgl. PoW, N 66 ff).[95]

---

91 Vgl. KIENZLER, Hyperledger, 114, 116 f.

92 BERENTSEN/SCHÄR, Kryptoassets, 58.

93 PLOOM, Blockchains, 126.

94 PLOOM, Blockchains, 126.

95 ANTONOPOULOS, Mastering Bitcoin, 163.

Der Block Body setzt sich aus einer Liste sämtlicher vorgelagerter Transaktionen sowie der Information der aktuellen Transaktion zusammen.[96] Je nach Art der Blockchain können im Block Body auch noch zusätzliche Informationen oder Programme (z.B. Smart Contract) enthalten sein. 73

II. Blockchain-Beispiele

Nachfolgend werden vier bekannte Blockchain-Plattformen als Anschauungsbeispiele vorgestellt; darunter sind jeweils zwei öffentliche und zwei geschlossene Plattformen. Dabei werden jeweils der Zweck und die grundlegenden Funktionalitäten erläutert. 74

1. Bitcoin-Blockchain

Die Bitcoin-Blockchain ist in erster Linie ein System für die Übertragung der Kryptowährung Bitcoin. Bitcoin ist (derzeit) die am besten kapitalisierte Kryptowährung.[97] Die Währung erlebt zwar extreme Kursschwankungen, erfreut sich aber trotzdem seit ihrer Einführung 2008 immer grösserer Beliebtheit. Bitcoin hat es geschafft, sich vom Stigma krimineller Geschäfte zu lösen. In der Schweiz können beispielsweise an den Billetautomaten der SBB Bitcoins erwerben werden.[98] Das Wirtschaftsprüfungsunternehmen EY geht sogar noch einen Schritt weiter: Neben der Tatsache, dass das Unternehmen ihren Mitarbeitern ein Bitcoin-Konto eingerichtet und Bitcoin-Geldautomaten in den Eingangsbereichen aufgestellt hat, ist es auch möglich, EY seit 2017 in 75

96 Vgl. ANTONOPOULOS, Mastering Bitcoin, 162.

97 https://coinmarketcap.com/currencies/.

98 www.sbb.ch/de/bahnhof-services/dienstleistungen/weitere-dienstleistungen/bitcoin.html.

Bitcoins zu bezahlen.[99] Auch die Städte Zug und Chiasso akzeptieren in einem gewissen Umfang Zahlungen in Bitcoin.[100]

a) Zweck

76 Zweck ist die Errichtung eines dezentralen, digitalen P2P-Zahlungssystems, der Kryptowährung Bitcoin.[101] Die Bitcoin-Blockchain sieht eine Grössenbeschränkung pro Block vor,[102] weshalb Zusatzanwendungen nur in einem sehr beschränkten Masse möglich sind. So besteht bspw. die Möglichkeit, Zusatzinformationen in begrenztem Umfang mit den einzelnen Transaktionen mitzusenden.[103] Diese Zusatzinformationen werden jedoch nicht durch das Netzwerk validiert.

b) Transaktionsmechanismus

77 Das Bitcoin-Modell sieht keine Kontoführung der Nutzer vor; aufgezeichnet werden lediglich Transaktionsresultate.[104] Jede Transaktion muss einen Input und einen Output aufweisen. Es ist nicht möglich, nur einen Teil der Kryptowährung zu transferieren, sondern es muss immer der gesamte Betrag übertragen werden (z.B. Anna hat fünf Bitcoins und will Bert zwei übertragen;

---

99 www.ey.com/ch/de/newsroom/news-releases/medienmitteilung-ey-schweiz-ermoglicht-bezahlung-ihrer-dienstleistungen-in-bitcoin.

100 KT. ZG, MM vom 2. November 2017; GEMEINDE CHIASSO, MM vom 7. September 2017.

101 NAKAMATO, Whitepaper Bitcoin, https://bitcoin.org/bitcoin.pdf; ausführlich zur Geschichte, Funktion und Anwendung statt vieler ANTONOPOULOS, Mastering Bitcoin, 1 ff.

102 Die ursprüngliche Blockheadergrösse beträgt ohne Transaktionen 80 Bytes: Vgl. ANTONOPOULOS, Mastering Bitcoin, 156; NAKAMATO, Bitcoin Whitepaper, 6.

103 Limite bei derzeit 40 Bytes, vgl. PLOOM, Blockchains, 136.

104 Vgl. ANTONOPOULOS, Mastering Bitcoin, 114 f.; BERENTSEN/SCHÄR, Kryptoassets, 170 ff.; KIENZLER, Hyperledger, 119.

in diesem Fall überträgt sie Bert zwei und sich selber drei Bitcoins).[105] Dieses Modell ist als *UTXO-Modell* (*Unspent Transaction Outputs*) bekannt.[106]

78 Für die Bitcoin-Blockchain wurde als Konsensverfahren Proof of Work gewählt (vgl. N 66 ff.). [107]

2. Ethereum-Blockchain

79 Die Ethereum-Blockchain gilt als vielseitig und innovativ. Einen Rückschlag erlitt die Ethereum-Blockchain allerding mit dem „DAO-Hack“, als ein Hacker die Summe von damals umgerechnet ca. 50 US-Dollar abzweigte und damit die gesamte Blockchain-Plattform ins Wanken brachte. Die Folge war eine Spaltung der Ethereum-Blockchain (*Hard Fork*, vgl. Anhang, N 36).[108] Der dadurch entstandene Reputationsschaden konnte die Ethereum-Blockchain jedoch nicht daran hindern, sich in viele Richtungen weiterzuentwickeln. Auch die von Ethereum lancierte Kryptowährung, Ether, erfreut sich wachsender Beliebtheit; sie ist neben Bitcoin eine der am besten kapitalisierten Kryptowährungen.[109] Ether ist zwar noch kein verbreitetes Zahlungsmittel, die Stadt Zug akzeptiert jedoch in einem gewissen Umfang Zahlungen in dieser Kryptowährung.[110]

a) Zweck

80 Die Ethereum-Blockchain ist grundsätzlich eine öffentliche Blockchain. Das Plattform-Modell (resp. der Code) könnte aber auch für den Betrieb eines privaten Netzwerkes eingesetzt werden. Sie ist nicht nur für die Übertragung

---

105 NAKAMATO, Bitcoin Whitepaper, 5.

106 ANTONOPOULOS, Mastering Bitcoin, 114 f.; BERENTSEN/SCHÄR, Kryptoassets, 171 ff.; NAKAMATO, Bitcoin Whitepaper, 2.

107 ANTONOPOULOS, Mastering Bitcoin, 191 ff.; BERENTSEN/SCHÄR, Kryptoassets, 61 ff.; NAKAMATO, Bitcoin Whitepaper, 3.

108 Vgl. GYR, DAO, N 11 ff.; SHIER U.A., DAO Attack; TOSOVIC, DAO-Hack, 159 ff.

109 https://coinmarketcap.com/currencies/.

110 KT. ZUG, MM vom 2. November 2017.

der Ethereum-eigenen Kryptowährung Ether geschaffen worden, sondern lässt weitergehende Anwendungen zu, d.h. sie ist eine universelle Plattform.[111] Es ist möglich, auf der Ethereum-Blockchain bspw. eine eigene Kryptowährung (Anhang, N 28 f.) zu kreieren oder eine DAO (Anhang, N 37) oder Smart Contracts (N 214 ff.) zu initialisieren.[112]

b) Transaktionsmechanismus

81 Im Gegensatz zur Bitcoin-Blockchain verfügt die Ethereum-Blockchain über ein Kontomodell, auf dem u.a. der Kontostand in Ether und allenfalls ein Smart Contract[113] gespeichert werden kann.[114] Aufgrund des Kontomodelles kann im Gegensatz zum UXTO-Modell (N 77) auch nur eine Teilmenge des auf dem Konto verbuchten Wertes transferiert werden.[115]

82 Die Ethereum-Blockchain wählte wie die Bitcoin-Blockchain das Konzept des Proof of Work (vgl. N 78, 66 ff.) als Konsensmechanismus.[116]

3. Hyperledger

83 *Hyperledger* ist eine Business-Blockchain-Plattform der *Linux Foundation*. Hyperledger ist der Oberbegriff für zahlreiche Anwendungen der Hyperledger-Technologie, deren verschiedene Projekte jeweils mit einem zusätzlichen Namen versehen und unterschiedlich ausgestaltet sind.[117] Aufgrund der

---

111 Für die (u.a. technische) ausführliche Beschreibung vgl. ETHEREUM WHITEPAPER, Abschnitt Ethereum.

112 Übersicht über die Möglichkeiten auf www.ethereum.org.

113 Ein Smart Contract ist eine Software, ausführlich zu Smart Contracts vgl. 2. Teil: Smart Contracts, N 211 ff.

114 ETHEREUM WHITEPAPER, Abschnitt Ethereum Accounts.

115 ETHEREUM WHITEPAPER, Abschnitt Ethereum Accounts; Vgl. KIENZLER, Hyperledger, 119.

116 Vgl. ETHEREUM WHITEPAPER, Abschnitt Blockchain and Mining.

117 Z.B. Hyperledger Fabric, Hyperledger Iroha, Hyperledger Burrow etc., Auflistung inkl. Projektbeschreibungen abrufbar unter www.hyperledger.org/projects.

Vielfalt der Projekte können nur wenige allgemeingültige Aussagen gemacht werden.

a) Zweck

84 Hyperledger ist auf Unternehmen ausgerichtet, die private Blockchains betreiben möchten.[118] Es sollen Standards geschaffen werden, damit die Interoperabilität zwischen den einzelnen Blockchains von Unternehmen sichergestellt werden kann.[119] Hyperledger bietet eine grosse Anzahl von Anwendungen, deren Strukturen modular sind, womit grössere Ausbau- und Anpassungsmöglichkeiten und Flexibilität versprochen werden.[120] Verfügbar sind u.a. eigene Distributed Ledgers, Smart Contracts, Kryptowährungen und Applikations-Vorlagen.[121]

b) Transaktionsmechanismus

85 Der Transaktionsmechanismus hängt davon ab, welche Hyperledger-Anwendung gewählt wird. Bei Hyperledger Fabric erfolgt eine Transaktion bspw. in drei Schritten: der Nutzer löst die Transaktion aus, der Smart Contract (hier Chaincode genannt) führt aus und schreibt das Ergebnis in die Transaktion; danach wird die Transaktion in eine Warteschlange weitergeleitet, wo sie auf eine Validierung (je nach Konsensverfahren) wartet, bevor sie in der Blockchain abgespeichert wird.[122]

86 Es werden verschiedene Konsensverfahren angeboten. Den Nutzern steht es frei, entweder ein Verfahren zu wählen, das auf Zufall beruht (wie z.B. Proof of Stake oder Proof of Work) oder ein Konsensmodell, das sich auf ein Abstimmungsverfahren stützt.[123]

---

118 www.hyperledger.org; vgl. KIENZLER, Hyperledger, 111.

119 Vgl. HYPERLEDGER WHITEPAPER, Hyperledger Architecture, V1, 2.

120 Vgl. HYPERLEDGER WHITEPAPER, Hyperledger Architecture, V1, 3.

121 Vgl. HYPERLEDGER WHITEPAPER, Hyperledger Architecture, V1, 2.

122 Vgl. PABST, Blockchain-Technologie, 25 f.

123 Zu den verschiedenen eingesetzten Algorithmen wie bspw. Kafka vgl. HYPERLEDGER WHITEPAPER, Hyperledger Architecture, V1, 6 f.

4. Corda

87 *Corda* ist eine Entwicklung des Bankenkonsortiums R3.[124] Sie ist wie Hyperledger eine Business-Blockchain und bezeichnet sich als halb-private Blockchain.[125] Nachdem die Plattform erst hinter geschlossenen Türen entwickelt wurde, wird sie unterdessen als Open-Source-Projekt weitergeführt (unter der Apache Lizenz 2.0).[126]

a) Zweck

88 In erster Linie dient Corda dazu, die zwischen verschiedenen (Finanz-) Instituten mehrfach geführten Dokumente auf eine einzige Plattform zu bringen, um mehr Effizienz zu schaffen.[127] Die Plattform soll im Gegensatz zu öffentlichen Blockchains eine hohe Skalierbarkeit aufweisen und die Geheimhaltung von Daten sicherstellen.[128]

89 Corda ist eine globale Plattform; die darauf gespeicherten Daten und Applikationen sind nur für die involvierten Parteien zugänglich.[129] Auf der Plattform können verschiedene Anwendungen (Apps, Smart Contracts) installiert werden. Corda verfügt nicht über eine eigene Kryptowährung.

b) Transaktionsmechanismus

90 Wie bei der Bitcoin-Blockchain werden bei Corda Daten nicht in Form einer Kontoführung gespeichert (UXTO-Modell, N 77); die Einträge sind entweder gültig (*current, unspent*) oder verbraucht (*consumed, spent*).[130] Jeder Eintrag muss einer originären Transaktion zugeordnet werden können: Er muss also

---

124 Zum R3-Konsortium gehören über 200 Finanzinstitute weltweit, darunter auch UBS und CS, vgl. www.r3.com.

125 Vgl. HEARN, Whitepaper Corda II, 7.

126 Vgl. https://github.com/corda/corda.

127 BROWN/CARLYLE/GRIGG/HEARN, Whitepaper Corda I, 3.

128 Vgl. BROWN/CARLYLE/GRIGG/HEARN, Whitepaper Corda I, 13 f.; HEARN, Whitepaper Corda II, 4, 48 ff.

129 BROWN/CARLYLE/GRIGG/HEARN, Whitepaper Corda I, 8.

130 HEARN, Whitepaper Corda II, 13.

auf der Liste sämtlicher Outputs abrufbar sein; ansonsten ist er nicht gültig.[131] Es ist jedoch möglich, dass ein Input oder ein Output null ist.[132]

91 Das Konsensverfahren findet nicht auf dem gesamten Netz statt, sondern nur zwischen den jeweils an einer Transaktion beteiligten Parteien. Es gibt zwei Konsensverfahren. Das eine betrifft die Gültigkeit der Transaktion, das andere die Einmaligkeit (d.h. dieselbe Transaktion wurde nicht bereits für gültig und einzigartig befunden).[133]

131 HEARN, Whitepaper Corda II, 13.

132 Ausführlich zum Transaktionsmechanismus HEARN, Whitepaper Corda II, 13 ff.

133 BROWN/CARLYLE/GRIGG/HEARN, Whitepaper Corda I, 9.

C. Vertragliche Aspekte der Blockchain-Technologie

92 Nachdem die technischen Anwendungen der Blockchain-Technologie veranschaulicht worden sind, werden im nachfolgenden Kapitel die möglichen Vertragsbeziehungen innerhalb der beiden Anwendungsmöglichkeiten der Blockchain-Technologie (Blockchain als Software und Blockchain als Plattform) sondiert.

93 Bei der Blockchain als Software kann es sich um eine proprietär erstellte Software oder um eine Open-Source-Software (zum Begriff sogleich N 112 ff.) handeln, wobei sich die Vertragsgestaltung nach der vorgesehenen Verwendungsart richtet. Allerdings sind Open-Source-Entwicklungen im Zusammenhang mit der Blockchain die Regel, weshalb in der Folge diese Form genauer untersucht wird.

94 Die Blockchain als Plattform kann als operativer Dienst oder als reines P2P-Netzwerk ausgestaltet sein. Die vertragsrechtliche Einordnung richtet sich bei einem operativen Dienst nach dem Vereinbarten, während bei einem P2P-Netzwerk zu untersuchen ist, ob die Blockchain-Gemeinschaft einer der Rechtsordnung bekannten juristischen Figuren zugeordnet werden kann.

95 In einem ersten Schritt werden zur besseren Verständlichkeit die involvierten Parteien einer Blockchain kurz eingeführt, um eine spätere vertragsrechtliche Einordnung zu erleichtern.

I. Involvierte Parteien

96 Eine Vielzahl von Akteuren stellen das Funktionieren einer Blockchain sicher. In der vorliegenden Arbeit wird eine Auswahl vorgenommen und lediglich auf die wichtigsten eingegangen. Es sind dies: die Softwareentwickler, die Nutzer, die Miner sowie die Wallet-Anbieter.

1. Softwareentwickler

97 Die Softwareentwickler stehen chronologisch am Anfang der Blockchain, da sie den Quellcode entwickeln. Die Software für öffentliche Blockchain-Plattformen, aber auch für zahlreiche private Blockchains, werden open source entwickelt. Das bedeutet, dass eine undefinierte Anzahl von Softwareentwicklern involviert ist, die in der Regel um die Welt verteilt an der (Weiter-) Entwicklung arbeiten. Es kann also davon ausgegangen werden, dass nicht ein einziger, sondern eine Vielzahl von Entwicklern an einer Open-Source-Software beteiligt ist. Der einfachen Lesbarkeit halber wird jedoch nachfolgend bei der Nennung von Softwareentwicklern die Einzahl verwendet.

98 Es ist im Übrigen nicht zwingend, dass eine Blockchain-Software als Open-Source-Software entsteht; sie kann auch proprietär für eine Partei entwickelt werden.

2. Nutzer

99 Die Nutzer (in der vorliegenden Arbeit stellenweise auch Teilnehmer genannt) einer Blockchain sind diejenigen Parteien, die einen Knotenpunkt der Blockchain-Plattform betreiben.[134] Sie können gleichzeitig auch Miner (N 101 ff.) und/oder Wallet-Anbieter (N 104 ff.) sein.[135] So beinhaltet bspw. bei der

---

134 Je nach Blockchain gibt es unterschiedliche Knotenpunkte. So wird in der Bitcoin-Blockchain zwischen den *Full Nodes* (auch *Bitcoin Core Client*), welche die gesamte aktualisierte Blockchain gespeichert haben und gleichzeitig auch eine Wallet- und Miningfunktion beinhalten und *Thin* oder *Light Nodes* unterschieden, wobei letztere eine vereinfachte Nutzung zulassen und nicht über eine Kopie der gesamten Blockchain verfügen und via sog. *Simplified-Payment-Verification (SPV)-Verfahren* das Netzwerk nutzen. Ausführlich zu den Knotenpunkten bei der Bitcoin-Blockchain ANTONOPOULOS, Mastering Bitcoin, 180 ff.; BERENTSEN/SCHÄR, Kryptoassets, 97 ff.; SIXT, Transaktionssysteme, ff.

135 Vgl. ANTONOPOULOS, Mastering Bitcoin, 172.

Bitcoin-Blockchain ein sog. *Full Node*, also ein vollständiger Knotenpunkt, jeweils auch eine Wallet-sowie eine Mining-Funktion.[136]

100 Nutzer, die zwar über Kryptowährung oder Token verfügen, aber selbst keinen Knotenpunkt des Netzwerkes unterhalten, werden in der vorliegenden Arbeit als *Nutzer ausserhalb der Blockchain* bezeichnet.[137]

3. Miner

101 Insbesondere bei öffentlichen Blockchains gehören die Miner zu den Hauptakteuren. Sie übernehmen die Erstellung von neuen Blocks, welche gemäss den Regeln im Konsensprotokoll vorgenommen wird (vgl. N 61 ff.). In der Regel werden Miner für die Zusammenstellung und Validierung der Blöcke mit einer Gebühr entlohnt (vgl. N 178, 181).

102 In der vorliegenden Arbeit wird keine Unterscheidung zwischen einzelnen Minern, Miningpools[138] und Mining-Farmen[139] gemacht; sämtliche Einheiten werden unter dem Begriff *Miner* zusammengefasst.

---

136 Vgl. ANTONOPOULOS, Mastering Bitcoin, 172 ff.; SIXT, Transaktionssysteme, 34.

137 Diese Gruppe stellt in der Praxis wohl die grösste Gruppe dar, da der Unterhalt eines Knotenpunktes nicht gerade massentauglich ist. Die meisten Besitzer von Kryptowährungen oder anderen Token (Anhang, N 30 ff.) verfügen nicht selbst über eine Kopie der Blockchain und stellen ihren Zugang zum Netzwerk über Drittparteien wie bspw. Wallet-Anbieter sicher.

138 In einem Miningpool schliessen sich mehrere Miner zusammen, um gemeinsam mehr Rechenkapazität (und damit auch einen höheren Verdienst) zu generieren, vgl. ANTONOPOULOS, Mastering Bitcoin, 27.

139 Mining-Farmen sind grosse Anlagen, in denen unzählige von spezialisierten Mining-Computern stehen, die dank ihrer enormen Rechenkraft viele Transaktionen validieren und so hohe Gewinne erzielen können, vgl. ANTONOPOULOS, Mastering Bitcoin, 27.

Miner können im Übrigen gleichzeitig Nutzer (N 99 f.) und/oder Wallet-Anbieter sein (N 104 ff.).[140] 103

4. Wallet-Anbieter

Als Wallet wird ein digitaler Container oder ein digitales Portemonnaie verstanden, in dem die kryptografischen Schlüssel (vgl. Anhang, N 13 ff.) und Adressen von Nutzern verwaltet werden.[141] Ein Wallet ist vereinfacht gesagt eine Datenbank, die für die Verwahrung von Schlüsseln geschaffen wurde.[142] Die in einem Wallet verwalteten Private Keys sind unabdingbar, um über die jeweiligen Kryptowährungen oder sonstigen Token (Anhang, N 30 ff.) verfügen zu können; ohne diese ist der Zugriff auf die Vermögenswerte nicht möglich.[143] 104

Es kann zwischen *Software Wallets*, auch *virtuelle Wallets* genannt (in Desktop-, Mobile- und Web-Varianten), und *Hardware Wallets* unterschieden werden.[144] Software Wallets können entweder heruntergeladen oder via eine Website bedient werden. Bei Software Wallets wird von sog. *Hot Storage* gesprochen, da das Wallet direkt oder indirekt mit dem Internet verbunden ist.[145] Bei Hardware Wallets kommen Datenträger zum Einsatz, die nicht mit dem Internet verbunden sind, wie bspw. USB-Sticks oder eine externe Festplatte; hierbei handelt es sich um das sog. *Cold Storage*.[146] Es ist auch 105

---

140 Vgl. ANTONOPOULOS, Mastering Bitcoin, 172.

141 Vgl. ANTONOPOULOS, Mastering Bitcoin, 93.

142 Vgl. ausführlich zu Wallets und deren technologischer Ausgestaltung ANTONOPOULOS, Mastering Bitcoin, 93 ff.; BERENTSEN/SCHÄR, Kryptoassets, 131 ff.

143 Vgl. BERENTSEN/SCHÄR, Kryptoassets, 310.

144 Vgl. ANTONOPOULOS, Mastering Bitcoin, 7; BERENTSEN/SCHÄR, Kryptoassets, 313 ff.

145 Die Verbundenheit mit dem Internet birgt Risiken, insbesondere von Hackerangriffen, vgl. ANTONOPOULOS, Mastering Bitcoin, 7; BERENTSEN/ SCHÄR, Kryptoassets, 313 f.

146 ANTONOPOULOS, Mastering Bitcoin, 7; BERENTSEN/SCHÄR, Kryptoassets, 318.

möglich, die Private Keys konventionell auf Papier aufzuzeichnen und aufzubewahren, wofür kein Wallet in vorgenanntem Sinne benötigt wird (sog. *Paper Wallet*[147]).[148]

106 Wallets sind insbesondere für Nutzer ausserhalb der Blockchain (N 100) von zentraler Bedeutung, da bspw. Software Wallets, die gleichzeitig einen vollständigen Knotenpunkt betreiben, Transaktionen für ihre Nutzer durchführen.[149]

107 Ein Wallet-Anbieter kann gleichzeitig auch Miner oder Nutzer sein.[150]

II. Blockchain als Software

108 Eine allgemeinverbindliche Definition des Begriffes *Software* existiert nicht. Mancherorts wird zwischen Computerprogramm und Software unterschieden, andernorts werden die Begriffe synonym verwendet. Wird Software als Überbegriff verstanden, so beinhaltet er nebst dem Computerprogramm selbst auch die dazugehörige Dokumentation.[151] Wird zwischen Computerprogramm und Dokumentation unterschieden, dann enthält das Computerprogramm den Code (als *Source*- oder *Objektcode*) und die Dokumentation die Beschreibung (z.B. Bedienungsanleitung, Installationsanleitung etc.).[152] Es gibt unzählige Arten von Software, die sich je nach Zweck und Anwenderkreis unterscheiden.[153]

---

147 Vgl. ANTONOPOULOS, Mastering Bitcoin, 88 ff.; BERENTSEN/SCHÄR, Kryptoassets, 319.

148 Vgl. ANTONOPOULOS, Mastering Bitcoin, 7, 88 ff; BERENTSEN/SCHÄR, Kryptoassets, 319 ff.

149 BERENTSEN/SCHÄR, Kryptoassets, 314; SIXT, Transaktionssysteme, 36 f.

150 Vgl. ANTONOPOULOS, Mastering Bitcoin, 172.

151 LUDEWIG/LICHTER, Software Engineering, 34; MORSCHER/DORIGO, Software-Lizenzverträge, 21; WIDMER, Software-pflegevertrag, 5 ff.; vgl. FRÖHLICH-BLEULER, Softwareverträge, N 25; FISCHER/HOFER, Lexikon der Informatik, 837.

152 FRÖHLICH-BLEULER, Softwareverträge, N 25 f.

153 Für eine Übersicht vgl. FRÖHLICH-BLEULER, Softwareverträge, N 29 ff.

Viele der Blockchain-Quellcodes sind als Open-Source-Software veröffentlicht (vgl. nachfolgend N 121). Im Gegensatz zur Entwicklung proprietärer Software, bei der in der Regel nur einzelne Entwickler involviert sind, die Entwicklung grundsätzlich geheim ist und der Quellcode dem Anwender nicht bekannt gegeben wird, ist bei Open-Source-Software-Projekten eine (generell unbekannte) Vielzahl von Entwicklern (meist dezentral und in einer virtuellen Entwicklungsgemeinschaft) involviert und der Quellcode steht allen offen.[154] 109

Die bekannten öffentlichen Blockchain-Plattformen sind alle als open source erstellt worden und auch private Blockchain-Software ist zwischenzeitlich meist open source ausgestaltet (vgl. nachfolgend N 121). Aufgrund der zentralen Bedeutung von Open-Source-Software bei der Blockchain-Technologie wird nachfolgend nur auf diese Art von Software eingegangen.[155] Open-Source-Software spielt nicht nur in Bezug auf die Blockchain-Technologie eine grosse Rolle; sie ist auch wirtschaftlich von grosser Bedeutung, da selbst die grossen Softwareanbieter, wie bspw. Google, IBM oder Microsoft Produkte unter Open-Source-Software-Lizenzen (nachfolgend: OSS-Lizenzen) entwickeln.[156] 110

1. Open-Source-Software

Nachfolgend wird als Einführung in die Open-Source-Software zuerst auf den Begriff eingegangen. Danach werden Abgrenzungen in Bezug auf Urheber- und Nutzungsrechte vorgenommen. Im letzten Abschnitt werden die in den gängigen Blockchains verwendeten OSS-Lizenzen aufgelistet. 111

154 FRÖHLICH-BLEULER, Softwareverträge, N 1834.

155 Zu andern Softwareverträgen und -lizenzen vgl. statt vieler FRÖHLICH-BLEULER, Softwareverträge, N 1 ff.

156 Vgl. FRÖHLICH-BLEULER, Softwareverträge, N 1835.

a) Begriff

112 Mit dem Aufkommen des Personalcomputers (PC) in den 50er Jahren waren Soft- und Hardware noch untrennbar miteinander verbunden und wurden als Gesamtpaket verkauft.[157] Dabei wurde der Softwarecode bspw. von IBM (dem damals marktbeherrschenden Hersteller) „offen“ geliefert, damit Kunden ihre individuellen Anpassungen selbst vornehmen konnten.[158] Mit dem aufkommenden Wettbewerb unter den Computerherstellern in den 70er Jahren wurden Soft- und Hardware allmählich losgelöst voneinander verkauft und entwickelt.[159] Anfang der 90er Jahre setzte sich die Idee der freien Software (heute: Open-Source-Software) durch.[160]

113 „Frei“ (resp. Open Source) ist dabei nicht als Synonym für „frei von Rechten und Pflichten“ zu verstehen, auch wenn dies auf den ersten Blick und aufgrund der Unentgeltlichkeit so erscheinen mag. Frei bedeutet in diesem Zusammenhang eine zweckoffene Verwendung der Software. Grundsätzlich gewährt Open-Source-Software die freie Nutzung, die Möglichkeit der individuellen Abänderbarkeit (durch Zugang zum Quellcode), die Weiterverbreitungsmöglichkeit und die Weiterentwicklungsmöglichkeit geknüpft an die Pflicht, Weiterentwicklungen ebenfalls jedermann zugänglich zu machen.[161]

---

157 ROWLAND/KOHL/CHARLESWORTH, IT Law, 517; ausführliche historische Ausführungen siehe bei WIDMER, urheberrechtliche Aspekte, 8 ff.

158 ROWLAND/KOHL/CHARLESWORTH, IT Law, 517 f.

159 ROWLAND/KOHL/CHARLESWORTH, IT Law, 518; WIDMER, urheberrechtliche Aspekte, 9; vgl. HILTY, Softwarevertrag, 66 f.

160 Vgl. WEBER, Freie Software, 42.

161 MARLY, Softwarerecht, N 938; ROWLAND/KOHL/CHARLESWORTH, IT Law, 519; WEBER, Freie Software, 42 f; WIDMER, urheberrechtliche Aspekte, 37 ff.; SESTER, Open-Source-Software, 797.
Es gibt vier Kriterien zur Definition von Open-Source-Software seitens der *Open Source Initiative OSI* sowie vier sog. Freiheiten zur Definition freier Software seitens der *Free Software Foundation FSF*. Die beiden Kriterienkataloge sind fast identisch; die Abweichungen sind unwesentlich (siehe ausführlich zu diesem Thema JAEGER/METZGER,

114 Es sind mehrere Open-Source-Software-Bewegungen bekannt. Eine der ersten Initiativen geht auf RICHARD STALLMANN zurück, der die *GNU-Lizenzen* entwickelt hat,[162] von denen mehrere Formen existieren,[163] wobei die die *GNU General Public License* (*GNU-GPL*) die meistverbreitete ist.[164] Ende der 90er Jahre formierte sich die *Open Source Initiative* (*OSI*)[165], die ein Zertifizierungsprogramm für die Beurteilung von Open-Source-Software etablierte.[166] Die verschiedenen Bewegungen sind sich bezüglich der Auslegung der Begrifflichkeiten und der Beweggründe nicht einig, jedoch sind die Grundprinzipien vergleichbar, weshalb nachfolgend nicht näher auf die einzelnen Begriffsauffassungen der einzelnen Open-Source-Software-Bewegungen eingegangen wird.[167]

b) OSS-Lizenzen

115 Open-Source-Software wird unter Lizenzen vertrieben. Diese enthalten im Gegensatz zu gewöhnlichen Softwarelizenzverträgen ein sog. *Copyleft* (als Gegensatz zu Copyright).[168] *Copyleft* steht jedoch nicht für eine Abkehr vom Urheberrecht, sondern für eine extensive Nutzung des Werkes durch den Lizenznehmer.[169] Das Copyleft soll eine Weiterverbreitung der Software unter den gleichen Bedingungen sicherstellen und gleichzeitig verhindern, dass ein auf Basis der Open-Source-Software entwickeltes Softwareprogramm

---

Open Source Software, N 2 ff.; WIDMER, urheberrechtliche Aspekte, 70 ff.).

162 WEBER, Freie Software, 42.

163 Übersicht über die verschiedenen Lizenzen unter www.gnu.org/licenses/.

164 Zur GNU-GPL vgl. WIDMER, urheberrechtliche Aspekte, 102 ff.

165 https://opensource.org.

166 ROWLAND/KOHL/CHARLESWORTH, IT Law, 519; WEBER, Freie Software, 42 f.

167 Ausführlich zu den Begriffen und der Entwicklung der Bewegungen statt vieler JAEGER/METZGER, Open Source Software, N 2 ff.

168 FRÖHLICH-BLEULER, Softwareverträge, N 1926 f.; JAEGER/METZGER, Open Source Software, N 5 f.; ROWLAND/KOHL/CHARLESWORTH, IT Law, 520.

169 Vgl. JAEGER/METZGER, Open Source Software, N 5; WIDMER, urheberrechtliche Aspekte, 16.

proprietär weitervertrieben werden kann.[170] Es gibt OSS-Lizenzen mit strengem[171], beschränktem[172] oder ohne Copyleft[173] (wobei letztere als die liberalsten Lizenzen gelten).[174]

116 Trotz der kostenlosen Zurverfügungstellung des Quellcodes und umfangreicher Nutzungsrechte ist Open-Source-Software urheberrechtlich geschützt.[175] Gemäss Art. 2 Abs. 3 Urheberrechtsgesetz (URG)[176] sind Computerprogramme den urheberrechtlichen Werken gleichgestellt.[177] Auch völkerrechtlich sind Computerprogramme gemäss Art. 4 WIPO-Urheberrechtsvertrag[178] urheberrechtlich geschützt. Bei Open-Source-Software verzichtet der Urheber (wie bei gewöhnlichen Softwarelizenz-verträgen

---

170 JAEGER/METZGER, Open Source Software, N 5 f.; MARLY, Softwarerecht, N 955.

171 Strenges Copyleft bedeutet, dass die Software ausschliesslich mit der ursprünglichen Lizenz verbreitet werden darf (Bsp. GNU-GPL-3.0).

172 Beschränktes Coypleft bedeutet, dass die Software unter gewissen Bedingungen nicht unter der ursprünglichen Lizenz verbreitet werden darf (Bsp. GNU-LGP-3.0).

173 Kein Copyleft bedeutet, dass der Erwerber keinerlei Restriktionen bezüglich der Weiterverbreitung unter der ursprünglichen Lizenz unterliegt (Bsp. MIT-Lizenz).

174 FRÖHLICH-BLEULER, Open Source Compliance, N 2; JAEGER/METZGER, Open Source Software, N 5.

175 MARLY, Softwarerecht, N 943 ff.; ROWLAND/KOHL/CHARLESWORTH, IT Law, 520.

176 Bundesgesetz über das Urheberrecht und verwandte Schutzgesetze (Urheberrechtsgesetz, URG) vom 9. Oktober 1992, SR. 231.1.

177 CHERPILLOD, SHK URG, Art. 2 N 64; HILTY, Lizenzvertragsrecht, 26 f.; MORSCHER/DORIGO, Software-Lizenzverträge, 19.

178 WIPO-Urheberrechtsvertrag (WTC), abgeschlossen in Genf am 20. Dezember 1996, von der Bundesversammlung genehmigt am 5. Oktober 2007, Schweizerische Ratifikationsurkunde hinterlegt am 31. März 2008, in Kraft getreten für die Schweiz am 1. Juli 2008, SR 0.231.151.

auch[179]) jedoch auf die Geltendmachung gewisser Urheberrechte (bspw. alleiniges Vervielfältigungs- und Verbreitungsrecht).[180]

c) Abgrenzungen

117 Open-Source-Software ist von *Freeware*, *Public Domain Software* und *Shareware* zu unterscheiden.[181]

118 Bei der Freeware handelt es sich um kostenlose Software, bei der im Unterschied zur Open-Source-Software der Quellcode nicht zur Verfügung gestellt wird und die grundsätzlich nicht verändert werden darf.[182] Beispiel für Freeware ist der Microsoft Internet Explorer.

119 Der Begriff *Public Domain Software* stammt aus dem US-amerikanischen Recht. Darunter fallen diejenigen Werke, bei denen der Urheber auf sämtliche Rechte verzichtet hat (das Werk ist nicht mehr urheberrechtlich geschützt) und die Gemeingut darstellen.[183] Im Gegensatz zum US-amerikanischen Urheberrecht ist nach dem Schweizer Immaterialgüterrecht allerdings kein vollständiger Verzicht auf die Urheberrechte (Urheberpersönlichkeitsrechte) möglich; eine Public-Domain-Software kann daher nur nach Ablauf der Schutzfrist entstehen.[184] Im deutschen Recht wird die Nutzung einer Public-

---

179 Zu Softwarelizenzverträgen allgemein siehe MORSCHER/DORIGO, Software-Lizenzverträge, 19 ff.

180 Zu urheberrechtlichen Fragen vgl. MARLY, Softwarerecht, N 943 ff.; MORSCHER/DORIGO, Software-Lizenzverträge, 19 f.; WIDMER, urheberrechtliche Aspekte, 70 ff; KOCH, Open-Source-Software (I), 275 ff.

181 Hilfreiche Tabelle zu Sonderformen der Softwareüberlassung bei MARLY, Softwarerecht, N 942.

182 CHIAMPI OHLY, Softwarerecht, 328; JAEGER/METZGER, Open Source Software, N 9; MARLY, Softwarerecht, N 940.

183 CHIAMPI OHLY, Softwarerecht, 327 f.; JAEGER/METZGER, Open Source Software, N 8.

184 Gem. Art. 29 Abs. 2 lit. a URG nach Ablauf von 50 Jahren nach dem Tod des Urhebers oder der Urheberin, vgl. CHIAMPI OHLY, Softwarerecht, 328; JAEGER/METZGER, Open Source Software, N 8; REUTTER GERSTER, SHK URG, Art. 29 N 10 f; WEBER, Freie Software, 42.

Domain-Software als einfaches Nutzungsrecht für jedermann mit unbeschränkter Verwertung ausgelegt.[185]

120 Shareware hingegen ist ein Vermarktungskonzept, wobei die Software für eine bestimmte Dauer (Testphase) dem Nutzer unentgeltlich zur Verfügung gestellt wird. Im Anschluss besteht die Möglichkeit des Erwerbs einer Nutzungslizenz.[186] Shareware ist grundsätzlich an eine herkömmliche Softwarelizenz geknüpft.[187]

d) Blockchain als Open-Source-Software

121 Viele der Blockchain-Quellcodes werden open source (weiter-) entwickelt; d.h. sie sind unter einer OSS-Lizenz veröffentlicht. So ist bspw. die Bitcoin-Blockchain unter der MIT-Lizenz[188] lizenziert.[189] Auch die Ethereum-Blockchain ist als Open-Source-Software ausgestaltet, so ist bspw. Go Ethereum[190] unter GNU-LGPL 3.0[191], Applikationen teilweise unter GNU-GPL lizenziert und die *Middleware*[192] steht unter GNU Affero-Lizenz.[193] Hyperledger, die Industrie-Blockchain, ist ebenfalls eine Open-Source-Software; sie läuft unter der Apache-Lizenz 2.0.[194] Die Banken-Blockchain des

---

185 CHIAMPI OHLY, Softwarerecht, 328; JAEGER/METZGER, Open Source Software, N 8.

186 CHIAMPI OHLY, Softwarerecht, 328; JAEGER/METZGER, Open Source Software, N 10; MARLY, Softwarerecht, N 919 ff.

187 JAEGER/METZGER, Open Source Software, N 10.

188 MIT steht für Massachusetts Institute of Technology.

189 https://bitcoin.org/de/ (Hinweis zur Lizenzierung am Seitenende).

190 Go Ethereum ist eine der drei originären Möglichkeiten zur Implementierung des Ethereum-Protokolls, vgl. https://geth.ethereum.org.

191 https://geth.ethereum.org.

192 Middleware ist ein Vermittlungsprogramm, sie steht zwischen der Anwender- und der Betriebssoftware und sie stellt das Funktionieren von verschiedenen Applikationen sicher: FRÖHLICH-BLEULER, Softwareverträge, N 32.

193 https://github.com/ethereum/wiki/wiki/Licensing.

194 https://github.com/hyperledger/fabric/blob/master/LICENSE; zur Apache License 2.0 siehe JAEGER/METZGER, Open Source Software, N 102 ff.

Konsortiums R3 hat ihre Blockchain Corda / R3-Corda nun ebenfalls als Open-Source-Software ausgestaltet; sie läuft unter der Apache-Lizenz 2.0.[195]

2. OSS-Lizenzvertrag

122 Wie vorgängig ausgeführt, wird Blockchain-Software in aller Regel unter OSS-Lizenzen angeboten. Nachfolgend wird dargelegt, wer bei einer Blockchain, die unter einer OSS-Lizenz steht, die Vertragsparteien sind und was der Vertragsgegenstand ist. Nicht ganz unumstritten in der Lehre ist der Zeitpunkt des Zustandekommens eines OSS-Lizenzvertrages, weshalb auch auf diese Frage kurz eingegangen wird. Im Anschluss daran wird anhand des charakteristischen Merkmals der Unentgeltlichkeit eine Vertragsqualifikation des OSS-Lizenzvertrages vorgenommen und kurz dargelegt, welche weiteren Vertragsbestandteile jeweils bei OSS-Lizenzen zu finden sind.

123 Software existiert nicht physisch. Wird sie auf einem physischen Datenträger (z.B. USB-Stick) verkörpert, dann hat diese Verkörperung keine Relevanz, da der Wert des Datenträgers kaum je von erheblichem Wert sein wird.[196] Die Unterscheidung, ob Software auf einem Datenträger oder online (*Download*, *Software-as-a-Service*) zur Verfügung gestellt wird, spielt in der Vertragsqualifikation keine Rolle. Der Europäische Gerichtshof stellt die Online-Übertragung von Software und die Aushändigung eines materiellen Datenträgers funktionell gleich.[197]

a) Vertragsparteien

124 Open-Source-Software kann grundsätzlich direkt vom Urheber oder einem Dritten erworben werden, je nachdem kostenlos zum Herunterladen oder allenfalls auch auf einem Datenträger.[198] Blockchain-Open-Source-Software

---

195 https://www.corda.net/downloads.

196 Vgl. HILTY, Rechtsnatur Softwarevertrag, 626; JAEGER/METZGER, Open Source Software, N 207; MORSCHER/DORIGO, Software-Lizenzverträge, 21.

197 Urteil EuGH vom 3. Juli 2012, C-128/11, *UsedSoft*, Rz. 61.

198 Vgl. JAEGER/METZGER, Open Source Software, N 202, 234, 249.

kann grösstenteils direkt von der Internetplattform *Github* oder direkt von der Website des Urhebers heruntergeladen werden und wird nicht auf Datenträgern vertrieben.

125 Wird die Open-Source-Software also von einem Dritten bezogen, können mehrere Vertragsverhältnisse entstehen: zwischen dem Entwickler (Urheber) und dem Nutzer; zwischen dem Entwickler und dem Dritten (Distributor, bei Blockchain-Software z.B. Github)[199] sowie zwischen dem Nutzer und dem Dritten.[200] Mit Nutzer sind vorliegend auch der Miner (N 101 ff.) sowie Wallet-Anbieter (N 104 ff.) gemeint; also grundsätzlich sämtliche Parteien, die einen Knotenpunkt betreiben. Von Interesse für die vorliegende Arbeit ist insbesondere das Verhältnis zwischen dem Nutzer und dem Entwickler, da der OSS-Lizenzvertrag zwischen diesen Parteien zustande kommt.

126 Nicht näher eingegangen wird auf das Vertragsverhältnis zwischen dem Dritten und dem Nutzer, da zwischen diesen Parteien kein Lizenzvertrag zustande kommt (Dritter ist nicht Urheber). Diese Konstellation wird bei kostenloser Zurverfügungstellung der Software in der deutschen Lehre als Schenkung klassifiziert.[201] Diese Ansicht kann auch für das Schweizer Recht gelten. Zwischen dem Urheber und dem Dritten kommt, wie zwischen dem Urheber und dem Nutzer, allenfalls ein OSS-Lizenzvertrag zustande (vgl. nachfolgend N 127), weshalb das nachfolgend Ausgeführte auch für diese Konstellation gilt.[202]

---

199 Zum Vertragsverhältnis zwischen Nutzer und Distributor vgl. JAEGER/METZGER, Open Source Software, N 173 ff., 251.

200 JAEGER/METZGER, Open Source Software, N 201 ff.; MARLY, Softwarerecht, N 959 ff.; POLEDNA/SCHLAURI/SCHWEIZER, Open Source Software in der öffentlichen Verwaltung, N 48.

201 JAEGER/METZGER, Open Source Software, N 251.

202 Vgl. JAEGER/METZGER, Open Source Software, N 251.

b) Vertragsgegenstand

127 Gegenstand des OSS-Lizenzvertrages ist sowohl der Quellcode des Programmes (die Software selbst) als auch das Nutzungsrecht daran.[203] Diese stellen theoretisch zwei verschiedene Vermögenswerte dar.[204] Diese Unterscheidung ergibt auf abstrakter Ebene Sinn, in praktischer Hinsicht jedoch weniger, da die beiden Vermögenswerte so eng aneinandergeknüpft sind, dass eine Trennung nicht zweckdienlich ist.[205] Gemäss JAEGER/METZGER ist jedoch die Unterscheidung dort angebracht, wo die Open-Source-Software nicht direkt vom Urheber, sondern von einer Drittpartei erworben wird. In diesen Fällen wird die Software vom Dritten übertragen, resp. kostenlos zur Verfügung gestellt (was gem. dt. Lehre eine Schenkung darstellt, vgl. vorhergehend N 123) und das Nutzungsrecht daran wird vom Urheber an den Nutzer übertragen.[206]

c) Zeitpunkt des Zustandekommens des OSS-Lizenzvertrages

128 Ein Vertrag kann nebst übereinstimmender Willenserklärung auch durch konkludentes Verhalten oder stillschweigend zustande kommen (Art. 1 OR).[207] Teilweise wird in OSS-Lizenzen ausdrücklich darauf hingewiesen, dass der Lizenzvertrag mit Nutzung der Software zustande kommt (z.B. Ziff. 5 GNU-GPL-1.0)[208] oder erst zu dem Zeitpunkt, wenn die Software verändert oder verbreitet wird (z.B. Ziff. 9 GNU GPL-3.0).[209] Enthält eine OSS-Lizenz eine

---

203 Nur Computerprogramm als Vertragsgegenstand: FRÖHLICH-BLEULER, Softwareverträge, N 1851.

204 JAEGER/METZGER, Open Source Software, N 203 f.

205 Vgl. Urteil EuGH vom 3. Juli 2012, C-128/11, *UsedSoft*, Rz. 44; HILTY, Rechtsnatur Softwarevertrag, 628.

206 JAEGER/METZGER, Open Source Software, N 252.

207 BERGER, Allgemeines Schuldrecht, N 236 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 177 ff.; SCHWENZER, OR AT, N 27.98 ff.; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 1 N 15 ff.

208 Vgl. FRÖHLICH-BLEULER, Softwareverträge, N 1857; WEBER, Open Source Software, 81.

209 Vgl. MEYER/SCHUPPLI, Smart Contracts, 211.

entsprechende Klausel, dann richtet sich der Zeitpunkt des Zustandekommens des Vertrages nach diesen Bestimmungen.

129 Enthält der OSS-Lizenzvertrag keine diesbezügliche Bestimmung (z.B. MIT-Lizenz), fragt sich, zu welchem Zeitpunkt der Lizenzvertrag zustande kommt. Open-Source-Software ist urheberrechtlich geschützt (vgl. N 115 f.), das heisst der Urheber kann grundsätzlich bestimmen, ob, wann und wie sein Werk verwendet werden darf (Art. 10 Abs. 1 Urheberrechtsgesetz, URG[210]), wobei gesetzliche Schranken für die Zustimmung vorgesehen sind. Gemäss dem Erschöpfungsgrundsatz in Art. 12 Abs. 2 URG darf der Erwerber der Software diese nutzen und weiterveräussern, wenn der Urheber ihm diese Software veräussert hat oder der Veräusserung zugestimmt hat.[211] Unter *bestimmungsgemässer Gebrauch* wird gem. Art. 17 Urheberrechtsverordnung (URV)[212] die bestimmungsgemässe Verwendung des Programms sowie dazugehörige Handlungen (laden, anzeigen, ablaufen, übertragen oder speichern etc.) erwähnt; es handelt sich dabei um das sog. Gebrauchsrecht.[213] Bei Open-Source-Software wird unter bestimmungsgemässem Gebrauch von der regulären Nutzung (inkl. dem Herunterladen und Kopieren) der Software ausgegangen, wobei die Weiterentwicklung und Weiterveräusserung nicht darunter fallen.[214] Sofern also der Erwerber die Open-Source-(Blockchain)-

---

210 Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG) vom 9. Oktober 1992, SR 213.1.

211 BARRELET/EGLOFF, URG-KOM, Art. 12 N 12.

212 Verordnung über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsverordnung, URV) vom 26. April 1993, SR 231.11.

213 Das Gebrauchsrecht enthält einen zwingenden Kern, welcher die Installation auf dem Arbeitsspeicher und die damit verbundene Vervielfältigung sowie Speicherung umfasst, damit der Nutzer die Software überhaupt benützen kann. Für weitere bestimmungsgemässe Elemente ist sodann eine Einzelfallbetrachtung der jeweiligen Software von Nöten. Vgl. ausführlich zum Gebrauchsrecht FRÖHLICH-BLEULER, Softwareverträge, N 146 ff.

214 FRÖHLICH-BLEULER, Softwareverträge, N 1854, 1857; JAEGER/METZGER, Open Source Software, N 182.

Software bestimmungsgemäss nutzt, ist davon auszugehen, dass für diese Nutzung kein Lizenzvertrag mit dem Urheber zustande kommt.

130 OSS-Lizenzen sind als Allgemeine Geschäftsbedingungen (AGB) ausgestaltet.[215] AGB sind einseitig vorformulierte Vertragsbedingungen, die nicht verhandelt werden können und sich so von einer Individualabrede unterscheiden.[216] AGB müssen, wie jeder andere Vertrag auch, vom Konsens beider Vertragsparteien getragen sein, d.h. sie müssen angenommen werden.[217] Bei AGB gilt die Global- oder Vollübernahme, je nachdem ob die akzeptierende Vertragspartei die AGB tatsächlich gelesen, verstanden und akzeptiert hat (Vollübernahme) oder die Möglichkeit bestand, den Inhalt mit zumutbarem Aufwand zu konsultieren, dieser jedoch ungelesen übernommen wird (Globalübernahme).[218] Bei elektronischem Vertragsschluss muss überdies die Möglichkeit bestehen, die AGB herunterzuladen, abzuspeichern und auszudrucken.[219] Diese Erfordernisse müssen auch bei jeder Blockchain-OSS-Lizenz erfüllt sein, damit ein OSS-Lizenzvertrag gültig zustande kommen kann.

d) Vertragstypologie

131 Der OSS-Lizenzvertrag ist (wie allgemein der Lizenzvertrag) nicht gesetzlich geregelt. Verträge, die weder im Besonderen Teil des Obligationenrechts (OR BT) noch in einem Spezialgesetz geregelt sind, werden Innominatverträge genannt. Dabei wird zwischen gemischten Verträgen und Verträgen *sui generis*

---

215 FRÖHLICH-BLEULER, Softwareverträge, N 1866; JAEGER/METZGER, Open Source Software, N 179.

216 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1117; KRAMER/PROBST/PERRIG, AGB, N 73; SCHWENZER, OR AT, N 44.01.

217 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1128; KRAMER/PROBST/PERRIG, AGB, N 86; SCHWENZER, OR AT, N 45.01.

218 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1128c; KRAMER/PROBST/PERRIG, AGB, N 86 f.; SCHWENZER, OR AT, N 45.01 ff.

219 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1135c; KRAMER/PROBST/PERRIG, AGB, N 90; SCHWENZER, OR AT, N 45.06a; WEBER, E-Commerce, 350.

unterschieden, wobei letztere Elemente enthalten, die in keinem gesetzlichen Vertragstyp vorkommen.[220]

132 Standard-Softwarelizenzverträge stellen im Schweizer Recht Innominatkontrakte dar, auch wenn sie zwischenzeitlich als „konstituiert" angesehen werden können.[221] Dabei werden je nach Typus Elemente des Pacht-, Miet-, Werkvertrag- und/oder Kaufrechts herangezogen.[222] Bei der vertragsrechtlichen Einordnung von Standard-Softwareverträgen gibt es in der Lehre grundsätzlich zwei Meinungen. Ein Teil der Lehre plädiert für die konsequente Anwendung von Lizenzvertragsrecht[223], da es sich bei Software um ein immaterielles Gut handle und daher lediglich Nutzungsbefugnisse eingeräumt werden können.[224] Der andere Teil der Lehre spricht sich hingegen für die Anwendung von Kaufrecht aus, da der Parteiwille sich jeweils auf einen einmaligen und dauerhaften Leistungsaustausch beziehe, man sich demgemäss also auf einen Kauf einige.[225] Der EuGH hat sich bezüglich Standard-Software für die Anwendung von Kaufrecht ausgesprochen.[226]

---

220 BERGER, Allgemeines Schuldrecht, 296 ff.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, 252; SCHWENZER, OR AT, 3.16.

221 HILTY, Softwarevertrag, 62 ff. m.w.H.; MORSCHER/DORIGO, Software-Lizenzverträge, 19 f.; WEBER, Open Source Software, 78.

222 MORSCHER/DORIGO, Software-Lizenzverträge, 29 ff.

223 Der Lizenzvertrag wird in mehreren Gesetzen erwähnt, jedoch nicht näher definiert. In der Lehre wird der Lizenzvertrag als Vertrag umschrieben, in dem sich der Lizenzgeber verpflichtet, dem Lizenznehmer ein Immaterialgut zu Gebrauch und Nutzung zu überlassen, in der Regel gegen eine Lizenzgebühr: AMSTUTZ/MORIN, BSK OR I, Einl. vor Art. 184 N 238; PROBST, der Lizenzvertrag, N 4; WEBER, Freie Software, 50 f.

224 HILTY, Rechtsnatur Softwarevertrag, 626; MORSCHER/DORIGO, Software-Lizenzverträge, 29; WEBER, Open Source Software, 79; WIDMER, Softwarepflegevertrag, 76.

225 Für eine Übersicht über den Meinungsstand ADLER, Rechtsfragen der Softwareüberlassung, 27 ff. m.w.H.; FRÖHLICH-BLEULER, Softwareverträge, N 1643 ff.; MORSCHER/DORIGO, Software-Lizenzverträge, 30.

226 Urteil EuGH vom 3. Juli 2012, C-128/11, *UsedSoft*.

133 Der OSS-Lizenzvertrag stellt wie der Standard- Softwarelizenzvertrag einen Innominatkontrakt dar.[227] Im Gegensatz zu Standard-Softwarelizenzverträgen ist bei einem OSS-Lizenzvertrag keine Vergütung (Gegenleistung) vorgesehen und auch die Verpflichtung, eine allfällige Weiterentwicklung ebenfalls kostenlos zur Verfügung zu stellen, ist atypisch für einen gewöhnlichen Softwarelizenzvertrag.[228] Aufgrund der fehlenden Entgeltlichkeit fallen die bei einem gewöhnlichen Softwarelizenzvertrag angenommenen Elemente des Kauf-, Miet-, Pacht- oder Werkvertrages bei einer OSS-Lizenz ausser Betracht.[229]

134 OSS-Lizenzen sind bezüglich der Einräumung von Rechten und Pflichten sehr unterschiedlich ausgestaltet und können daher nicht über einen Leisten geschlagen werden.[230] Charakteristisches Merkmal jeder OSS-Lizenz ist jedoch die Unentgeltlichkeit. Für die Analogieschlüsse zu Nominatkontrakten kommen daher nur diejenigen Verträge in Betracht, die die Unentgeltlichkeit als typisierendes Element beinhalten oder ein solches nicht ausschliessen. In Frage kommen daher die Schenkung, die Leihe oder der einfache Auftrag. Vorfrageweise ist zu prüfen, ob überhaupt ein vertragliches Verhältnis vorliegt oder allenfalls eine blosse Gefälligkeit.

aa) Gefälligkeit

135 Im Gegensatz zu einem Schuldvertrag besteht bei einer Gefälligkeit keinerlei Verpflichtung, diese zu erbringen.[231] Die Gefälligkeit ist laut Bundesgericht im Gegensatz zum Vertrag unentgeltlich, uneigennützig und erfolgt bei Gelegenheit, ohne dass eine rechtsgeschäftliche Verpflichtung zur Leistungserbringung besteht.[232] Die Gefälligkeit hat demgemäss ein altruistisches

---

227 WEBER, Freie Software, 46 ff.

228 WEBER, Freie Software, 51 f.; WEBER, Open Source Software, 78. Zum Softwarelizenzvertrag siehe HILTY, Softwarevertrag, 75 ff.; MORSCHER/DORIGO, Software-Lizenzverträge, 18 ff.

229 WEBER, Freie Software, 52.

230 Vgl. die umfassende Übersicht über die Ausgestaltung der einzelnen Lizenzen bei JAEGER/METZGER, Open Source Software, N 25 ff.

231 HÜRLIMANN-KAUP, privatrechtliche Gefälligkeit, N 108.

232 BGE 137 III 539 E. 4.1 S. 542 m.w.V.

Merkmal.[233] Ob eine Gefälligkeit oder ein Vertrag vorliegt, muss jeweils nach dem Willen der Parteien und dem Vertrauensprinzip ermittelt werden.[234] Dafür werden die Umstände des Einzelfalls betrachtet, namentlich die Art der Leistung, der Grund und Zweck, die rechtliche und wirtschaftliche Bedeutung, die Umstände, nach denen sie erbracht wurde und schliesslich die Interessenlage der Parteien.[235] Ein Bindungswille der Parteien wird verneint bei Gefälligkeitshandlungen des täglichen Lebens, bei Zusagen im rein gesellschaftlichen Verkehr oder bei ähnlichen Vorgängen.[236]

136 OSS-Lizenzen sind zwar unentgeltlich, jedoch ist ein altruistischer Charakter aufgrund der wirtschaftlichen Bedeutung von OSS-Lizenzen klar zu verneinen.[237] Auch kann die Nutzung oder die Weiterverbreitung einer Software, die unter einer OSS-Lizenz „erworben" wurde, nicht einer Gefälligkeitshandlung im täglichen Leben, dem gesellschaftlichen Verkehr oder einem ähnlichen Vorgang zugeordnet werden. OSS-Lizenzverträge sind gerichtlich durchsetzbar, was ebenfalls einer Qualifikation als Gefälligkeit widerspricht.[238]

bb) Schenkung

137 Als Schenkung gilt jede Zuwendung unter Lebenden, womit jemand aus dem Vermögen eines anderen ohne entsprechende Gegenleistung bereichert wird (Art. 239 Abs. 1 OR). Dazu benötigt der Schenker eine Schenkungsabsicht gegenüber dem Beschenkten, ohne dafür eine Gegenleistung erhalten zu wollen (subjektives Element) und der Beschenkte muss aus dem Vermögen des

---

233 WEBER, BSK OR I, Art. 419 N 9a.

234 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 353b.

235 BGE 137 III 539 E. 4.1 S. 542; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 353b; SCHWENZER, OR AT, N 4.46.

236 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 353b; SCHWENZER, OR AT, N 4.47.

237 Vgl. WEBER, Freie Software, 53; WEBER, Open Source Software, 77.

238 FRÖHLICH-BLEULER, Open Source Compliance, N 16 ff.; POLEDNA/SCHLAURI/SCHWEIZER, Open Source Software in der öffentlichen Verwaltung, N 100.

Schenkers bereichert werden (objektives Element).[239] Der Wert der geschenkten Sache sowie das Motiv sind unerheblich.[240]

138 In der deutschen Lehre wird bei OSS-Lizenzen teilweise von einer direkten oder analogen Anwendung des Schenkungsrechts ausgegangen.[241] In der Schweizer Lehre sind die Meinungen geteilt. Während teilweise der deutschen Lehre gefolgt und die Anwendung von Schenkungsrecht als gerechtfertigt angesehen wird,[242] verneint ein anderer Teil der Lehre eine analoge Anwendung von Schenkungsrecht.[243] So zweifelt WEBER bei einer schenkungsrechtlichen Qualifizierung am altruistischen Charakter von Nutzungsrechten bei Open-Source-Software; die Entwickler der Software würden regelmässig von einer gesteigerten Wertschöpfung (Pflege- und Wartungsfolgeaufträge) profitieren und auch strategische Zwecke seien nicht ausser Acht zu lassen.[244] Gegen die Annahme von Schenkungsrecht sprechen auch die unterschiedlichen Auflagen und Verpflichtungen in den OSS-Lizenzen, wie bspw. ein strenges Copyleft (N 115) oder die Beendigungsklauseln bei Nichteinhaltung von Lizenzbestimmungen. Gemäss Art. 245 OR können Schenkungen mit Auflagen verbunden werden, doch ist hier WEBERS Ansicht, das Auflagenkonzept der Schenkung würde bei einer Anwendung auf Open-Source-Software zu stark strapaziert, zuzustimmen: Ein Rückfall der Schenkung bei Nichteinhaltung der Auflage ist bei Open-Source-Software nicht möglich und die bedingungsgemässe Leistung (Zurverfügungstellung allfälliger Weiterentwicklungen unter gleichen Bedingungen) erfolgt nicht aus

239 VOGT/VOGT, BSK OR I, Art. 239 N 1.

240 VOGT/VOGT, BSK OR I, Art. 239 N 1.

241 JAEGER/METZGER, Open Source Software, N 205 ff.; MARLY, Softwarerecht, N 961 ff.; REDEKER, IT-Recht, N 595a ff.

242 FRÖHLICH-BLEULER, Softwareverträge, N 1879; POLEDNA/SCHLAURI/SCHWEIZER, Open Source Software in der öffentlichen Verwaltung, N 113; WEBER, Open Source Software, 89 (nur für Haftungsfragen bei isolierter Betrachtung der Einräumung von Nutzungsrechten).

243 WEBER, Open Source Software, 77 f.; für das dt. Recht KOCH, Open Source Software, 335; SESTER, Open Source Software, 799.

244 WEBER, Freie Software, 53; WEBER, Open Source Software, 77.

der Schenkung selbst.[245] Des Weiteren fehlt es am Element der Entreicherung des Schenkers, da die proprietären Rechte beim Urheber verbleiben und durch die Nutzungsrechte des Quellcodes keine Vermögensverminderung stattfindet.[246] Zudem fehlt im Falle von Open-Source-Software das Schrifterfordernis, sollte es eine Handschenkung darstellen.[247]

cc) Leihe

139 Obwohl die Leihe zwingend unentgeltlich ist, fällt eine entsprechende Subsumierung der OSS-Lizenz aufgrund der fehlenden Rückgabe nach erfolgter Nutzung an den Leihgeber sowie der Verpflichtung, eine allfällige Weiterentwicklung ebenfalls kostenlos zur Verfügung zu stellen, ausser Betracht.[248]

dd) Einfacher Auftrag

140 Die Unentgeltlichkeit der Open-Source-Software würde dem Wesen eines einfachen Auftrages gem. Art. 394 ff. OR nicht widersprechen, da eine Vergütung nicht zwingend vorgesehen ist (Art. 394 Abs. 1 OR). Der einfache Auftrag umfasst eine Arbeitsleistung und der Beauftragte hat eine bestimmte Tätigkeit zu erbringen.[249] Wesensmerkmale des einfachen Auftrages sind die Treuepflicht, ein besonderes Vertrauensverhältnis und ein Persönlichkeitsbezug.[250] Der Beauftragte ist verpflichtet, das ihm übertragene Geschäft vertragsgemäss zu besorgen.

141 Bei der OSS-Lizenz kommt als Tätigkeit i.S. des einfachen Auftrages die Nutzung der Software, eine allfällige Weiterentwicklung derjenigen sowie der kostenlose (Weiter-)Vertrieb (inkl. der Weiterentwicklung) in Frage. Die Treuepflicht sowie das besondere Vertrauensverhältnis und ein Persönlichkeitsbezug sind hingegen schwer zuzuordnen, da OSS-Lizenzen im Netz frei verfügbar sind und sich an einen offenen Personenkreis richten.

---

245 WEBER, Freie Software, 54.

246 Vgl. VOGT/VOGT, BSK OR I, Art. 239 N 1.

247 Zum Formerfordernis vgl. VOGT/VOGT, BSK OR I, Art. 243 N 1 ff.

248 Zur Leihe SCHÄRER/MAURENBRECHER, BSK OR I, Art. 305 OR N 1 ff.; WEBER, Freie Software, 52 f.; WEBER, Open Source Software, 77.

249 FELLMANN, BK OR, Art. 394 N 35; WEBER, BSK OR I, Art. 394 N 1.

250 WEBER, BSK OR I, Art. 394 N 3.

Zwischen dem Urheber und dem Nutzer (oder Weiterentwickler) besteht kein persönliches Verhältnis; meist hat der Urheber keine Kenntnis davon, wer seine unter einer OSS-Lizenz zur Verfügung gestellte Software nutzt, weiterentwickelt oder weitervertreibt.

ee) Zwischenfazit

142 Trotz des charakterisierenden Merkmals der Unentgeltlichkeit kann die OSS-Lizenz keinem gesetzlichen Vertragstyp zugeordnet werden, als charakteristisches Merkmal ebenfalls die Unentgeltlichkeit beinhaltet oder eine solche zumindest nicht ausschliesst. Es ist daher von einem unentgeltlichen Lizenzvertrag auszugehen; die analoge Anwendung von Schenkungsrecht, Bestimmungen über die Leihe oder des einfachen Auftrages sind abzulehnen.

e) Weitere Vertragsbestandteile

143 OSS-Lizenzen enthalten in der Regel Auflagen, die insbesondere mit der Weiterverbreitung und Weiterentwicklung der Software zusammenhängen, Beendigungsklauseln im Falle der Nichteinhaltung der Auflagen sowie umfassende Gewährleistungs- und Haftungsausschlüsse.

aa) Bedingung / Auflage

144 OSS-Lizenzen haben gemeinsam, dass ein Weitervertrieb der Software grundsätzlich erlaubt ist; dies meist unter der Auflage, dass die Weiterentwicklung oder der Weitervertrieb unter den gleichen Bedingungen gewährleistet wird, zu denen die Lizenz erworben wurde (sog. Copyleft, vgl. N 115 f.). Die Folge der Nichteinhaltung solcher Auflagen ist meist die Beendigung des Lizenzvertrages. Diese Bestimmungen sind grundsätzlich gerichtlich durchsetzbar, wobei in der Schweiz noch kein entsprechendes Urteil vorliegt.[251]

---

251 Vgl. FRÖHLICH-BLEULER, Open Source Compliance, N 16 ff.; JAEGER/METZGER, Open Source Software, 151 f. (m.H. auf dt. sowie US-amerikanische Urteile); POLEDNA/SCHLAURI/SCHWEIZER, Open Source Software in der öffentlichen Verwaltung, N 100.

bb) Haftungs- und Gewährleistungsausschlüsse

145 OSS-Lizenzen sind, wie bereits erwähnt, als AGB ausgestaltet (N 130) und enthalten umfassende Haftungs- und Gewährleistungsausschlüsse. Daneben sind teilweise (salvatorische) Klauseln anzutreffen, die bezüglich Freizeichnung subsidiär auf das anwendbare nationale Recht verweisen, sollten umfassende Freizeichnungen im nationalen Recht nicht gültig sein (z.B. Ziff. 17 GNU-GPL-3.0).[252]

146 Freizeichnungsklauseln in AGB sind dann unzulässig, wenn sie gegen die Bestimmungen von Art. 100 OR verstossen, das heisst, wenn sie eine Haftung auch für Vorsatz und grobe Fahrlässigkeit ausschliessen (Art. 100 OR).[253] Die Rechtsfolge von solchen Bestimmungen ist die Nichtigkeit (Art. 100 Abs. 1 OR).[254] Die Nichtigkeit betrifft in der Regel nur die entsprechende Bestimmung und nicht den ganzen Vertrag (Teilnichtigkeit), ausser es handelt sich bei dieser Bestimmung um das Kernstück des Vertrages.[255] Die nichtige Freizeichnungsklausel wird auf das gesetzlich erlaubte Mass reduziert, d.h. es besteht eine Haftung und Gewährleistung für Absicht und grobe Fahrlässigkeit.[256] Anders verhält es sich dann, wenn die in den AGB verankerten Freizeichnungsklauseln zulasten einer schwächeren Partei gehen; in diesen Fällen wird eine geltungserhaltende Reduktion von einem Teil der Lehre abgelehnt.[257] OSS-Lizenzverträge sind zwar als AGB ausgestaltet, doch kann hier nicht von einer stärkeren Position der Urheber ausgegangen werden, da den Nutzern einerseits freisteht, andere Software zu nutzen und diese im Alltag nicht unersetzlich ist und andererseits kostenlos zur Verfügung steht.

---

252 Vgl. JAEGER/METZGER, Open Source Software, N 221.

253 KRAMER/PROBST/PERRIG, AGB, N 279, 530; WIEGAND, BSK OR I, Art. 100 N 3 ff.

254 KRAMER/PROBST/PERRIG, AGB, N 530; WEBER, BK OR, Art. 100 N 156; WIEGAND, BSK OR I, Art. 100 N 3.

255 WEBER, BK OR, Art. 100 N 156.

256 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3082; WEBER, BK OR, Art. 100 N 156; WIEGAND, BSK OR I, Art. 100 N 4.

257 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3082; SCHWENZER, OR AT, N 32.45.

Dem Erwerber werden durch die OSS-Lizenz weitergehende Befugnisse eingeräumt und nicht eingeschränkt.

147 Die Freizeichnungsklausel in den OSS-Lizenzverträgen ist in Anwendung von Schweizer Recht also ungültig; es besteht demgemäss keine Freizeichnung für Vorsatz und grobe Fahrlässigkeit.

3. Fazit

148 Open-Source-Software ist ein Gegenkonzept zu Standard-Software und räumt dem Erwerber umfangreiche und weitgehende Nutzungs-, Vervielfältigungs-, Weiterentwicklungs- und Weiterverbreitungsrechte ein. Blockchain-Software wird fast ausschliesslich open source entwickelt. Open-Source-Software wird grundsätzlich lizenziert, wobei dieser OSS-Lizenzvertrag einen Innominatvertrag darstellt. Zusammenfassend kann festgehalten werden, dass ein OSS-Lizenzvertrag unentgeltlich und teilweise mit Auflagen versehen ist und umfangreiche Nutzungs- und Weiterverarbeitungsbefugnisse unter Ausschluss von Haftungs- und Gewährleistungsansprüchen erteilt. Trotz des charakteristischen Merkmals der Unentgeltlichkeit ist ein Analogieschluss zu Nominatverträgen nicht angezeigt; auch die Anwendung von Schenkungsrecht ist aufgrund der besonderen Ausgestaltung der Lizenzverträge abzulehnen.

149 Es ist daher von einem unentgeltlichen Softwarelizenzvertrag auszugehen. Es sind die von der Lehre entwickelten Grundsätze des Softwarelizenzvertragsrechts sowie die Allgemeinen Bestimmungen des Obligationenrechts heranzuziehen.

III. Blockchain als Plattform

150 Wird die Blockchain als Plattform verwendet, stellt sie die Infrastruktur dar, auf der Daten gespeichert werden. Diese Infrastruktur kann entweder durch ein reines P2P-Netzwerk betrieben werden oder als Betriebsplattform (operativer Dienst) eines Anbieters ausgestaltet sein.[258] Ist die Blockchain als operativer Dienst eingerichtet, der von einem Anbieter zur Verfügung gestellt wird, dann orientieren sich die vertraglichen Verhältnisse am jeweiligen Plattformvertrag. Auf dieses Verhältnis wird in der vorliegenden Arbeit nicht näher eingegangen, weil es einerseits eine neuere Erscheinung darstellt und andererseits bei privaten Blockchains die vertraglichen Verhältnisse mannigfaltig ausgestaltet sein können; eine entsprechende Abhandlung würde den Umfang dieser Arbeit sprengen. Wird die Plattform jedoch von einem P2P-Netzwerk betrieben – wie dies bei öffentlichen Blockchains der Fall ist –, dann ist zu prüfen, wie ein solches P2P-Netzwerk aus einer Schweizer Perspektive zivilrechtlich eingeordnet werden kann.

151 Wie bereits die ausführlichen Diskussionen zum Internet zeigten, sind weltweite und dezentrale P2P-Netzwerke nur schwer fassbar. Das hat u.a. dazu geführt, dass Verantwortlichkeiten dort angeknüpft werden, wo ein Zugang zum Netzwerk gewährt wird. Dies geschieht im Falle des Internet über Provider. Es wurden verschiedene Provider-Kategorien geschaffen, um je nach Konstellation die Verantwortlichkeit zu eruieren. Da die Blockchain als dezentrales P2P-Netzwerk ebenso schwer fassbar ist, ist zu prüfen, ob auch hier (zivilrechtliche) Verantwortlichkeiten dort angeknüpft werden müssen, wo der Zugang zu diesem Netzwerk ermöglicht wird.

---

258 BURGWINKEL, Blockchain Technology, 10 f.

1. P2P-Netzwerk

Nachfolgend wird das P2P-Netzwerk begrifflich eingeführt und seine Eigenschaften dargelegt. 152

a) Begriff

In das Bewusstsein der breiteren Öffentlichkeit rückten P2P-Netzwerke durch die Verbreitung des kostenlosen *Filesharing* (damals v.a. MP3-Musikdateien), welches weltweit betrieben werden konnte. Bekannte Beispiele für P2P-Netzwerke waren in den 90ern und anfangs der 2000er Jahre *Napster*[259] und *Gnutella*[260]. Auch das Internet war in seiner ursprünglichen Ausgestaltung ein P2P-Netzwerk.[261] Bei einem P2P-Netzwerk sind mehrere gleichberechtigte Nutzer (Endgeräte) miteinander direkt über ein Datennetz verbunden.[262] Im Unterschied zu den Client-Server-Diensten zeichnen sich P2P-Netzwerke durch eine bessere Skalierbarkeit (z.B. effizientes Wachstum in grossen Dimensionen), mehr Sicherheit und Verlässlichkeit (zensurresistente Speicherung sowie Schutz vor Angriffen auf zentrale Dienste) und mehr Flexibilität aus.[263] Die Nutzung erfolgt ohne zentrale Koordination und der 153

---

259 Napster Inc., bot die ursprüngliche Software zum kostenlosen Austausch von MP3 Musikdateien an; aufgrund von Urheberrechtsverletzungen und Klagen durch die Musikindustrie stellte die Plattform den Dienst 2002 definitiv ein; vgl. *A&M Records Inc. v. Napster Inc.*, 239 F.3d, 1004 (9th Cir. 2001).

260 Gnutella, als eines der beliebtesten dezentralen P2P-Netzwerke, gibt es in der ursprünglichen Form nicht mehr. Das Netzwerk wurde benutzt, um vielerlei Daten (nicht nur MP3) direkt zwischen den Nutzern auszutauschen.

261 ANTONOPOULOS, Mastering Bitcoin, 171.

262 ANTONOPOULOS, Mastering Bitcoin, 171; BERENTSEN/SCHÄR, Kryptoassets, 95; CREUTZ, virtuelle Welten, 9; SIXT, Transaktionssysteme, 13.

263 ROHN, Verantwortlichkeit der Provider, 44; STEINMETZ/WEHRLE, Peer-to-Peer-Networking, 51.

Zugriff auf die erforderlichen Betriebsmittel (z.B. Speicherplatz, Rechenleistung) erfolgt direkt zwischen den Teilnehmern.[264]

154 Bei P2P-Netzwerken kann zwischen zentralisierten und dezentralisierten Netzwerken unterschieden werden.[265] Bei zentralisierten Netzwerken laufen die Suchanfragen der Netzwerkteilnehmer über einen Server. Dieser speichert zwar selbst keine Daten, vermittelt aber zwischen den Teilnehmern. Bei einem dezentralen P2P-Netzwerk existiert keine Zentraleinheit; die Teilnehmer sind untereinander direkt vernetzt.[266] Rechtlich betrachtet fanden P2P-Netzwerke meist im Zusammenhang mit Urheberrechtsverletzungen Beachtung (vgl. N 157).[267] In öffentlichen Blockchains werden für die Aufrechterhaltung der Infrastruktur dezentralisierte P2P-Netzwerke eingesetzt.[268]

b) Eigenschaften

155 Ein P2P-System zeichnet sich durch folgende Eigenschaften aus:

- Jeder Knotenpunkt (Endgerät, Nutzer) stellt Ressourcen zur Verfügung und nutzt Ressourcen, wie bspw. Rechenleistung, Speicherkapazität, Bandbreite;
- Das Netzwerk ist dynamisch; es können jederzeit Knotenpunkte hinzukommen oder wegfallen, die „Mitgliedschaft“ ist dynamisch ausgestaltet, was sich auf die Stabilität und Robustheit des Netzwerkes auswirkt;
- Die einzelnen Mitglieder des Netzwerkes sind i.d.R. autonom, d.h. sie entscheiden selbst, ob und wie lange sie in einem P2P-Netzwerk bleiben und welche Ressourcen sie zur Verfügung stellen;

---

264 STEINMETZ/WEHRLE, Peer-to-Peer-Networking, 52.

265 ENGELHARDT, Urheberrechtsverletzungen, 26; SIXT, Transaktionssysteme, 13.

266 ANTONOPOULOS, Mastering Bitcoin, 171; ENGELHARDT, Urheberrechtsverletzungen, 26 f.

267 Siehe ausführlich dazu ENGELHARDT, Urheberrechtsverletzungen, 190 ff.

268 ANTONOPOULOS, Mastering Bitcoin, 171; BERENTSEN/SCHÄR, Kryptoassets, 95; SIXT, Transaktionssysteme, 13.

- P2P-Netzwerke sind oft als *Overlay Network* des Internet ausgestaltet, d.h. das Internet gewährleistet den Zugriff und die Verbindung zwischen den einzelnen Knotenpunkten.[269]

2. Gesellschaftsrechtliche Aspekte eines P2P-Blockchain-Netzwerkes

156 Am Anfang eines P2P-Blockchain-Netzwerks steht die Entwicklung der entsprechenden Software. Wenn der Entwickler diese unter einer OSS-Lizenz veröffentlicht hat, dann richtet sich das vertragliche Verhältnis zwischen den einzelnen Nutzern und dem Entwickler nach diesen Lizenzbestimmungen (vgl. vorhergehend N 122 ff.). Durch diese Open-Source-Software sind die Nutzer in der Lage, sich als P2P-Netzwerk zu konstituieren.

157 Bis anhin wurden P2P-Netzwerke insbesondere im Zusammenhang mit der Verletzung von Urheberrechten (z.B. Austausch urheberrechtlich geschützter Werke wie Filme oder Musik) einer genaueren rechtlichen Betrachtung unterzogen.[270] Als bekanntestes Beispiel ist das Verfahren gegen Napster zu

---

269 EFFELSBERG/STEINMETZ/LEHN, Peer-to-Peer Systems, 4; vgl. BGer Urteil 6B_757/2010 vom 7. Februar 2011, E.1, S. 3 (Verletzung von Urheberrechten, Gehilfenschaft); vgl. ANTONOPOULOS, Mastering Bitcoin, 139 f.

270 Bei Urheberrechtsverletzungen durch Nutzer eines P2P-Netzwerkes stellen sich in der Schweiz folgende Probleme: Pflichten zur Verhinderung von Urheberrechtsverletzungen, wie sie bspw. Hosting- oder Accessprovider haben (zur Providerhaftung vgl. RIGAMONTI, Providerhaftung, 119 ff.), sind gegenüber P2P-Netzwerken nicht durchsetzbar, da sie eine dezentrale und weltweit verteilte Struktur aufweisen (N 24). Ein direktes Vorgehen gegen die einzelnen Nutzer gestaltet sich aufgrund der fehlenden Identifikation als schwierig; eine gezielte Auswertung von IP-Adressen ist seit dem *Logistep*-Urteil (BGE 136 II 508; Logistep hat IP-Adressen von P2P-Netzwerken ausgewertet, um betroffenen Urheberrechtsinhabern die Verfolgung ihrer Ansprüche ermöglichen zu können) aus datenschutzrechtlichen Gründen (derzeit) nicht möglich (vgl. RIGAMONTI, Providerhaftung, 129 f.

nennen.[271] Bei der Beurteilung der urheberrechtlichen Problemstellungen wurde die Frage, wie die Gemeinschaft der Knotenpunkte (zivil)rechtlich einzuordnen ist, jeweils ausser Acht gelassen. Dies liegt nicht zuletzt daran, dass ein P2P-Netzwerk in seiner dezentralen und globalen Ausgestaltung in juristischen Kategorien nur sehr schwer fassbar ist. Ein P2P-Blockchain-Netzwerk ist unbestrittenermassen eine Art Gemeinschaft. Nachfolgend wird nun geprüft, ob ein solches Netzwerk einer dem Schweizer Recht bekannten Gesellschaftsform zugeordnet werden kann.

a) Körperschaft

158 Eine Qualifikation als juristische Person des Schweizer Rechts kommt für ein P2P-Netzwerk nicht in Frage: Für Körperschaften gibt es einen *numerus clausus* der möglichen Gesellschaftsformen.[272] Sie müssen eine gewisse organisatorische Struktur (verschiedene Organe) aufweisen und gewisse zwingende Bestimmungen zur Gründung einer solchen Gesellschaft einhalten.[273] So sind bspw. Kapitalgesellschaften ohne (menschliche, nicht computergenerierte) Oberleitung nicht zulässig.[274] Ein P2P-Netzwerk basiert in der Regel auf der Gleichberechtigung aller beteiligten Parteien: es gibt keine Organe. Zwingende Bestimmungen zur Gründung einer Körperschaft sind aufgrund der Natur eines solchen Netzwerkes zu verneinen.

b) Personengesellschaft

159 Nebst Körperschaften gibt es auch Personengesellschaften. Diese sind, wie es der Name schon sagt, personenbezogen ausgestaltet und besitzen im Gegensatz zu Körperschaften keine eigene Rechtspersönlichkeit.[275] Die Grundformen der

---

271 *A&M Records Inc. v. Napster Inc.*, 239 F. 3d, 1004 (9th Cir. 2001).

272 AG (Art. 620 ff. OR), Kommandit-AG (Art. 764 ff. OR), GmbH (Art. 722 ff. OR), Genossenschaft (Art. 828 ff. OR), Verein (Art. 60 ff. ZGB), SICAV (Art. 26 ff. KAG) oder SICAF (Art. 110 ff. KAG).

273 Vgl. MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §2 N 49 ff.

274 BAYERN U.A., Gesellschaftsrecht und autonome Systeme, 194; JUNG, ZK OR, Art. 625 N4 und 36.

275 MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §2 N 81; VONZUN, Personengesellschaft, N 393 ff.

Personengesellschaften sind die einfache Gesellschaft (Art. 530 ff. OR), die Kollektivgesellschaft (Art. 522 ff. OR) sowie die Kommanditgesellschaft (Art. 594 ff. OR). Daneben existiert die Spezialform der Kommanditgesellschaft für kollektive Kapitalanlagen (Art. 98 ff. KAG).[276] Die Kommandit- und die Kollektivgesellschaft sind Handelsgesellschaften mit dem Zweck des Betriebes eines kaufmännisch geführten Gewerbes.[277] Diese Zweckbestimmung trifft auf ein P2P-Netzwerk, insbesondere ein P2P-Blockchain-Netzwerk, nicht zu; diese beiden Gesellschaftsformen sind folglich auszuschliessen. Gleich verhält es sich mit der Kommanditgesellschaft für kollektive Kapitalanlagen, deren einziger Zweck die kollektive Kapitalanlage ist (vgl. Art. 98 Abs. 1 KAG).

160 Die einfache Gesellschaft ist die Grundform der Personengesellschaften und dient als Auffangbecken, wenn keine andere Gesellschaftsform zum Tragen kommt.[278] Sie wird in der Folge genauer untersucht.

c) Einfache Gesellschaft

161 Wie erwähnt ist die einfache Gesellschaft eine vertragliche Personengemeinschaft, deren Regelungen subsidiär zur Anwendung gelangen, wenn andere Gesellschaftsformen ausgeschlossen werden können.[279] Eine einfache Gesellschaft ist gem. Art. 530 Abs. 1 OR die Verbindung von zwei oder mehr Personen zur Erreichung eines gemeinsamen Zweckes mit gemeinsamen Mitteln oder Kräften.

aa) Zwei oder mehr Personen

162 Erforderlich für die Gründung einer einfachen Gesellschaft sind zwei oder mehr Personen, wobei juristische Personen Teil einer einfachen Gesellschaft

---

276 Vgl. DU PASQUIER/POSKRIAKOV, BSK KAG, Art. 98 N 1 ff.; JUNG/KUNZ/BÄRTSCHI, Gesellschaftsrecht, §7 N 3.

277 JUNG/KUNZ/BÄRTSCHI, Gesellschaftsrecht, §7 N 39.

278 FELLMANN/MÜLLER, BK OR, Art. 530 N 133; MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §12 N 34.

279 FELLMANN/MÜLLER, BK OR, Art. 530 N 27 ff. und 133; MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §12 N 34; SCHÜTZ, SHK OR, Art. 530 N 1.

sein können.[280] In einem P2P-Blockchain-Netzwerk sind mehrere Akteure involviert. Es sind dies die unterschiedlichen Knotenpunkt-Betreiber, d.h. die Nutzer (N 99 f.), die Miner (N 101 ff.) und/oder die Wallet-Anbieter (N 104 ff.).[281] Daneben können noch weitere Parteien involviert sein, wie bspw. Börsen oder andere Handelsplätze. Bei einem P2P-Blockchain-Netzwerk sind in der Regel zwei oder mehr Parteien involviert.

bb) Vertragsmässige Verbindung

163 Die vertragliche Verbindung der Parteien muss nicht bewusst erfolgen; es kann auch Teil einer einfachen Gesellschaft werden, wer sich dessen nicht bewusst ist.[282] Zwingend ist jedoch der Rechtbindungswille mindestens einer Partei. Einen beidseitig unbewussten und ungewollten Vertragsschluss gibt es nicht.[283] Die Verbindung zur einfachen Gesellschaft kann formfrei zustande kommen.[284] Inhaltlich besteht die vertragliche Vereinbarung aus der Einigung über die Zweckverfolgung und der Beitragspflicht.[285]

164 Die Abgrenzung zu Austauschverhältnissen oder zu Personenverbindungen ohne rechtlichen Bindungswillen (lose Gesellschaft) ist nicht evident. Lose Gesellschaften ohne Bindungswillen werden als kurzfristige Verbindung geselligen Charakters umschrieben.[286] Hier ist jeweils eine Einzelbetrachtung erforderlich, wobei als Abgrenzungskriterien auch die Art des Projektes sowie dessen wirtschaftliche Bedeutung heranzuziehen sind.[287]

---

280 HANDSCHIN, BSK OR II, Art. 530 N 3.

281 Vgl. für das Bitcoin-Netzwerk ANTONOPOULOS, Mastering Bitcoin, 172 ff.

282 HANDSCHIN, BSK OR II, Art. 530 N 2. BGer Urteil 4A_27/2008 vom 9. Mai 2008 E. 2.3.

283 BGer Urteil 4C.24/2000 vom 28. März 2000 E. 3d; FELLMANN/MÜLLER, BK OR, Art. 530 N 61 und 440 ff; HANDSCHIN, BSK OR II, Art. 530 N 2.

284 HANDSCHIN, BSK OR II, Art. 530 N 2; VONZUN, Personengesellschaft, N 506 f.; vgl. BGE 96 II 325 S. 332 E.6c.

285 HANDSCHIN, BSK OR II, Art. 530 N 2.

286 FELLMANN/MÜLLER, BK OR, Art. 530 N 434; MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §1 N 62 f.

287 HÜRLIMANN-KAUP, privatrechtliche Gefälligkeit, 103 ff.

165 Bei P2P-Blockchain-Netzwerken ist es grundsätzlich möglich, nur für eine kurze Dauer Mitglied zu werden. Die Motivation für die Teilnahme an einem P2P-Blockchain-Netzwerk ist jedoch kaum je geselligen Charakters, sondern eher profitstrebender Natur. Je nach Ausgestaltung der Blockchain steht dabei die Speicherung und Übertragung von Daten oder Vermögenswerten (wobei es sich bei Vermögenswerten streng genommen auch um Daten handelt) im Vordergrund und es gibt, wie einleitend dargelegt, verschiedene Rollen, die in einem solchen Netzwerk eingenommen werden können (N 96 ff.). Es kann bei sämtlichen involvierten Parteien ein Motiv ausgemacht werden, das über einen geselligen Charakter hinausgeht. Generell wollen Nutzer ihre Daten in einem sicheren (und transparenten) System übertragen und speichern. Miner stellen ihre Rechenleistung zur Verfügung, um Transaktionen zu verifizieren und erhalten dafür eine Transaktionsgebühr (z.B. bei der Bitcoin-Blockchain durch die Nutzer und das System selbst [N 181], bei Ethereum durch die Nutzer [N 178]). Die Wallet-Anbieter verwalten Schlüssel (und Adressen) der Nutzer und führen teilweise selbst Transaktionen durch (vgl. N 104 ff.); auch bei ihnen kann kein geselliger Charakter in Bezug auf diese Dienstleistungen ausgemacht werden, sondern ein wirtschaftlicher. Insgesamt kann also von einem wirtschaftlichen Nutzen aller Teilnehmer des P2P-Blockchain-Netzwerkes ausgegangen werden. Das wiederum lässt auf einen Rechtsbindungswillen der Teilnehmer schliessen, auch wenn nur ein kurzzeitiger Beitritt zum Netzwerk vorliegt.

166 Das mit Blick auf die Miner an ein Austauschverhältnis erinnernde Konstrukt oder das vorliegende Abhängigkeitsverhältnis von Leistung und Gegenleistung (Rechenleistung gegen Kryptowährung) spricht nicht per se gegen die Annahme einer einfachen Gesellschaft. Es steht nämlich nicht der Austausch, d.h. die wechselseitige Erbringung von Leistungen, im Vordergrund, sondern vielmehr die koordinierte Zusammenführung der Leistungen.[288]

167 Zusammenfassend kann festgehalten werden, dass ein Rechtsbindungswille und somit eine vertragsmässige Verbindung bei Teilnehmern von P2P-Blockchain-Netzwerken angenommen werden kann.

[288] Vgl. FELLMANN/MÜLLER, BK OR, Art. 530 N 70.

cc) Gemeinsamer Zweck mit gemeinsamen Mitteln

168 Die Zweckverfolgung einer einfachen Gesellschaft kann wirtschaftlicher oder ideeller Natur sein.[289] Der gemeinsame Zweck geht dabei über das Interesse der reinen Vertragserfüllung hinaus: Er wird nicht mit den gemeinsamen Mitteln, sondern mittels der vorgesehenen Leistungen erreicht.[290] In Abgrenzung zu einem Austauschvertrag ist zu untersuchen, ob es sich wirklich um einen gemeinsamen Zweck oder lediglich um ein gemeinsames Motiv für den Vertragsschluss handelt.[291] Sobald das Motiv gemäss dem gemeinsamen Willen der Beteiligten zur Pflicht wird, liegt der gemeinsame Zweck im Umfang der gemeinsamen Pflichtverfolgung.[292] Entscheidend ist also der gemeinsame Wille zur Verfolgung des Zweckes.

169 Bei einem P2P-Blockchain-Netzwerk orientiert sich die Zweckverfolgung an der Ausgestaltung der Blockchain. Als grundsätzliche Zweckverfolgung jeder Blockchain kann die Schaffung und Aufrechterhaltung des Netzwerkes genannt werden – denn ohne Teilnehmer, die Rechenleistung zur Verfügung stellen und somit ein dezentrales System schaffen, gibt es keine Plattform. Als weiterer Zweck kann die dauerhafte und transparente Speicherung von Daten genannt werden. Die gemeinsamen Mittel sind dabei die von jedem einzelnen Knotenpunkt zur Verfügung gestellten Ressourcen, welche die dezentrale Speicherung der gesamten Systemdaten ermöglichen. Die von den Minern geleisteten Validierungen von Transaktionen stellen hingegen keine gemeinsamen Mittel dar, da sie separat vergütet werden (vgl. N 61, 178, 181).

---

289 HANDSCHIN, BSK OR II, Art. 530 N 4; MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §12 N 35 f.; BGE 99 II 315 S. 322 E. 5b; Urteil des Bundesgerichts 9C_455/2008 vom 5. November 2008 E. 5.

290 HANDSCHIN, BSK OR II, Art. 530 N 5.

291 HANDSCHIN, Abgrenzung einfache Gesellschaft, 112; vgl. MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §12 N 19 f.

292 HANDSCHIN, Abgrenzung einfache Gesellschaft, 113.

dd) Fehlende Identifizierbarkeit der Gesellschafter

170 Die einfache Gesellschaft ist eine Personengesellschaft, bei der die Persönlichkeit der Gesellschafter im Vordergrund steht.[293] Dies spielt insbesondere bei der Zweckerreichung eine Rolle, welche durch den Einsatz der persönlichen Eigenschaften der Gesellschafter geprägt ist.[294] Auch die Treue- und Sorgfaltspflichten sowie die Haftung sind personenbezogen ausgestaltet.[295]

171 Die Teilnehmer eines P2P-Netzwerkes kennen sich grundsätzlich nicht persönlich (vgl. N 28 ff.). Die einzelne Person spielt aber insofern eine Rolle, als ohne sie (resp. das von ihr zur Verfügung gestellte Endgerät) das P2P-Blockchain-Netzwerk nicht bestehen würde. Bei einem P2P-Blockchain-Netzwerk ist die Rolle der einzelnen Teilnehmer ambivalent: grundsätzlich herrscht Gleichberechtigung und das Netzwerk ist ohne Teilnehmer nicht funktionsfähig. Gleichzeitig ist aber durch die dezentrale Struktur und die jederzeitige Möglichkeit des Ein- und Austrittes jeder einzelne Teilnehmer austauschbar. In dieser Art des virtuellen Zusammenschlusses spielt die Persönlichkeit, im Sinne der Identifizierbarkeit der Personalien und die persönliche Bekanntschaft, eine untergeordnete, wenn nicht sogar gar keine Rolle. Bei einer generellen Betrachtung eines P2P-Blockchain-Netzwerks lässt sich feststellen, dass einzig die zur Verfügung stehenden Ressourcen in Form von Rechenleistung für das Funktionieren des Netzwerks von Interesse sind. Mit einer Personengesellschaft, auch in der abgewandelten Form einer virtuellen Personengesellschaft, können keine Gemeinsamkeiten mehr festgestellt werden.[296]

---

293 FELLMANN/MÜLLER, BK OR, Art. 530 N 172; vgl. HANDSCHIN, BSK OR II, Art. 530 N 6.

294 FELLMANN/MÜLLER, BK OR, Art. 530 N 172; JUNG, CHK-OR, Art. 530 N 23.

295 FELLMANN/MÜLLER, BK OR, Art. 530 N 173 ff.

296 Anders aber bei einer blockchainbasierten Anwendung einer DAO (vgl. Anhang, N 37 f.), wie bspw. „The DAO“, wo zusätzlich Abstimmungen über gemeinsame Investitionen getätigt werden: GYR, DAO, N 31 f.

d) Fazit

172 Bei einem P2P-Blockchain-Netzwerk können die Kriterien des Rechtsbindungswillens der Teilnehmer und der gemeinsamen Zweckverfolgung mit gemeinsamen Mitteln bejaht werden. Ein Analogieschluss zur einfachen Gesellschaft ist unter gewissen Vorbehalten also nicht per se ausgeschlossen. Jedoch wird der Begriff der Personengesellschaft in dieser virtuellen Form (zu) sehr strapaziert, da ein Personenbezug praktisch nicht mehr vorhanden ist.

173 Folglich ist bei einem P2P-Blockchain-Netzwerk von einer Gemeinschaft auszugehen, die zwar einen gemeinsamen Zweck mit gemeinsamen Mitteln verfolgt; allerdings geschieht dies ausserhalb eines juristisch fassbaren Konstruktes. Es handelt sich vielmehr um einen losen Zusammenschluss, zu dem ein jederzeitiger Ein- und Austritt möglich ist. Die Gemeinschaft bleibt nur so lange bestehen, wie Teilnehmer gewillt sind, daran teilzunehmen. Rechte und Pflichten richten sich nach dem vorgegebenen System (Software), wobei durch die Teilnehmer grundsätzlich keine Einflussmöglichkeit besteht[297] und auch keine verbindlichen Rechte und Pflichten ausgemacht werden können – ausser der Entrichtung einer Transaktionsgebühr für die Validierung einer Transaktion durch die Miner.[298]

3. Vertragsverhältnis innerhalb des P2P-Netzwerkes

174 Wie im vorangehenden Kapitel aufgezeigt, ist das P2P-Blockchain-Netzwerk den im Schweizer Recht bekannten Gesellschaftsformen schwerlich zuzuordnen. Es ist daher angezeigt, einzelne Vertragsverhältnisse innerhalb

---

297 Eine Einflussmöglichkeit besteht insofern, als durch die Teilnehmer ein neues oder abgewandeltes System geschaffen werden kann, wobei für dieses System wiederum genügend Teilnehmer gefunden oder überzeugt werden müssen, damit es betrieben werden kann (z.B. durch Hard Fork [Anhang, N 36] oder durch die Mehrheit der Knotenbetreiber, die die aktualisierte Software übernehmen, ohne dass es zum Hard Fork kommt).

298 Es besteht grundsätzlich kein Anrecht darauf, dass eine Transaktion „gemint“ wird; dies ist jedoch im System impliziert.

des P2P-Blockchain-Netzwerkes zu eruieren. Wie bereits angesprochen, sind die Teilnehmer einer öffentlichen Blockchain grundsätzlich gleichberechtigt. Es besteht jedoch die Möglichkeit, unterschiedliche Funktionen einzunehmen, wie z.B. als Miner oder als Wallet-Anbieter. Da Miner für die Validierung der Transaktionen besorgt sind und dafür eine Gebühr kassieren, ist das Verhältnis zwischen Miner und Nutzer näher zu betrachten. Der Wallet-Anbieter verwaltet die Schlüssel und Adressen von Nutzern, primär jedoch nur von solchen ausserhalb des P2P-Netzwerkes. Nutzer besitzen auch ein Wallet, welches jedoch in ihrem Knotenpunkt als Anwendung integriert ist und nicht über einen Drittanbieter läuft. Daher wird eine gesonderte Betrachtung des Verhältnisses zwischen Nutzer und Wallet-Anbieter an dieser Stelle nicht vorgenommen (vgl. jedoch N 198 ff.).

175 Als mögliches gesondertes Vertragsverhältnis kommt also lediglich das Verhältnis zwischen Nutzer und Miner in Betracht. Da Miner eine zentrale Rolle in der Blockchain übernehmen und Nutzer ausserhalb der Blockchain die grösste Nutzergruppe darstellen, wird in einem Exkurs noch der Frage nachgegangen, wie das Verhältnis zwischen Miner und Nutzer ausserhalb der Blockchain vertraglich qualifiziert werden könnte.

a) Vertragsverhältnis Nutzer – Miner

176 Wenn Nutzer ihre Transaktionsdaten in die Blockchain aufnehmen lassen wollen, müssen diese vorgängig validiert werden (N 61 ff.), was Miner übernehmen.[299] Dafür werden sie in irgendeiner Form (i.d.R. mit Kryptowährung), entweder durch die an der Transaktion beteiligten Parteien und/oder durch das System selbst, entschädigt.

177 Um zu prüfen, ob zwischen dem Nutzer und dem Miner ein vertragliches Verhältnis entsteht, ist eine Einzelbetrachtung der verschiedenen Blockchain-Netzwerke vorzunehmen, da die Konsensprotokolle und das Mining sehr unterschiedlich ausgestaltet sein können. Nachfolgend wird beispielhaft auf die Ethereum-Blockchain und die Bitcoin-Blockchain eingegangen.

---

299 MEYER/SCHUPPLI, Smart Contracts, 212.

aa) Ethereum-Blockchain

178 Der Nutzer bestätigt eine Transaktion mittels Signatur, welche anschliessend im Transaktionspool zwischengespeichert wird, bis sie von einem Miner validiert und anschliessend in die Transaktionskette aufgenommen wird (vgl. N 61 ff.). Das System (Software) bestimmt für jede Transaktion den Rechenaufwand, welcher in Gas[300] angegeben wird. Ebenfalls berechnet es die Höhe der Transaktionsgebühr für den Rechenaufwand. Dem Nutzer steht es zwar grundsätzlich frei, in welcher Höhe er den Miner dafür entschädigen möchte.[301] Hierbei ist jedoch zu beachten, dass eine Unterschreitung des vom System vorgerechneten Preises nicht ratsam ist, da die Transaktion ansonsten mit hoher Wahrscheinlichkeit nicht von einem Miner bearbeitet und folglich auch nicht in die Transaktionskette aufgenommen wird.[302] Der Nutzer und der Miner kennen sich nicht und treten auch nie in Kontakt.

179 Bei diesem Verhältnis zwischen dem Nutzer und dem Miner könnte es sich um eine Auslobung gem. Art. 8 OR handeln.[303] Eine Auslobung ist ein einseitiges Rechtsgeschäft, ein Versprechen zu Gunsten eines unbestimmten Personenkreises, zu dem sich der Versprechende für den Fall einer bestimmten Leistung zur Ausrichtung einer Belohnung verpflichtet.[304] Vorausgesetzt wird eine öffentliche Erklärung, die sich an eine Vielzahl von Personen richten muss und

---

300 Gas ist eine Einheit für die Berechnung der Rechenkapazität. Aus dem Gas-Wert kann ein Wert in der Kryptowährung Ether berechnet werden, welche vom Nutzer als Transaktionsgebühr an den Miner bezahlt werden muss (der Gas-Preis bewegt sich zwischen ca. 2 und 50 GWEI [Bezeichnung für die viertkleinste Einheit von Ether], je nachdem, wie schnell die Transaktion in die Blockchain aufgenommen werden soll); vgl. MEYER/SCHUPPLI, Smart Contracts, 212.

301 Vgl. MEYER/SCHUPPLI, Smart Contracts, 212.

302 MEYER/SCHUPPLI, Smart Contracts, 212.

303 MEYER/SCHUPPLI, Smart Contracts, 214.

304 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1041; vgl. SCHWENZER, OR AT, N 28.52 f.; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 8 N 1.

nicht bloss an einzelne Interessenten gerichtet sein darf.[305] Sodann ist die Auslobung bedingt. Erforderlich ist eine beliebig geartete Leistung der Gegenpartei.[306] Die Belohnung kann aus Geld oder auch aus einer anderen Leistung bestehen.[307] Grundsätzlich ist bei der Auslobung ein Widerruf möglich, wobei eine allfällige Schadenersatzpflicht gemäss Art. 8 Abs. 2 OR besteht.[308]

180 Die Voraussetzungen der Auslobung sind vorliegend gegeben: Der Nutzer bestätigt seine Transaktion und setzt die Transaktionsgebühr fest. Diese Transaktionsgebühr ist die ausgeschriebene Belohnung dafür, dass eine Transaktion durch einen Miner validiert wird. Die signierte Transaktion befindet sich im Transaktionspool, wo sie für alle Miner der Ethereum-Blockchain zugänglich ist (vgl. N 58). Die Ansetzung der Belohnung für die Transaktionsvalidierung ist also öffentlich, da auch die Ethereum-Blockchain grundsätzlich öffentlich ist und es jedermann offensteht, an dieser als Miner teilzunehmen. Die Leistung, die von Minern erbracht werden muss, ist die Validierung der Transaktion. Der Nutzer hat grundsätzlich keinen Einfluss auf die tatsächliche Validierung seiner Transaktion; er kann lediglich durch die Höhe der Transaktionsgebühr einen Anreiz setzen.

bb) Bitcoin-Blockchain

181 Beim Bitcoin-Netzwerk wird dem Miner sein Rechenaufwand zweimal vergütet: einmal durch eine im System hinterlegte, vordefinierte Anzahl Bitcoins[309] und einmal durch eine Transaktionsgebühr, die von den Nutzern zu bezahlen ist.[310] Den Hauptanreiz für das Mining stellen derzeit noch die vom

---

305 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1042; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 8 N 17.

306 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1043; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 8 N 10 ff.

307 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1044; KRAMER/SCHMIDLIN, BK OR, Art. 8 N 31.

308 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1048; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 8 N 38 f.

309 Der vom System bezahlte Betrag wird kleiner, umso mehr Bitcoins bereits gemint sind, vgl. ANTONOPOULOS, Mastering Bitcoin, 214.

310 ANTONOPOULOS, Mastering Bitcoin, 214.

System neu ausgegeben Bitcoins dar.[311] Bei der Bitcoin-Blockchain werden so lange neue Bitcoins ausgegeben, bis die vordefinierten Summe von 20.99999998 Millionen Bitcoins erreicht ist; danach werden sich Miner für die Validierung von Transaktionen ausschliesslich über Gebühren finanzieren können.[312]

182 Die Transaktionsgebühr, die vom Nutzer an den Miner bezahlt wird, kann wie bei der Ethereum-Blockchain vom Nutzer selbst angesetzt werden. Auch sonst ist der Ablauf identisch (N 178). Zwischen dem Nutzer und dem Miner entsteht also wie bei der Ethereum-Blockchain ein einseitiges Rechtsgeschäft in Form einer Auslobung (N 179 f.).

b) Exkurs: Vertragsverhältnis Miner – Nutzer ausserhalb des Netzwerkes

183 Wie bereits dargelegt, werden in der vorliegenden Arbeit nur diejenigen Parteien als Teilnehmer der Blockchain-Plattform verstanden, die auch tatsächlich Teil des P2P-Netzwerkes sind, in dem sie einen Knotenpunkt betreiben (vgl. N 162). Die Nutzer ausserhalb der Blockchain-Plattform (welche faktisch die grösste Gruppe darstellen), die nur punktuell auf das Netzwerk zugreifen, wurden in den bisherigen Ausführungen nicht berücksichtigt.

184 Solange das P2P-Netzwerk keiner vertragsfähigen Gemeinschaft zugerechnet werden kann,[313] ist auch das Eingehen eines Schuldverhältnisses mit diesem Netzwerk nicht möglich, da hierfür die Rechts- und Geschäftsfähigkeit beider Vertragsparteien vorliegen muss.[314] In diesen Fällen ist zwischen den Nutzern ausserhalb der Blockchain und den Minern wie beim Verhältnis Nutzer-Miner (zumindest bei der Bitcoin- und Ethereum-Blockchain) ebenfalls von einer Auslobung gem. Art. 8 OR auszugehen (N 176 ff.), wobei das Angebot des Nutzers ausserhalb der Blockchain mangels eigenem Zugang zum Netzwerk in

---

311 Derzeit noch ca. 12.5 Bitcoins pro Block.

312 ANTONOPOULOS, Mastering Bitcoin, 214.

313 Vgl. vorhergehend zum P2P-Netzwerk als einfache Gesellschaft Kapitel C.II, N 157 ff.

314 Zur Rechts- und Geschäftsfähigkeit vgl. Kapitel E.II., N 277 ff.

den meisten Fällen via Wallet-Anbieter (Bote, vgl. N 416) in die Blockchain gestellt wird.

185 Vorgängig wurde die Qualifizierung des P2P-Blockchain-Netzwerkes oder eine analoge Anwendung von Regeln der einfachen Gesellschaft abgelehnt (vgl. N 157 ff.). Würde man jedoch der Annahme folgen, dass es sich beim P2P-Blockchain-Netzwerk um eine einfache Gesellschaft handelt, wäre zu prüfen, ob ein Miner gegenüber den aussenstehenden Nutzern des Netzwerkes in Stellvertretungsfunktion (nachfolgen N 186 f.) oder als Erfüllungsgehilfe (nachfolgend N 188) der Gesellschaft handelt.

aa) Stellvertretung

186 Die einfache Gesellschaft wird gegen aussen nicht als Gesellschaft (da sie kein Rechtssubjekt darstellt), sondern durch die Gesamtheit der Gesellschafter vertreten.[315] Bei einer einfachen Gesellschaft gilt die Vermutung, dass der geschäftsführende Gesellschafter Vertretungsbefugnis besitzt (Art. 543 Abs. 3 OR). Ist kein solcher bestimmt, sind alle Gesellschafter gleichermassen vertretungsbefugt (Art. 535 Abs. 1 OR). Bei der einfachen Gesellschaft sind die Regeln der Stellvertretung anwendbar, sofern der gegen aussen auftretende Gesellschafter im Namen aller Gesellschafter handelt (Art. 543 Abs. 2 OR).[316] Die Stellvertreter müssen überdies von der Gesellschaft dazu ermächtigt worden sein (Art. 543 Abs. 2 i.V.m. Art. 32 OR).[317]

187 Bei der Bitcoin-Blockchain wie auch bei der Ethereum-Blockchain sind keine Organe vorgesehen.[318] Es gibt demgemäss auch keinen geschäftsführenden

---

315 MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §12 N 62; PESTALOZZI/VOGT, BSK OR II, Art. 543 N 1.

316 MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §12 N 62; PESTALOZZI/VOGT, BSK OR II, Art. 530 N 5.

317 Vgl. MEIER-HAYOZ/FORSTMOSER, Gesellschaftsrecht, §12 N 62 f.; PESTALOZZI/VOGT, BSK OR II, Art. 530 N 7 ff.

318 Faktisch verhält es sich jedoch so, dass einzelne Akteure (Bitcoin-Core-Entwickler und Miningpools) einen wesentlichen Einfluss auf die Anpassungen und Änderungen des Systems haben, sei es durch ihre Reputation als Entwickler, sei es durch ihre vorherrschende Stellung im

Gesellschafter. Miner treten gegen aussen auch nicht in Erscheinung. Die zu bearbeitenden Transaktionen werden gesammelt und von den Minern anonym abgearbeitet.[319] Da die Miner den Nutzern gegenüber also nicht in Erscheinung treten, agieren sie somit auch nicht als Stellvertreter des Netzwerkes.

bb) Hilfsperson

188 Wenn die Schuldnerin (hier: das P2P-Netzwerk) ihre Schuldpflicht nicht persönlich, sondern durch einen Dritten erfüllen lässt, kann es sich bei dem Dritten um eine Hilfsperson handeln (vgl. Art. 101 OR).[320] Eine Hilfsperson kann der Schuldnerin bei der Erfüllung lediglich unterstützen oder alleine, aber nach der Einzelanweisung der Schuldnerin erfüllen. Der Hilfsperson kann auch die selbständige Erfüllung des Geschäftes übertragen werden.[321] Notwendige Voraussetzung für die Hilfspersonenstellung ist ein bestehendes Schuldverhältnis der Geschäftsherrin mit einer Vertragspartei.[322] Für die Annahme einer Hilfspersonenstellung ist erforderlich, dass die Hilfsperson mit Einwilligung der Schuldnerin handelt; auf das Innenverhältnis kommt es indessen nicht an.[323] Die Qualifizierung als Hilfsperson spielt insbesondere dort eine Rolle, wo ein Schaden entsteht; der durch die Hilfsperson verursachte Schaden muss in einem funktionellen Zusammenhang zu der durch den Geschäftsherrn übertragenen Aufgabe stehen.[324]

System durch eine grosse Anzahl Knotenpunkte und der zur Verfügung stehender Rechenkraft.

319 Vgl. für das Bitcoin-Netzwerk ANTONOPOULOS, Mastering Bitcoin, 220 f.

320 BERGER, Allgemeines Schuldrecht, N 1768; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3016; SCHWENZER, OR AT, N 23.04.

321 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3021 ff.; WEBER, BK OR, Art. 101 N 45 ff.

322 Im Normalfall ein Vertragsverhältnis, ausnahmsweise aber auch aus einem anderen Rechtsgrund wie Gesetz oder Vertragsverhandlung: GAUCH/ SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3030.

323 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3027 f.; SCHWENZER, OR AT, N 23.04; WEBER, BK OR, Art. 101 N 48.

324 Vgl. BERGER, Allgemeines Schuldrecht, N 1775; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3032 ff.; SCHWENZER, OR AT, N 23.09.

c) Fazit

189 Ob zwischen dem P2P-Netzwerk (als Geschäftsherrin) und dem Nutzer ausserhalb der Blockchain ein Schuldverhältnis besteht, muss im Einzelfall und je nach Blockchain betrachtet werden. Für die Bitcoin- und die Ethereum-Blockchain kann wie bereits dargelegt nicht von einem zweiseitigen Vertragsverhältnis ausgegangen werden: Das System gibt zwar vor, unter welchen Bedingungen eine Transaktion als valide eingestuft wird und wie der Validierungsmechanismus vorgenommen werden muss, der Nutzer hat aber grundsätzlich keinen Anspruch darauf, dass seine Transaktion validiert und in die Blockchain aufgenommen wird (N 176 ff.).[325] Es ist vielmehr (zumindest in Bezug auf die Bitcoin- und Ethereum-Blockchain) von einem einseitigen Rechtsgeschäft in Form der Auslobung gem. Art. 8 OR auszugehen (N 176 ff.). Da zwischen dem P2P-Netzwerk und dem Nutzer ausserhalb der Blockchain kein Schuldverhältnis besteht, kann einem Miner keine Hilfspersonenstellung des P2P-Netzwerkes zukommen.

[325] Siehe für den Transaktionsmechanismus bei der Bitcoin-Blockchain ANTONOPOULOS, Mastering Bitcoin, 22 ff.

4. Zugang zum P2P-Blockchain-Netzwerk

190 Wie in den ersten Abschnitten des vorliegenden Kapitels erwähnt, sind P2P-Blockchain-Netzwerke dezentral ausgestaltet und die Teilnehmer pseudoanonym. Die Gemeinschaft ist in juristischen Kategorien nicht klar fassbar (vgl. N 157 ff.). Die gleiche Problematik stellte sich bereits mit dem Aufkommen des Internet. Bei rechtswidrigem Verhalten im Internet, bspw. bei einer Urheberrechts- oder Persönlichkeitsverletzung, war und ist nicht nur die Eruierung des Täters ein Problem,[326] sondern auch die nicht in juristischen Kategorien fassbare Netzwerkgemeinschaft.[327] Für das Internet als Netzwerk wurde jedoch keine neue Gesellschaftsform geschaffen, sondern die Verantwortlichkeit dort angeknüpft, wo Zugang zu diesem Netzwerk gewährt wird. Für die Zugänge zum Internet wurden Providerkategorien geschaffen, die zusammengefasst *Internet Service Provider (ISP)* genannt werden.

a) Internet Service Provider

191 Es kann grundsätzlich zwischen *Content*, *Host*, und *Access Provider* unterschieden werden, wobei teilweise auch andere Begriffe benutzt werden.[328] Der Content Provider hält auf seinem eigenen Server (oder auf dem eines Host Providers) eigene oder fremde Inhalte zum Abruf oder Herunterladen bereit.[329] Wenn ein Dritter seine Informationen bei einem Content Provider ablegt, dann beinhaltet dies nebst Content oftmals auch Host Providing.[330]

---

326 U.a. auch aus datenschutzrechtlichen Gründen, vgl. BGE 136 II 508 (Logistep-Urteil).

327 RIGAMONTI/WULLSCHLEGER, Teilnahme an Urheberrechtsverletzungen, 48.

328 Vgl. die verschiedenen Definitionen im Bundesratsbericht vom 11. Dezember 2015, 17 ff.; zur Herleitung der Wortbedeutungen FERCSIK SCHNYDER, Internet-Access-Providing-Verträge, 28 ff., 34 ff.

329 ROHN, Verantwortlichkeit der Provider, 18; WEBER, E-Commerce, 500; Bundesratsbericht vom 11. Dezember 2015, 17.

330 ROHN, Verantwortlichkeit der Provider, 24; WEBER, E-Commerce, 500, 516.

192 Host Provider stellen Dritten Speicherkapazität und Kommunikationsfunktionen zur Verfügung, damit diese ihre Inhalte im Internet bereithalten können.[331] Dabei wird jeweils davon ausgegangen, dass der Host Provider die Herrschaft über die Daten via die Herrschaft über den Server, auf dem die entsprechenden Informationen gespeichert sind, innehat.[332]

193 Im Gegensatz zum Host und Content Provider hat der Zugangsvermittler zum Inhalt, der Access Provider, keine Herrschaft über die Server, auf dem die fremden Daten gespeichert sind.[333] Der Access Provider ermöglicht grundsätzlich den Zugang zum Internet, meist gegen Entgelt und zusätzliche Dienstleistungen (bspw. E-Mail).[334]

b) Internet-Provider-Haftung

194 Die Haftung von ISP ist umstritten und nicht gesetzlich geregelt.[335] Der Bundesrat hat in einem Bericht 2015 auch ausdrücklich auf eine gesetzliche Regelung der zivilrechtlichen Verantwortlichkeit von Providern verzichtet.[336] Es geht bei der Providerhaftung grundsätzlich um eine Haftung für das Verhalten von Dritten, wobei seitens der in Recht gefassten Partei (Provider) keine direkte schädigende Handlung vorliegt.[337] Es kann dabei zwischen negatorischen Ansprüchen (z.B. Unterlassung), reparatorischen Ansprüchen

---

331 ROHN, Verantwortlichkeit der Provider, 24; Bundesratsbericht vom 11. Dezember 2015, 17.

332 ROHN, Verantwortlichkeit der Provider, 24 f.; siehe auch FERCSIK SCHNYDER, Internet-Access-Providing-Verträge, 38.

333 ROHN, Verantwortlichkeit der Provider, 32 f.; vgl. WEBER, E-Commerce, 507; FERCSIK SCHNYDER, Internet-Access-Providing-Verträge, 34.

334 ROHN, Verantwortlichkeit der Provider, 233; THOUVENIN U.A., Netzsperren, 718; vgl. Bundesratsbericht vom 11. Dezember 2015, 17 f.; FERCSIK SCHNYDER, Internet-Access-Providing-Verträge, 34 f.

335 Vgl. KERNEN, Verantwortlichkeit Host Provider, N 13 ff. (in Besprechung des BGer Urteil 5A_792/2011 vom 14. Januar 2013); PRAZELLER, Mitwirkungsbegriff, N 14 ff.; THOUVENIN, Vergleichs- und Bewertungsdienste, 146; THOUVENIN U.A., Netzsperren, 718.

336 Bundesratsbericht vom 11. Dezember 2015, 4.

337 RIGAMONTI, Providerhaftung, 117.

(z.B. Schadenersatz) oder Auskunftsansprüchen gegenüber den ISP unterschieden werden.[338]

195 Bei negatorischen Ansprüchen ist grundsätzlich umstritten, ob ISP eine Teilnahmehandlung (Tun oder Unterlassen) zur Verhinderung von rechtsverletzendem Verhalten trifft. Der Bundesrat geht dabei von einem Tun aus, d.h. der Provider setzt durch das Bereitstellen seines Angebots eine aktive Ursache für die widerrechtliche Handlung eines Dritten;[339] die Lehre differenziert mehrheitlich und verweist auf eine Einzelfallbetrachtung.[340] Negatorische Ansprüche können durch eine Beseitigung des Inhalts auf dem Server oder durch eine Beschränkung des Zugangs mittels Sperren erreicht werden.[341] Es ist jedoch jeweils zu beachten, dass nicht alle Provider die Möglichkeit haben, Inhalte zu löschen und Sperren (von IP- oder DNS-Adressen[342]) bekanntermassen einfach zu umgehen sind und der Nutzen von solchen daher fraglich ist.[343]

196 Reparatorische Ansprüche gegenüber einem Provider werden über Art. 50 OR hergeleitet.[344] Hierbei stellt insbesondere die Frage nach der Verletzung einer Sorgfaltspflicht eine besondere Herausforderung dar, da in der Schweiz weder gesetzliche Regelungen noch eine konkretisierende Rechtsprechung zur

---

338 Bundesratsbericht vom 11. Dezember 2015, 12.

339 Bundesratsbericht vom 11. Dezember 2015, 28 (Herleitung eines Tuns auch durch BGer Urteil 5A_792/2011 vom 14. Januar 2013, mit dem Argument, dass das Bundesgericht durch die Nichtbehandlung dieser Frage stillschweigend von einem Tun ausgegangen ist).

340 RIGAMONTI, Providerhaftung, 119 ff.; ROHN, Verantwortlichkeit der Provider, 82; WEBER, E-Commerce, 508 f.

341 Bundesratsbericht vom 11. Dezember 2015, 44, 47.

342 Jedes an das Internet angeschlossene System besitzt eine IP-Adresse; diese ist eine Kombination aus Zahlen (z.B. 19.324.33.1). DNS steht für Domain Name System und stellt für Nutzer lesbare Namen dar, die einer IP-Adresse zugeordnet werden (z.B. www.adresse.ch); vgl. THOUVENIN U.A., Netzsperren, 704.

343 Eingehend zu Netzsperren THOUVENIN U.A., Netzsperren, 701 ff.

344 Bundesratsbericht vom 11. Dezember 2015, 60; Vgl. RIGAMONTI, Providerhaftung, 50; ROHN, Verantwortlichkeit der Provider, 100.

Sorgfaltspflicht von ISP vorliegt.[345] Private Regelwerke[346] und Lehre weisen hierbei auf Regelungen aus dem Ausland hin, insbesondere auf die *E-Commerce-Richtlinie*[347] der EU.[348] Erst wenn eine Sorgfaltspflichtverletzung des Providers bejaht wird, kann allenfalls eine solidarische Haftung gem. Art. 50 OR (unter Erfüllung der übrigen Voraussetzungen) zustande kommen.[349]

197 Im Zivilrecht kann kein Anspruch gegen Unbekannt anhängig gemacht werden und die ZPO sieht keine Möglichkeit vor, an die Identität eines Rechtsverletzers zu gelangen. Auskunftsansprüche spielen daher insbesondere im Strafrecht eine Rolle; indirekt ist dies jedoch auch für das Zivilrecht relevant, da via Strafprozess die Identität des Täters festgestellt und im Anschluss ein Zivilprozess eingeleitet werden kann.[350] Von Interesse ist in der Praxis insbesondere die Auskunft von Providern über die Identität von Personen aus P2P-Netzwerken, in denen urheberrechtliche Verletzungen begangen werden (vgl. N 154).[351]

c) Wallet-Anbieter als Provider?

198 Es ist zu prüfen, ob analog zu den für das Internet geschaffenen Providerkategorien zivilrechtliche Verantwortlichkeiten ebenfalls dort

---

345 Bundesratsbericht vom 11. Dezember 2015, 62.

346 Z.B. der von der SWISS INTERNET INDUSTRY ASSOCIATION (SIMSA) ausgearbeitete Code of Conduct Hosting (abrufbar unter: https://www.simsa.ch/_Resources/Persistent/53642eb64a0552851325159 6c00840097445f789/ 130201-simsa-cch-public-web.pdf).

347 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABl. EG Nr. L 178/1.

348 Vgl. RIGAMONTI, Providerhaftung, 124; WEBER, E-Commerce, 517.

349 Vgl. Bundesratsbericht vom 11. Dezember 2015, 65.

350 Bundesratsbericht vom 11. Dezember 2015, 79.

351 Vgl. RIGAMONTI, Providerhaftung, 128; RIGAMONTI/WULLSCHLEGER, Teilnahme an Urheberrechtsverletzungen, 54.

angeknüpft werden können, wo Zugang zu einem P2P-Blockchain-Netzwerk geschaffen wird. In der Praxis wird der Zugang zu einer Blockchain oft durch Wallet-Anbieter gewährt, da die wenigsten Nutzer einer Blockchain die gesamte Blockchain heruntergeladen haben und ihre Private Keys selbst verwalten. Daneben wird der Zugang grundsätzlich ebenfalls über die Internet-Provider hergestellt, da Blockchain-Netzwerke (vereinfacht ausgedrückt) Teil des Internet sind.

199 Wie einleitend erwähnt gibt es Software- und auch Hardware-Wallets (vgl. N 104 ff.). Unterschieden werden kann zudem bei Software-Wallets auch danach, ob das Wallet einen vollständigen Knotenpunkt unterhält, der den Zugang zum Netzwerk gewährleistet (Full Node), ob es über einen sog. *Lightweight Client* handelt, der für Informationen über das Netzwerk mit den Full Nodes kommuniziert aber selber die Daten seiner Nutzer speichert oder Wallets, die keinen direkten Zugang zum Netzwerk haben, sondern sich diesen wiederum über eine Drittpartei einholen (sog. *Third Party API client*).[352] Hardware-Wallets sind externe Geräte, die lediglich zur sicheren Aufbewahrung der Schlüssel dienen und selbst keinerlei Verbindung zum Internet oder Netzwerk aufbauen (vgl. N 104); über diese wird also kein Zugang zum Netzwerk hergestellt. Nachfolgend wird bei der Verwendung des Begriffs *Wallet* daher jeweils von Software-Wallets ausgegangen.[353]

200 Ein Wallet-Anbieter verfügt in der Regel über eine Kopie der Blockchain auf seinem Rechner (Full Node oder *SPV Node*, FN 134). Als Knotenbetreiber der Blockchain ist er selbst Teil des P2P-Netzwerkes. Der Inhalt, der den Nutzern zur Verfügung gestellt wird, ist also eine Mischung aus eigenen sowie fremden Inhalten, was einer Mischung von Content und Host Providing entsprechen würde. Ein Wallet-Anbieter hat jedoch keine Kontrolle über die Daten, resp. keine Herrschaft über den Server, auf dem die Daten gespeichert sind, da die

---

352 ANTONOPOULOS, Mastering Bitcoin, 7 f.; BERENTSEN/SCHÄR, Kryptoassets, 314 f.; SIXT, Transaktionssysteme, 36.

353 Wallet-Software ist meist unter einer Open-Source-Software veröffentlicht (vgl. Auflistung bei BERENTSEN/SCHÄR, Kryptoassets, 316). Der Nutzer und der Wallet-Anbieter stehen allenfalls in einem lizenzvertraglichen Verhältnis, vgl. zum OSS-Lizenzvertrag Kapitel C.II., N 115 ff.

Daten gerade nicht zentral, sondern dezentral verteilt im P2P-Netzwerk abgespeichert sind. Es ist einem Wallet-Anbieter in keiner Weise möglich, auf diese Daten Einfluss zu nehmen; er kann lediglich Zugang dazu vermitteln. Die Funktion der Wallet-Anbieter ist also ähnlich wie die eines Access Providers, nur erfolgt die Zugänglichmachung in der Regel unentgeltlich.

d) Fazit

Bei einem Wallet-Anbieter könnte für die Zugänglichmachung zu einem P2P-Blockchain-Netzwerk die Funktion eines Access Providers angenommen werden. Er wäre folglich auch der Providerhaftung ausgesetzt. 201

5. Fazit

Ist die Blockchain-Plattform als dezentrales und verteiltes P2P-Netzwerk ausgestaltet, kann sie keiner dem Schweizer Recht bekannten vertraglichen Form zugeordnet werden – auch eine Qualifikation als einfache Gesellschaft ist aufgrund der Ausgestaltung abzulehnen. 202

Das Verhältnis zwischen Miner und Nutzer ist je nach Blockchain-Plattform verschieden; bei der Bitcoin- sowie der Ethereum-Blockchain kann ein vertragliches Verhältnis in Form einer Auslobung gem. Art. 8 OR angenommen werden. 203

Auch für das Verhältnis zwischen den Nutzern ausserhalb der Blockchain und den Minern kann ein einseitiges Rechtsgeschäft in Form einer Auslobung angenommen werden – zumindest gilt dies für die Bitcoin- und Ethereum-Blockchain. Wenn von der Annahme ausgegangen wird, dass das P2P-Blockchain-Netzwerk eine einfache Gesellschaft darstellt, kann zwischen dem Netzwerk und dem Nutzer ausserhalb der Blockchain keine vertragliche Verbindung eruiert werden; den Minern kommt in dieser Konstellation weder eine Stellvertreter- noch eine Hilfspersonenstellung zu. 204

Werden aufgrund der fehlenden Annahme von vertraglichen Verhältnissen bei der Blockchain in ihrer Funktion als Plattform die für die Internethaftung geschaffenen Providerkategorien betrachtet, kann bei Wallet-Anbietern eine 205

Funktion als Access Provider hergeleitet werden. Ein Wallet-Anbieter könnte sich demgemäss mit Ansprüchen aus der Providerhaftung konfrontiert sehen.

IV. Fazit

206 Bei der Blockchain als Software wie auch bei der Blockchain als Plattform können verschiedene vertragliche Verhältnisse festgestellt werden.

207 Blockchain-Software ist open source ausgestaltet und unter entsprechenden Lizenzbestimmungen veröffentlicht. Zwischen den Knotenbetreibern (Nutzer, Miner, Wallet-Anbieter) kann mit dem Urheber der Software zumindest dann ein OSS-Lizenzvertrag entstehen, wenn die Blockchain-Software über das normale Gebrauchsrecht hinaus benutzt wird. Bei einem OSS-Lizenzvertrag ist von einem unentgeltlichen Softwarelizenzvertrag auszugehen; es sind die von der Lehre entwickelten Grundsätze des Softwarelizenzvertragsrechts sowie die Allgemeinen Bestimmungen des Obligationenrechts heranzuziehen.

208 Die Blockchain als Plattform wird bei öffentlichen Blockchains durch ein P2P-Netzwerk aufrechterhalten. Dieses Netzwerk ist keiner der im Schweizer Recht bekannten Gesellschaftsformen zuzuordnen. Es handelt sich um einen losen Zusammenschluss, der zwar ein gemeinsames Ziel mit gemeinsamen Mitteln verfolgt, jedoch keinerlei Rechte und Pflichten begründet.

209 Innerhalb des P2P-Netzwerkes besteht zwischen den Minern und den Nutzern und den Nutzern ausserhalb der Blockchain ein einseitiges Rechtsgeschäft in Form einer Auslobung gem. Art. 8 OR.

210 Die Wallet-Anbieter gewähren Nutzern ausserhalb der Blockchain Zugang zur Blockchain, weshalb ihnen die Funktion eines Access Providers zukommt. Daraus folgt, dass dem Wallet-Anbieter allenfalls Ansprüche aus der Providerhaftung geltend gemacht werden können.

2. Teil: Smart Contracts

Nachdem im ersten Teil der Arbeit die Blockchain-Technologie auf ihre technischen und vertragsrechtlichen Aspekte untersucht worden ist, gilt das Hauptaugenmerk in diesem zweiten Teil einer konkreten Anwendungsform der Technologie: dem Smart Contract. 211

Im Einführungsteil wird zunächst eine historische und begriffliche Einordnung des Smart Contract vorgenommen, gefolgt von einem Definitionsversuch und einer Beschreibung der grundlegenden Funktionsweise; im anschliessenden Teil wird sodann geprüft, ob mit Smart Contracts direkt Verträge abgeschlossen werden können. Die folgenden Kapitel sind der Fragestellung gewidmet, ob die allgemeinen Regeln zu Leistungsstörungen, Haftung und Gewährleistung auch auf Smart Contracts angewendet werden können oder ob allenfalls neue Regelungen erforderlich sind. Im Abschlusskapitel wird der Frage nachgegangen, wie das Halten von Vermögenswerten durch einen Smart Contract vertragsrechtlich eingeordnet werden kann. 212

Nachfolgend wird mit Ausnahme von vier kurzen Anwendungsfällen bewusst auf Beispiele verzichtet. Dies aus den folgenden Gründen: Bei medienwirksam vorgestellten Anwendungsfällen der Blockchain-Technologie in Verbindung mit Smart Contracts handelt es sich oft um Projekte von Unternehmen, die noch nicht die Phase des *Proof of Concept* erreicht haben und daher ungewiss ist, ob sie jemals umgesetzt werden. In anderen Fällen sind Anwendungen von Start-ups betroffen, deren weiterer Fortgang offen ist. Auch werden in einer hohen Kadenz neue Anwendungen hervorgebracht und wieder verworfen, so dass es kaum möglich ist, den aktuellsten Stand abzubilden 213

A. Einführung Smart Contracts

214 Der folgende einführende Teil befasst sich vorerst mit einer historischen und begrifflichen Einordnung sowie der Herleitung einer Definition. Anschliessend wird in einem zweiten Kapitel die Funktionsweise eines Smart Contract erläutert.

I. Historie und Begriff

215 Eine eindeutige und allgemeingebräuchliche Definition des Begriffes *Smart Contract* existiert zum heutigen Zeitpunkt nicht, da diese Anwendung von unterschiedlichen Akteuren zu unterschiedlichen Zwecken eingesetzt wird. Es herrscht sowohl im Internet als auch in der Fachliteratur eine nuancenreiche Definitionsvielfalt. Um den Begriff und das Konzept des Smart Contract zu erfassen, wird der Begriff in den folgenden Kapiteln zuerst in einen historischen Kontext eingeordnet und danach sukzessive mit verschiedenen Definitionsansätzen eingegrenzt. Abschliessend wird daraus eine eigene Definition des Begriffes *Smart Contract* hergeleitet.

1. Historie

216 Erstmals verwendet hat den Begriff *Smart Contracts* NICK SZABO[354] in seinem 1994 erschienenen Aufsatz „Smart Contracts“ (zur Definition von SZABO vgl. nachfolgend N 224). Als Veranschaulichungsbeispiel für den Mechanismus eines Smart Contract wählt SZABO in weiteren Aufsätzen zu Smart Contracts einen Verkaufsautomaten: Jede beliebige Person kann mit dem Verkäufer (also dem Automaten) in Kontakt treten. Wenn die Grundvoraussetzungen erfüllt sind (ein bestimmter Geldbetrag, bezahlt in Münzen), wird der Vertrag automatisch ausgeführt (der Automat gibt das gewünschte Produkt frei). Gesichert wird der Automat durch einen speziellen Schliessmechanismus und andere Sicherungsmassnahmen. Der Automat ist genügend sicher, damit das

[354] Ein Computer- und Rechtswissenschaftler aus den USA.

Geschäft sowohl für den Käufer als auch den Verkäufer attraktiv ist und in verschiedenen Bereichen breit eingesetzt werden kann.[355] Dieses Beispiel soll zeigen, wie durch einen einfachen Sicherungsmechanismus ein konkreter Vertrag entsteht, d.h. wie eine „neue“ Technik eine automatisierte Art von Vertragsabschluss und -abwicklung ermöglicht.[356] SZABO ging bereits in den 90er Jahren davon aus, dass ein ausgereiftes (technisches) Sicherungssystem dazu führen würde, Verträge automatisch abzuwickeln und dass dadurch Kosten bei der Durchsetzung von Verträgen eingespart werden können.[357] Die Ausführungen von SZABO werden noch heute von vielen Autoren als die Grundlagen von Smart Contracts betrachtet und oft zitiert.[358]

2. Neuere Entwicklungen

217 Heute wird der Begriff *Smart Contract* oft als Sammelbegriff für eine Reihe von Anwendungen verwendet. Er bezieht sich jedoch auch auf spezifische Anwendungen und Produkte (z.B. nennt die Ethereum-Stiftung eine ihrer Anwendungen Smart Contracts[359]). Ihnen allen ist gemein, dass sie auf der Blockchain-Technologie aufbauen.

218 Grob kann zwischen einer technologisch eingefärbten sowie einer juristischen Sichtweise der Begrifflichkeit unterschieden werden. Dabei wird der Fokus jeweils auf die Eigenschaften und Möglichkeiten gelegt; die Fachdisziplin gibt dabei den Schwerpunkt der jeweiligen Betrachtung vor. Eine neuere Tendenz geht dahin, zwischen *Smart Contract Code* und Smart Legal Contract zu

---

355 Vgl. SZABO, Formalizing and Securing Relationship, Titel Contracts Embedded in the World, 1. Abschnitt.

356 SZABO, Smart Contract, 6. Abschnitt.

357 SZABO, Smart Contract, 3. Abschnitt; SZABO, Idea of smart contract, 2. Abschnitt ff.

358 So bspw. MEYER/SCHUPPLI, Smart Contracts, 207 f.; MOUGAYAR, Business Blockchain, 41; SWAN, Blockchain, 16 f.; SWANSON, Great Chain, 15 f.; WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, RN 2 FN 1.

359 Zur Programmierung siehe https://solidity.readthedocs.io/en/develp/introduction-to-smart-contracts.html.

unterscheiden.[360] Diese Zweiteilung dient der Differenzierung des durchzusetzenden Aspektes: Der Smart Contract Code setzt die Programmierung um (operationelle Ausführung), während der Smart Legal Contract die mehr oder weniger komplexen rechtlichen Verpflichtungen durchsetzt.[361]

219 Mancherorts wird ausserdem ausgeführt, dass im Zusammenhang mit Smart Contract Code das Wort *Contract* die Ausführung von rechtlichen Verpflichtungen auf einer Blockchain impliziere[362] und ein Smart Legal Contract die Art und Weise bezeichne, wie ein rechtlicher Vertrag in Software abgebildet werden kann.[363]

220 Diese skizzierte Zweiteilung in Smart Contract Code und Smart Legal Contract bringt also keine eindeutige Klärung der Begrifflichkeit, sondern schafft vielmehr eine weitere Kategorie von Begriffen, die wiederum unterschiedlich ausgelegt und verstanden werden können. So ist bspw. nicht klar, ob der Begriff *Smart Legal Contract* auf eine Programmiersprache oder aber die Art und Weise, wie ein Smart Contract rechtliche Verpflichtungen durchsetzt, hinweist. Diese weitere Unterteilung ist im Hinblick auf eine einheitliche Definition oder Klärung des Begriffes nicht zielführend.

221 Doch damit nicht genug: Aktuell wird nicht mehr nur von Smart Contract Code und Smart Legal Contracts gesprochen. Bereits ist eine neue Schöpfung mit dem Präfix *smart* entstanden: Neuerdings wird im Zusammenhang mit Smart Contracts von *Smart Legal Context* gesprochen.[364] Auf diese Verästelung wird

---

360 BACON/BAZINAS, Smart Contracts, N 3; JACCARD, Smart Contract, 21 ff.; MEYER/SCHUPPLI, Smart Contracts, 207.

361 BACON/BAZINAS, Smart Contracts, N 4; vgl. MEYER/SCHUPPLI, Smart Contracts, 207 f.

362 CLACK/BAKSHI/BRAINE, Smart Contract Templates, 2; MEYER/SCHUPPLI, Smart Contracts, 207.

363 CLACK/BAKSHI/BRAINE, Smart Contract Templates, 2; MEYER/SCHUPPLI, Smart Contracts, 208; KRONBALD/HAAPIO verstehen generell unter Smart Contract jeweils einen rechtlich durchsetzbaren Vertag im Sinne eines Smart Legal Contracts, vgl. KRONBLAD/HAAPIO, Smart Contracts, N 1 FN 4.

364 Unter Smart Legal Context verstehen EBENHOCH/GANTER (aus Sicht des Softwareentwicklers) den klassischen Vertragstext als denjenigen

hier nicht näher eingegangen;[365] dieses Beispiel soll jedoch zeigen, wie dynamisch sich die Begrifflichkeiten (im Gleichschritt mit der Technologie) weiterentwickeln.

3. Smart Contract von Ethereum

222 Eine Vorreiterrolle kommt im Zusammenhang mit Smart Contracts der in der Schweiz ansässigen Ethereum-Stiftung zu. Ethereum nennt bestimmte Codes, die auf der Ethereum-Blockchain initiiert werden können, Smart Contracts und umschreibt deren Funktion folgendermassen: Als *account holding objects* auf der Blockchain können sie mit anderen Smart Contracts interagieren, Entscheidungen treffen, Daten speichern und *Ether* (die Kryptowährung von Ethereum, vgl. Anhang, N 28 f.) versenden. Die jeweiligen Eigenschaften können durch ihre Schöpfer bestimmt werden – die Ausführung und allfällige weitere Serviceleistungen werden jedoch durch die Ethereum-Blockchain vorgenommen. Smart Contracts existieren solange, wie das Netzwerk (die Blockchain) selbst existiert und sie werden nur dann aufgelöst, wenn sie zur Selbstzerstörung programmiert wurden.[366]

223 Die Beschreibung des Smart Contract der Ethereum-Blockchain wird an dieser Stelle deshalb ausdrücklich erwähnt, weil diese Blockchain eine der bedeutendsten ist und Ethereum im Bereich der Smart Contracts eine wichtige Rolle spielt. Der Begriff *Smart Contract* wurde von der Ethereum-Plattform geprägt und so einer breiten Öffentlichkeit zugänglich gemacht, obschon SZABO als Urheber dieses Begriffes gilt (vgl. RN 216). Zwischenzeitlich findet der Terminus allgemeine Verwendung.

Kontext, in dem das Programm entwickelt wird: EBENHOCH, Blockchain Compliance, N 38 f.; EBENHOCH/GANTER, Smart Context für Smart Contracts, N 18.

365 Ausführlich dazu EBENHOCH/GANTER, Smart Context für Smart Contracts, N 18 ff.

366 Vgl. www.ethereum.org/greeter.

4. Definitionsansätze

224 Wie schon angedeutet, wird der Begriff *Smart Contract* je nach Kontext und Quelle unterschiedlich ausgelegt und verstanden. Obwohl sein Wortlaut das Vorliegen eines smarten, also intelligenten Vertrages suggeriert, liegt ein solcher bei genauerer Betrachtung nicht vor. Im Zusammenhang mit Technologie wird der Begriff *smart* geradezu inflationär etlichen Begriffen vorangestellt – wobei die eigentliche Wortbestimmung verloren geht.[367] Beim Begriff *Smart Contract* liegt gleich eine doppelte Ungenauigkeit vor: Einerseits herrscht Einigkeit darüber, dass dem Wort *smart* in diesem Kontext nicht die Bedeutung von *intelligent* zu attestieren ist; andererseits scheiden sich die Geister an der Frage, ob ein Smart Contract tatsächlich als Vertrag einzustufen ist.

225 Wie eingangs erwähnt, wird im Zusammenhang mit der Blockchain-Technologie Algorithmen mehr vertraut (vgl. N 38 ff.) als menschlicher Interaktion,[368] was sich teilweise auch in den Definitionen des Begriffes *Smart Contract* widerspiegelt. Aus der schier unüberschaubaren Fülle an Definitionen hat sich bis dato noch keine durchgesetzt. Es sind jedoch Definitionsansätze erkennbar, welche nachfolgend gruppiert und vorgestellt werden.[369]

a) Technische Ansätze

226 SZABO (Computer- und Rechtswissenschaftler) gilt als ideeller Vater des Smart Contract (vgl. N 216 f.). Er hat ihn 1994 – lange vor dem Durchbruch der Blockchain-Technologie – folgendermassen definiert: Ein Smart Contract ist

---

367 Man denke bspw. an Smart Phone, Smart Home, Smart Watch, Smart Car, Smart Shoes etc.

368 Vgl. MIK, Smart Contract, 2.

369 Viele inhaltliche Diskussionen rund um die Blockchain-Technologie und Smart Contracts finden in Internetforen statt. Es gibt unzählige (qualitativ hochwertige) Blogs, die sich dem Thema widmen. Foren und Blogbeiträge können in dieser Arbeit nicht ausführlich zitiert werden. Nichtsdestotrotz soll an dieser Stelle darauf hingewiesen werden, dass die aktuellsten und teilweise auch aufschlussreichsten Diskussionen jeweils in den einschlägigen Foren zu finden sind.

ein computerisiertes Transaktionsprotokoll, das Vertragsbestandteile ausführt. Hauptzweck ist die Durchsetzung von allgemeinen Vertragsbedingungen (Zahlungskonditionen, Retentionsrecht, Vertraulichkeit und sogar Durchsetzbarkeit), die Minimierung von vorsätzlichen und fahrlässigen Vertragsbrüchen und der Notwendigkeit von vertrauenswürdigen Intermediären. Ökonomisch betrachtet führe dies zu weniger Verlusten durch Betrug, Schlichtungs- und Durchsetzungskosten sowie anderen Transaktionskosten.[370]

227 SWANSON (interdisziplinärer Wissenschaftler) beschreibt einen Smart Contract als ein Computerprotokoll, das einen Vertrag selbst ausführen, selbst durchsetzen und selbst überprüfen kann.[371] Im Unterschied zu klassischen Verträgen sind Smart Contracts laut SWANSON nicht auf eine physische Durchsetzungskraft angewiesen.[372]

228 Eine kurze Definition findet sich bei SWAN (Philosophin und Naturwissenschaftstheoretikerin). Nach dieser Autorin sind Smart Contracts blockchainbasierte Transaktionen, die über einfache Kaufs-/Verkaufs-Transaktionen hinausgehen.[373] Gemäss SWAN sind die Vorteile von Smart Contracts die Autonomie, Eigenständigkeit und Dezentralität.[374] Unter Autonomie versteht sie die Annahme, dass der Smart Contract – sobald initiiert und operativ – keine Interaktion zwischen dem Agenten und dem Vertrag mehr erfordere. Eigenständig können Smart Contracts Ressourcen einteilen, indem sie bspw. die mittels Kapitalbeschaffung erhaltenen Mittel (bspw. durch die Ausgabe von Anteilen) in die notwendigen Ressourcen (bspw. Rechenleistung oder Speicherplatz) investieren. Die Dezentralität bezieht sich auf die Blockchain, auf der ein Smart Contract gespeichert ist.[375] SWAN schlägt vor,

370 SZABO, Smart Contract, Glossary.
371 SWANSON, Great Chain, 16.
372 SWANSON, Great Chain, 16.
373 SWAN, Blockchain, 16.
374 SWAN, Blockchain, 16.
375 SWAN, Blockchain, 16.

für diese Art von codebasierten Regelungen neue Rechtsgefässe zu schaffen, um der digitalen Realität Rechnung tragen zu können.[376]

229 Mit einem Negativkatalog sowie einer Aufzählung von Eigenschaften umschreibt MOUGAYAR (Unternehmer) Smart Contracts. Demgemäss ist ein Smart Contract kein Vertrag, kein Ricardian Contract[377], kein Gesetz, enthält keine künstliche Intelligenz, keine Blockchain-Applikation, nicht nur für Softwareentwickler gedacht und einfach zu programmieren sowie sicher und sehr breit in den Anwendungsmöglichkeiten.[378] Die Quintessenz dieser Umschreibung ist, dass ein Smart Contract eine individuell anpassbare Software ist, die auf Blockchain-Netzwerken betrieben wird.

230 Die Definition von BUTERIN (Softwareentwickler) besitzt eine gewisse Aussagekraft, da er als einer der Hauptentwickler der Ethereum-Blockchain in der Blockchain-Community eine Schlüsselrolle spielt. Gemäss BUTERIN ist ein Smart Contract die einfachste Form von dezentraler Automatisierung. Ein Smart Contract sei ein Mechanismus, wobei digitale Vermögenswerte und zwei oder mehr Parteien involviert sind. Die Parteien bringen ihre Vermögenswerte ein und diese werden automatisch gemäss den von den Parteien vereinbarten Regeln verteilt, wobei auf Daten zurückgegriffen wird, die zum Zeitpunkt der Initiierung des Smart Contract noch nicht bekannt sind.[379]

231 Schliesslich ist noch die Definition von CLACK/BAKSHI/BRAINE (Computerwissenschaftler) zu erwähnen. Diese schlagen gewissermassen als Kompromiss zwischen einer rein technischen und einer rein juristischen Sichtweise (zur juristischen Sichtweise siehe später) folgende Definition vor:

---

376 SWAN, Blockchain, 17.

377 Ein Ricardian Contract ist eine Form des digitalisierten Vertrags und geht auf eine Idee von IAN GRIGG aus den 90er Jahren zurück. Ein Vertrag im Rechtssinne soll ohne Verlust der Gültigkeit und des tatsächlich Vereinbarten digital abgebildet werden („The Ricardian Contract“ von GRIGG abrufbar unter: http://iang.org/papers/ricardian_contract.html; bildliche Darstellung auch bei MEYER/SCHUPPLI, Smart Contracts, 207).

378 MOUGAYAR, Business Blockchain, 42 f.

379 https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

Ein Smart Contract ist eine automatisierbare und durchsetzungsfähige Vereinbarung. Automatisierbar ist ein Smart Contract durch den Computer, auch wenn gewisse Teile davon menschlichen Input und Kontrolle benötigen können. Durchsetzbar ist er im rechtlichen Sinne oder mit Hilfe der manipulationssicheren Durchführung des Computercodes.[380]

b) Juristische Ansätze

232 Auch Juristen haben sich schon mit der Definition und Verortung von Smart Contracts beschäftigt. So schlagen KAULARTZ/HECKMANN folgende Definition vor: Ein Smart Contract ist eine Software, „die rechtlich relevante Handlungen (insbesondere einen tatsächlichen Leistungsaustausch) in Abhängigkeit von digital prüfbaren Ereignissen steuert, kontrolliert und/oder dokumentiert, mit dessen Hilfe aber unter Umständen auch [...] dingliche und/oder schuldrechtliche Verträge geschlossen werden können.“[381]

233 MEYER/SCHUPPLI definieren Smart Contracts als „digitale Programme, die sich, gestützt auf die Blockchain-Architektur, beim Eintritt gewisser Bedingungen selbst ausführen und aufgrund der dezentralen und kryptografischen Ausgestaltung der Blockchain selbstdurchsetzend und manipulationssicher sind“.[382]

234 Die SWISS LEGAL TECH ASSOCIATION (SLTA) hat ebenfalls eine Definition von Smart Contracts vorgeschlagen. Gemäss Whitepaper vom 27. April 2018 ist ein Smart Contract ein sich selbstausführender Software-Code, der dazu entwickelt wird, vordefinierte Bedingungen, Funktionen oder Aktionen auszuführen. Wesentliche Eigenschaften sind die selbständige Durchsetzbarkeit sowie die Unveränderlichkeit.[383]

---

380 CLACK/BAKSHI/BRAINE, Smart Contract Templates, 2.

381 KAULARTZ/HECKMANN, Smart Contract, 618.

382 MEYER/SCHUPPLI, Smart Contracts, 208.

383 SLTA, Data, Blockchain and Smart Contracts, 9.

5. Eigene Definition von Smart Contracts

235 Wie bereits vorhergehend ausgeführt werden Smart Contracts je nach Quelle und Kontext unterschiedlich definiert. Den meisten Definitionen gemein ist, dass sie den Begriff *Software* oder *Computerprogramm* (vgl. Anhang, N 1 ff.) enthalten oder Smart Contracts pleonastisch durch Nennung der Begriffselemente charakterisieren. Des Weiteren enthalten die meisten der hier exemplarisch aufgelisteten Definitionen Adjektive (bspw. automatisiert, selbstausführend, selbstdurchsetzend etc.), die generell den Terminus *Software* umschreiben und weisen auf die technologischen Möglichkeiten hin (bspw. Vertragsschluss, Vertragsdurchsetzung, Senkung von Transaktions- oder Prozesskosten etc.).

236 Es ist daher zielführend, in einem ersten Schritt pleonastische Elemente zu entfernen und so eine möglichst griffige Definition von Smart Contracts herzuleiten. Um den rasch voranschreitenden Entwicklungen gerecht zu werden, sind Beschreibungen der Eigenschaften und der technologischen Möglichkeiten von Smart Contracts aus der Definition zu verbannen. So kann eine möglichst universelle Gültigkeit hergestellt werden.

237 Da Einigkeit darüber herrscht, dass ein Smart Contract im Kern ein Computerprogramm darstellt, muss hierauf nicht näher eingegangen werden.[384] Software ist ein Überbegriff und inkludiert Computerprogramme (vgl. Anhang, N 1). Die Einordnung, ob ein Smart Contract eine Software oder ein Computerprogramm darstellt, kann aus juristischer Sicht nicht beurteilt werden und sei den Computerwissenschaftlern überlassen.

238 Vereinfachend und die vorgängig aufgeführten Definitionen zusammenfassend kann festgehalten werden, dass unter Smart Contracts die diversen Programmiermöglichkeiten verstanden werden, die mit einer einfachen

[384] Vgl. auch KAULARTZ/HECKMANN, Smart Contract, 618 f.; MEYER/SCHUPPLI, Smart Contracts, 204; MIK, Smart Contract, 3 ff.; WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, 2 f.

Transaktion auf einer Blockchain verknüpfbar sind (bspw. die Verbindung einer Transaktion mit einer Bedingung).[385]

239 Aufgrund der rasanten Entwicklung und der heute noch nicht vollständig bekannten oder realisierten Möglichkeiten bietet es sich an, eine möglichst stringente Definition des Begriffes *Smart Contract* zu verwenden, die weitgehend auf deskriptive Elemente verzichtet (den Merkmalen des Smart Contract ist der folgende Abschnitt gewidmet). Dadurch soll die Definition möglichst lange ihre Gültigkeit und Plausibilität behalten. Gemäss dem vorhergehend Ausgeführten lässt sich in der Quintessenz die Definition auf Folgendes reduzieren: *Ein Smart Contract ist ein auf der Blockchain-Technologie basierendes, individualisierbares Computerprogramm.*

6. Merkmale

240 In den in dieser Arbeit exemplarisch aufgeführten Definitionen (vgl. N 224 ff.), aber auch in vielen anderen Definitionsansätzen kristallisieren sich als vorherrschende Eigenschaften von Smart Contracts *Autonomie/ Eigenständigkeit*, *Unveränderbarkeit* und *fehlende Interpretationsmöglichkeit* heraus. Auf diese Merkmale wird nachfolgend im Detail eingegangen.

a) Autonomie/Eigenständigkeit

241 Die vorprogrammierten Regeln werden durch das Programm selbständig, d.h. ohne jegliche menschliche Interaktion, angewandt. Darunter kann auch die selbständige Durchsetzung von Vertragsbestandteilen fallen. Der Code kann – einmal auf der Blockchain abgespeichert – im Nachhinein nicht mehr abgeändert werden und entwickelt so eine gewisse Eigendynamik. Ein Smart Contract kann einzelne vertragliche Elemente autonom ausführen und macht somit die Intervention eines Intermediärs (z.B. Anwalt oder Gericht) zur

[385] Gemäss BERENTSEN/SCHÄR werden die durch die Smart Contracts „geskripteten Abfolgen“ durch die Blockchain „besichert“: BERENTSEN/ SCHÄR, Kryptoassets, 289.

Durchsetzung teilweise überflüssig.[386] Ein Smart Contract kann zwar selbständig vorprogrammierte Befehle ausführen. Allerdings ist festzuhalten, dass es sich nicht um eine eigenständig handelnde Entität mit eigener Rechtspersönlichkeit handelt.[387] Sämtliche Befehle, die durch den Smart Contract ausgeführt werden, stammen von einer oder mehreren Parteien, die die entsprechenden Befehle vorgängig programmiert und/oder initiiert haben. Dies gilt auch für komplexe Smart Contracts, wie beispielsweise DAOs (vgl. Anhang N 37 f.)[388]

b) Unveränderbarkeit

242 Unveränderbarkeit gilt als zentrales Merkmal von Smart Contracts. Es muss hier präzisiert werden, dass Smart Contracts zwar auf der Blockchain-Technologie aufbauen, welche als unveränderlich gilt. Die Unveränderbarkeit bezieht sich im Zusammenhang mit der Blockchain-Technologie aber in der Regel auf die Transaktionen, die definitiv in das Transaktionsregister aufgenommen wurden. Smart Contracts können als Zustand auf die Blockchain gespeichert werden; bei der Ethereum-Blockchain bspw. ist der Code als *Zustand* im entsprechenden Konto gespeichert (vgl. N 80) und wird bei Eintritt der erforderlichen Bedingung ausgeführt. Durch die Speicherung im entsprechenden Konto, das wiederum auf sämtlichen beteiligten Nodes abgespeichert ist, erwirbt der Smart Contract die Eigenschaft der Blockchain, also die Unabänderbarkeit der in der Blockchain gespeicherten Daten.[389] Es besteht jedoch die Möglichkeit, dass ein Smart Contract nur das Resultat in die Blockchain speichert, er selbst jedoch nicht auf der Blockchain, sondern in einem virtuellen Container (z.B. *Cloud*) ausserhalb der Blockchain

---

386 SWAN, Blockchain, 16; SWANSON, Great Chain, 16; WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 4.

387 Vgl. KAULARTZ/HECKMANN, Smart Contract, 618 f.; a.A. ROON, Schlichtung und Blockchain, 360.

388 Vgl. GYR, DAO, N 17 ff.

389 Vgl. MIELKE/WOLFF, Smart Contracts als interdisziplinäres Problem, N 10 ff.; PLOOM, Blockchains, 129.

abgespeichert ist (vgl. nachfolgend N 250).[390] In diesen Fällen besitzt der Smart Contract selbst nicht zwingend die Eigenschaft der Unveränderbarkeit.

c) Keine Interpretationsmöglichkeit

243 Die im Smart Contract hinterlegten Regeln sind nicht auslegbar. Sie sind im Sinne der Naturgesetze deterministisch.[391] Es wird durch das Computerprogramm ausgeführt, was als Regel hinterlegt wurde. Verträge im Rechtssinne können im Gegensatz dazu interpretiert und gemäss dem Willen der Vertragsparteien ausgelegt werden (vgl. nachfolgend N 326 ff.).

7. Exkurs: Elektronischer Agent

244 Teilweise findet sich im Zusammenhang mit Smart Contracts die Fragestellung (oder auch die Feststellung), ob ein Smart Contract eine eigenständig handelnde Entität darstellt und ihm aus diesem Grund allenfalls sogar eine eigene Rechtspersönlichkeit zukommen sollte.[392] Diese Fragestellung erinnert an die Diskussion über die *elektronischen Agenten* (auch intelligente Agenten, Softwareagenten, Computererklärungen, oder Agentenerklärungen genannt), als mit dem Aufkommen des E-Commerce[393] die gleiche Frage aufgeworfen wurde.[394]

---

390 Vgl. PLOOM, Blockchains, 144.

391 GANTER, Is Law Code?, N 28.

392 Vgl. KOLVART/POOLA/RULL, Smart Contracts, 134; ROON, Schlichtung und Blockchain, 360 f.

393 E-Commerce steht für Elektronischer Geschäftsverkehr; Begriff und Entwicklung von E-Commerce siehe BRÄUTIGAM, E-Commerce 2.0, N 1 ff.

394 Vgl. BALSCHEIT, Konsumvertragsrecht, 168 ff.; GISLER, vertragliche Aspekte elektronischer Märkte, 97 ff.; KIANICKA, Agentenerklärung, 53 ff.; WEBER/JÖHRI, Vertragsschluss im Internet, 48 ff.

a) Begriff

245 Mit dem Aufkommen des Internet und des E-Commerce verbreitete sich der Begriff des elektronischen Agenten.[395] Darunter ist ein Programm zu verstehen, das selbständig Aufgaben ausführt, ohne auf den kontinuierlichen Input oder die Kontrolle eines Menschen angewiesen zu sein.[396] Analog zu Smart Contracts wurde auch bei elektronischen Agenten bereits das Adjektiv *smart* vorangestellt. Allerdings wies *smart* schon damals auf die Programmierung hin; der Agent ist so intelligent wie die Programmierung es vorgesehen hat.[397] Ein Agent ist also nichts Anderes als Software.

246 Im Zusammenhang mit elektronischen Agenten wurde ebenfalls diskutiert, ob ihnen aufgrund ihrer suggerierten künstlichen Intelligenz eine eigenständige Rechtspersönlichkeit zukommt oder zukommen soll. Dies wurde und wird grossmehrheitlich verneint, da auch die Handlungen eines elektronischen Agenten jeweils einer Person zugerechnet werden können.[398]

b) Smart Contracts und elektronische Agenten

247 Gemäss den Ausführungen im vorangehenden Kapitel (vgl. N 238 f.) sind Smart Contracts ebenfalls als Agenten zu qualifizieren, da sie ebenfalls Software darstellen. Der Terminus Agent sollte jedoch vermieden werden, da er eine Eigenständigkeit suggeriert, die nicht vorhanden ist.

248 Aus heutiger Perspektive unterscheiden sich die vormals vieldiskutierten elektronischen Agenten und Smart Contracts vor allem in der ihnen zugrundeliegenden Technologie. Die aufgeworfenen Fragen, insbesondere in Bezug auf das Vertragsrecht, wie bspw. zur elektronischen Willenserklärung und Zurechenbarkeit von elektronischen Willenserklärungen (vgl. nachfolgend N 287 ff.) bleiben indes praktisch identisch.

---

395 KIANICKA, Agentenerklärung, 53.

396 KIANICKA, Agentenerklärung, 53.

397 Vgl. KIANICKA, Agentenerklärung, 54.

398 KIANICKA, Agentenerklärung, 63 ff.

II. Funktionsweise von Smart Contracts

Im nachfolgenden Kapitel wird – stark vereinfachend – die Funktionsweise von Smart Contracts erläutert. Dabei wird dargelegt, wie ein Smart Contract auf Ereignisse ausserhalb der Blockchain zugreifen kann und wie es möglich ist, Vermögenswerte an einen Smart Contract zu übertragen. Abgeschlossen wird das Kapitel durch konkrete Anwendungsbeispiele von Smart Contracts. 249

1. Allgemeines

Ein Smart Contract ist, wie vorgängig ausgeführt, ein Computerprogramm, das auf einer Blockchain-Plattform ausgeführt werden kann (vgl. N 238 ff.). 250

Ein Smart Contract kann direkt auf einer (öffentlichen) Blockchain als Zustand abgespeichert werden. Bei der Ethereum-Blockchain bspw. wird ein Smart Contract in einem Konto, also direkt auf der Blockchain (d.h., gleichzeitig auf allen Knotenpunkten), abgespeichert.[399] Dadurch, dass er direkt[400] auf der Blockchain abgespeichert ist, kann der Smart Contract nachträglich nicht mehr abgeändert werden (vgl. N 242). Das Ergebnis, also die durch den Smart Contract durchgeführte Transaktion, kann jederzeit durch die Knotenpunkte überprüft und validiert werden, was auf ein sicheres Ergebnis schliessen lässt.[401] Die direkte Verankerung des Smart Contract auf der Blockchain ist hinsichtlich der Manipulationssicherheit sowie der Validierung der Transaktion durch das Netzwerk sicher ein Vorteil; im Fall von fehlerhaften 251

399 Vgl. MIELKE/WOLFF, Smart Contracts als interdisziplinäres Problem, 3 f.; PLOOM, Blockchains, 129.

400 Direkt meint in diesem Zusammenhang, dass der Smart Contract als Applikation auf der Blockchain-Plattform verankert ist. Durch diese Verankerung wird der Smart Contract auf dem gesamten Blockchain-Netzwerk hinterlegt, d.h. er ist auf allen Knotenpunkten verteilt und alle Knotenpunkte führen den Smart Contract einzeln aus (vgl. PLOOM, Blockchains, 128.).

401 Vgl. PLOOM, Blockchains, 129; MIELKE/WOLFF, Smart Contracts als interdisziplinäres Problem, 4; FURRER, Smart Contracts, 104.

Smart Contracts, die nicht mehr abgeändert werden können, stellt sie jedoch einen Nachteil dar (vgl. nachfolgend N 341 ff.).[402]

252 Neben der Speicherung des Smart Contract als Zustand auf der Blockchain besteht die Möglichkeit, ihn ausserhalb der Blockchain z.B. in einem virtuellen Container (Cloud) zu speichern und nur den Hash[403] des Smart Contract und/oder nur das Ergebnis des Smart Contract in der Blockchain abzuspeichern. Dieses Modell wurde insbesondere für private Anwendungen und Unternehmen entwickelt, da ein solches Modell ermöglicht, dass der Smart Contract auch auf Systeme von Unternehmen zugreifen kann (was bei Smart Contracts von Ethereum bspw. nicht möglich ist) und nicht viel Speicherplatz auf der Blockchain benötigt.[404] Ist der Smart Contract ausserhalb der Blockchain gespeichert, lässt dies allenfalls auch ein Eingreifen durch die Parteien zu (bspw. bei einer fehlerhaften Programmierung oder geänderten Umständen).

253 Als Grundsatz für den Mechanismus kann festgehalten werden, dass bei einem Smart Contract die von den Parteien eingebrachten Vermögenswerte automatisch gemäss den von den Parteien vereinbarten Regeln verteilt werden; dabei wird auf Daten zurückgegriffen, die zum Zeitpunkt der Initiierung des Smart Contract noch nicht bekannt sind (vgl. hiervor N 230).

---

402 Da Smart Contracts auf sämtlichen Knotenpunkten abgespeichert sind, jeder Knoten den Smart Contract ausführt und das Ergebnis, also die Transaktion, immer wieder validiert wird, führt dies zu einem enormen Speicher- und Rechenaufwand im Netzwerk (vgl. PLOOM, Blockchains, 129, 144.).

403 Für Erklärungen zum Begriff *Hash* vgl. Anhang, N 5 f.

404 So z.B. Chaincode von Hyperledger, Übersicht der Chaincodes auf den verschiedenen Blockchain-Infrastrukturen von Hyperledger im WHITEPAPER HYPERLEDGER, Hyperledger Architecture, Volume II, 8; Vgl. PLOOM, Blockchains, 144.

2. Bezug zu Ereignissen ausserhalb der Blockchain

254 Ein Smart Contract referenziert auf Daten, die zum Zeitpunkt der Initiierung noch nicht vorliegen (vgl. N 253). Diese Dateninformation kann sich entweder auf der Blockchain befinden (sog. *on chain*) oder von einem Ereignis, resp. einer Information, ausserhalb der Blockchain (sog. *off chain*), entweder in der virtuellen oder realen Welt, abhängen. Der Bezug zu einer Information ausserhalb der Blockchain kann durch ein sog. *Orakel* hergestellt werden. Das Orakel ist eine Drittpartei, eine von den Parteien auserkorene, vertrauenswürdige Instanz, welche bspw. den Eintritt eines bestimmten Ereignisses als Transaktion in der Blockchain speichert, worauf wiederum der Smart Contract referenziert.[405] Oder das Orakel hält einen privaten Schlüssel, der für die Auslösung der Transaktion als Bedingung vorausgesetzt wird.[406] Es ist hierbei zu beachten, dass diese Schnittstellen nicht die gleichen (Sicherheits-) Merkmale wie die Daten auf Blockchain selbst aufweisen und dass die Informationen, die von aussen in die Blockchain getragen werden, nicht durch das Netzwerk (Miner) validiert werden.[407]

255 Die Verbindung von einem Smart Contract zu einem Gegenstand in der realen Welt kann auch mittels Schnittstellen zum *Internet of Things (IoT)* hergestellt werden.[408] IoT ist eine internetbasierte Informationsarchitektur, die realen Gütern mit Hilfe von eingebauten Kleinstcomputern die Kommunikation mit der virtuellen Welt ermöglicht.[409]

---

405 Vgl. SWAN, Blockchain, 17; SWANSON, Great Chain, 61; WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 33 f.; BERENTSEN/SCHÄR, Kryptoassets, 294.

406 Vgl. BERENTSEN/SCHÄR, Kryptoassets, 294.

407 FURRER, Smart Contracts, 104; MIK, Smart Contract, 9; vgl. BERETSEN/SCHÄR, Kryptoassets, 294 f.

408 Zur möglichen Verbindung zwischen Blockchain und IoT vgl. CHRISTIDIS/DEVETSIKIOTIS, Smart Contracts for IoT, 2298 ff.

409 EGGEN, Home Smart Home, 1131 f.; WEBER/WEBER, IoT, 1.

3. Übertragung von Vermögenswerten an den Smart Contract

256 Ein Smart Contract kann Vermögenswerte halten.[410] So ist es beispielsweise möglich, an die Adresse eines Smart Contract Kryptowährung oder andere Token (Anhang, N 30 ff.) zu senden.[411] Der Smart Contract kann diese Token halten und nach Eintritt der vordefinierten Bedingungen an die vorbestimmte Partei (resp. deren Adresse) übertragen.

4. Beispiele

257 Nachfolgend werden exemplarisch Anwendungsgebiete vorgestellt, in denen Smart Contracts zum Einsatz kommen könnten. Smart Contracts kommen bereits heute weit verbreitet zum Einsatz. Allerdings agieren diese im Verborgenen (innerhalb von Anwendungen) und sind nicht per se als „Verträge“ erkennbar. Auf diese Frage wird jedoch später eingegangen (vgl. N 266 ff.). Die nachfolgenden Beispiele sind bewusst kurz und oberflächlich gehalten und dienen lediglich der Veranschaulichung. Sie weisen nicht auf allfällige juristische Fallstricke hin.

a) Wohnungs- oder Automiete: Smarte Schlösser

258 Smart Contracts können via IoT mit einem Gegenstand in der realen Welt verbunden sein. So können bspw. Mietverträge über Wohnungen oder Autos mit einem Smart Contract abgewickelt werden. Der Mieter hinterlegt beim Smart Contract die Miete sowie eine Kaution. Im Anschluss erhält er einen Schlüssel, mit dem er die Wohnung oder das Fahrzeug öffnen kann. Der Mietgegenstand, der via IoT mit dem Smart Contract verbunden ist, „weiss“ sodann, dass der Mieter die Zahlungen hinterlegt hat und gibt das Schloss, wenn es mit dem entsprechenden Schlüssel geöffnet wird, frei. Bei Rückgabe

410 Vgl. hierzu Kapitel I., N 517 ff.

411 Zu Token und deren Klassifizierung vgl. Anhang, N 30 ff.

der Wohnung oder des Autos wird die Kaution dann automatisch zurücküberwiesen.[412]

b) Versicherung

259 Ein Smart Contract kann im Versicherungsbereich eingesetzt werden. Es kursieren viele Beispiele, die praktisch jedoch noch nicht umgesetzt worden sind.[413]

260 Bei Schadensversicherungen bspw. würde der Smart Contract die Versicherungsbedingungen enthalten. Bei Eintritt des versicherten Schadenereignisses würde automatisch die versprochene Versicherungsleistung ausbezahlt.

261 Bei der Haftpflichtversicherung eines Autolenkers könnte der Smart Contract direkt mit dem Fahrzeug des Lenkers verbunden sein. Via IoT würde dem Smart Contract mitgeteilt, ob der Lenker verkehrswidrige Verhaltensweisen (z.B. wiederholtes zu schnelles Fahren) aufzeigt und so die Prämien entsprechend automatisch angepasst.

c) Musik

262 Ein bereits seit längerem bekanntes Problem in Bezug auf Streamingdienste könnte mit Hilfe der Blockchain-Technologie gelöst werden. Eine Band könnte bspw. ihre Musik mit Hilfe einer Blockchain direkt an ihre Fans verkaufen und den Preis so selbst festlegen. Musiktitel können mit einem Smart Contract hinterlegt werden, der bei Nutzung der Musik die erforderliche Gebühr automatisch von dem Nutzer einfordert und danach die Musik freigibt. Der Musiker muss so nicht mehr auf die Bezahlung durch die Streamingdienste oder Musiklabels warten, sondern interagiert direkt mit den Nutzern.[414]

---

412 Z.B. https://slock.it.

413 Die Flugverspätungs-App der AXA, die auf Blockhain basiert (https://fizzy.axa), befindet sich noch in der Testphase und ist nur für ausgewählte Flüge für Kunden aus Frankreich und Italien zugänglich.

414 Z.B. https://ujomusic.com.

d) Logistik

263 In der Logistik sind komplexe Abläufe die Regel, was zu einem hohen administrativen Aufwand und vielen Dokumentenflüssen führt. Dies ist ein Feld, in dem Blockchain-Anwendungen mit hoher Intensität entwickelt werden.[415] So versucht *Maersk*, die gesamte Logistikkette auf der Blockchain abzubilden und allen involvierten Parteien den gleichen Einblick auf den aktuellen Status zu ermöglichen. Mit Smart Contracts werden dabei die einzelnen Schritte durchgesetzt, um die erforderliche Abfolge sicherzustellen. Maersk setzt dabei auf eine private Blockchain-Plattform (Hyperledger).[416]

III. Fazit

264 Je nach Quelle und Kontext werden Smart Contracts unterschiedlich definiert und ausgelegt. Den meisten Definitionen ist gemein, dass sie den Begriff *Software* enthalten oder Adjektive verwenden, die die Funktion von Software generell umschreiben. Es wird als möglichst griffige und generelle Definition Folgendes vorgeschlagen: *Ein Smart Contract ist ein auf der Blockchain-Technologie basierendes, individualisierbares Computerprogramm.* Universelle Eigenschaften des Smart Contract sind seine Eigenständigkeit, Unveränderbarkeit sowie die fehlende Interpretationsmöglichkeit.

265 Wie vorgängig aufgezeigt, existieren unzählige Smart Contracts, die je nach Ausgestaltung und verwendeter Programmierung unterschiedliche Funktionsweisen aufweisen. Ist der Smart Contract auf eine Information aus der realen Welt oder ausserhalb der Blockchain angewiesen, so wird diese durch ein Orakel abgerufen. Auch die Verbindung von Smart Contracts mit realen Gegenständen ist mit Hilfe von IoT möglich.

---

415 Z.B. von Maersk in Zusammenarbeit mit IBM.

416 www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=CPV03008USEN

B. Vertragsabschluss und Smart Contracts

266 Um gültig einen Vertrag gemäss Schweizer Recht abzuschliessen, müssen die Voraussetzungen des Obligationenrechts erfüllt sein; dies gilt unabhängig davon, welches Medium dafür verwendet wird. Für das gültige Zustandekommen eines Vertrages braucht es rechts- und geschäftsfähige Vertragsparteien (N 277 ff.), gegenseitige übereinstimmende Willenserklärungen (N 284 ff.) sowie einen Konsens über die wesentlichen Vertragsbestandteile (N 333 ff.). Zudem darf weder ein Willensmangel noch ein Irrtum oder eine Täuschung vorliegen (N 412 ff.). Im Schweizer Vertragsrecht gilt der Grundsatz der Inhalts- und Formfreiheit unter Vorbehalt bestimmter Sondernormen (N 270, 349 ff.).

267 Unbestritten ist, dass ein Smart Contract als Hilfsmittel dienen kann, einen (ausserhalb der Blockchain geschlossenen) Vertrag umzusetzen. Nachfolgend wird daher insbesondere untersucht, ob ein Smart Contract selbst das Vertragsverhältnis darstellen kann. Teilweise decken sich die Fragen, die nachfolgend untersucht werden, mit denjenigen, die sich beim Abschluss eines digitalen Vertrages generell stellen. Es werden daher neben den allgemeinen Regeln auch die zum E-Commerce erarbeiten Grundsätze herangezogen. Fragestellungen, die im Zusammenhang mit dem E-Commerce bereits ausführlich diskutiert und geklärt wurden (z.B. digitale Willenserklärung, Vertragsschluss per Mausklick etc.)[417] werden in der vorliegenden Arbeit nur kurz behandelt.

268 Bevor die soeben aufgeworfenen Problemstellungen angegangen werden, wird vorfrageweise untersucht, ob eine Programmiersprache gemäss Schweizer Recht Vertragssprache sein kann.

[417] Vgl. FREI, Konsumentenverträge im Internet, 54 ff.; GISLER, vertragliche Aspekte elektronischer Märkte, 94 ff.; WEBER, E-Commerce, 321 ff.

I. Vorfrage: Programmiersprache als Vertragssprache

269 Mit der Automatisierung von Verträgen, und insbesondere im Zusammenhang mit Smart Contracts, stellt sich die Frage, ob ein Vertrag auch direkt in Programmiersprache verfasst sein kann. Von Interesse ist diese Fragestellung selbstredend nur dort, wo sonst kein Vertrag in einer anderen (z.B. verschriftlichten) Form vorliegt.

1. Formfreiheit und Stillschweigen

270 Grundsätzlich herrscht im Schweizer Vertragsrecht Formfreiheit (siehe dazu nachfolgend N 365 f). Das heisst, der Vertrag muss weder schriftlich fixiert, noch „*sprachlich gefertigt*“ werden.[418] Gemäss HUGUENIN blickt die fehlende Sprach- und Formbedürftigkeit von Verträgen auf eine lange Entwicklung zurück.[419] Jedoch ist auch bei einer fehlenden Sprach- und Formbedürftigkeit von entscheidender Bedeutung, dass zwischen den Parteien eine übereinstimmende gegenseitige Willenserklärung vorliegt (Art. 1 OR).[420]

2. Programmiersprache

271 Software ist in einer bestimmten Programmiersprache verfasst und abgesehen von den entsprechenden Spezialisten nur durch Computer lesbar, resp. übersetzbar. Eingesetzt werden heutzutage vor allem sog. höhere Programmiersprachen, die nicht mehr direkt von einem Computer gelesen

---

418 HUGUENIN, linguistische Kommunikation und Verträge, 114.

419 HUGUENIN, linguistische Kommunikation und Verträge, 114.

420 Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 286; KRAMER/SCHMIDLIN, BK OR, Art. 1 N 4; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 1 N 2 ff.

werden müssen, sondern durch ein Übersetzungsprogramm (Compiler[421]) in Maschinensprache übersetzt werden und dadurch nicht nur problemorientierter, sondern auch einfacher verständlich sind.[422] Bekannte (höhere) Programmiersprachen sind *Java*, *C++* oder die in Blockchain-Anwendungen verbreiteten Sprachen *JavaScript*, *Go*, *Python* oder *Solidity*.[423]

3. Unterschied Programmiersprache zu konventioneller Sprache

Im Gegensatz zur natürlichen Sprache[424] kann Programmiersprache nur Syntax abbilden, jedoch keine Semantik. Programmiersprache besteht aus einer Abfolge von Zeichen, denen jeweils eine bestimmte Funktion zukommt. Es ist also nicht möglich, mittels Programmiersprache bspw. unbestimmte Rechtsbegriffe abzubilden.[425] Ein vollständig ausformulierter Vertrag kann mit Programmiersprache daher nicht aufgesetzt werden; doch ist zu bedenken, dass auch konventionelle Verträge nicht ausschliesslich vollständig oder widerspruchsfrei aufgesetzt sind. Zu denken ist hier auch an mündliche oder stillschweigend geschlossene Verträge. Programmiersprache ist im Gegensatz zu konventioneller Sprache der Allgemeinheit nicht zugänglich;[426] dies könnte 272

[421] Ein Compiler übersetzt eine (höhere) Programmiersprache in Maschinensprache, damit das Programm durch den Computer ausgeführt werden kann (vgl. HEROLD/LURZ/WOHLRAB/HOPF, Grundlagen der Informatik, 138 f.).

[422] HEROLD/LURZ/WOHLRAB/HOPF, Grundlagen der Informatik, 148 f., 233; KRYPZCYK/BOCHKOR, Programmieren, 5.

[423] Vgl. FURRER, Smart Contracts, 107; HEROLD/LURZ/WOHLRAB/HOPF, Grundlagen der Informatik, 149; WHITEPAPER HYPERLEDGER, Hyperledger Architecture, Volume II, 8.

[424] Natürliche Sprache ist die von Menschen gesprochene Sprache.

[425] Vgl. WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 18.

[426] Vgl. FURRER, der festhält, dass für interessierte Laien höhere Programmiersprachen grundsätzlich nachvollziehbar seien: FURRER, Smart Contracts, 107.

sich jedoch angesichts des technologischen Wandels und der Digitalisierung aller Lebensbereiche in Zukunft ändern.

4. Programmiersprache als Vertragssprache

273 Wie bereits ausgeführt, ist die materielle Voraussetzung für einen Vertragsabschluss gem. Art. 1 OR die gegenseitige übereinstimmende Willenserklärung. Da ein Vertrag auch ohne sprachliche Fixierung zustande kommen kann, soll er daher grundsätzlich auch in Form einer Programmiersprache aufgesetzt werden können, sofern dies dem übereinstimmenden Willen der Vertragsparteien entspricht.[427]

274 Von diesem Grundsatz zu differenzieren ist die Frage nach der Tauglichkeit eines Smart Contract, den tatsächlichen Willen der Vertragsparteien abzubilden (vgl. nachfolgend N 287 ff.), allfällige Formvorschriften einzuhalten (vgl. nachfolgend N 298 ff.) oder als Beweis vor Gericht zugelassen zu sein.

275 An dieser Stelle sei erwähnt, dass es bereits seit den 90er Jahren Bestrebungen gibt, Verträge digital zu erfassen[428] oder juristische Programmiersprachen zu entwickeln, die Verträge juristisch korrekt in Algorithmen festhalten sollen.[429] Durchgesetzt hat sich allerdings noch keines dieser Systeme. Es ist nach dem Gesagten ohnehin fraglich, ob eine solche Digitalisierung für einen Grossteil von Verträgen erforderlich ist. Die Notwendigkeit besteht allenfalls dort, wo Formvorschriften vorgesehen sind und die entsprechende gesetzliche Regelung, die wie auch immer ausgestaltete elektronische Form anerkennt.

---

427 Gleiche Ansicht für das dt. Recht: KAULARTZ/HECKMANN, Smart Contract, 621 f.

428 Als Beispiel diene der Ricardian Contract (siehe FN 377).

429 Es gibt diverse Projekte, die sich mit der Ausarbeitung von juristischen Programmiersprachen (sog. *Legal Programming*) auseinandersetzen. Für eine Übersicht über die in der Schweiz laufenden Projekte siehe <www.swisslegaltech.ch/mapping>. Kritisch zu Verträgen direkt als Code MIK, Smart Contract, 15 ff.

5. Fazit

Aufgrund der Formfreiheit im Schweizer Vertragsrecht ist es grundsätzlich möglich, dass ein Vertrag in Programmiersprache verfasst ist. Voraussetzung ist, dass dies dem Willen der Parteien entspricht und die übrigen Voraussetzungen zum gültigen Vertragsschluss gem. Obligationenrecht erfüllt sind. 276

II. Vertragsparteien: Rechts- und Geschäftsfähigkeit

277 Ein Vertragsschluss setzt mehrere beteiligte Parteien voraus; ein Vertrag kann nicht mit sich selbst abgeschlossen werden.[430] Die Rechts- und Geschäftsfähigkeit sind dabei unabdingbare Voraussetzungen an die Parteien, um Verträge rechtsgültig abschliessen zu können.[431] Um die Rechts- und Geschäftsfähigkeit zu gewährleisten, resp. überprüfen zu können, müssen sich die Parteien in irgendeiner Form identifizieren. In praktischer Hinsicht werden diese Voraussetzungen nicht getrennt voneinander, sondern vielmehr gemeinsam überprüft.

1. Rechtsfähigkeit

278 Rechtsfähig sind in der Schweiz alle natürlichen und juristischen Personen (Art. 11 und 53 ZGB).[432] Die Rechtsfähigkeit wird vermutet.[433] Allfällige Einschränkungen sind von derjenigen Partei, die daraus etwas ableiten will, zu beweisen.[434] Fehlt es an der Rechtsfähigkeit einer Partei, fehlt es auch an der vertraglichen Wirkung des Vereinbarten.[435] Die Rechtsfähigkeit ist also unabdingbar, um nach Schweizer Recht einen Vertrag gültig abzuschliessen. Dabei ist zu beachten, dass mit einer Maschine aufgrund deren fehlender Rechtspersönlichkeit kein Vertragsverhältnis eingegangen werden kann.[436]

---

430 BGE 132 III 32 E. 5.2 S. 43; SCHWENZER, BSK OR I, Art. 13 N 14 ff.

431 Vgl. BERGER, Allgemeines Schuldrecht, N 300, 305; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 299 f.

432 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 300. HÜRLIMANN-KAUP/SCHMID, Personenrecht, N 566 ff.; HOFER/HRUBESCH-MILLAUER, Personenrecht, N 11.03 f.

433 FANKHAUSER, BSK ZGB I, Art. 11 N 22.

434 STEINAUER/FOUNTOULAKIS, Droit des personnes, N 40 f. ; FANKHAUSER, ZGB I, Art. 11 N 22.

435 Vgl. FANKHAUSER, BSK ZGB I, Art. 11 N 4.

436 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 300.

Nicht zu verwechseln ist die Konstellation Mensch-Maschine jedoch mit den Fällen, in denen mittels Programmen automatisch eine Willenserklärung übermittelt wird. Dort muss sich die betreffende Partei die durch das Computerprogramm übermittelte Willenserklärung als eigene zurechnen lassen (vgl. nachfolgend N 321 ff.).[437]

2. Geschäftsfähigkeit

279 Nebst der Rechtsfähigkeit bedarf es zum gültigen Vertragsschluss auch der Geschäftsfähigkeit. Die Geschäftsfähigkeit ist (mit der Deliktsfähigkeit) eine Unterart der Handlungsfähigkeit gem. Art. 12 ZGB für natürliche, resp. Art. 54 ZGB für juristische Personen. Sie steht für die Fähigkeit einer Person, rechtsgeschäftliche Willenserklärungen abzugeben.[438] Die Handlungsfähigkeit ist sowohl für die zweiseitigen Verfügungs- und Verpflichtungsgeschäfte als auch für die einseitigen Rechtsgeschäfte unabdingbar; durch sie werden Rechte und Pflichten begründet.[439] Natürliche Personen müssen volljährig (Vollendung des 18. Lebensjahres, Art. 14 ZGB)[440] sowie urteilsfähig (Art. 16 ZGB)[441] sein und dürfen nicht unter umfassender Beistandschaft stehen (Art. 17 ZGB).[442] Juristische Personen sind handlungsfähig, sobald nach

---

437 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 300; WEBER, E-Commerce, 340.

438 HOFER/HRUBESCH-MILLAUER, Personenrecht, N 10.14; HUGUENIN, OR, N 142; HÜRLIMANN-KAUP/SCHMID, Personenrecht, N 591.

439 HOFER/HRUBESCH-MILLAUER, Personenrecht, N 10.14; HÜRLIMANN-KAUP/SCHMID, Personenrecht, N 590 ff.; FANKHAUSER, BSK ZGB I, Art. 12 N 12 f.

440 HOFER/HRUBESCH-MILLAUER, Personenrecht, N 10.17; HUGUENIN, OR, N 145 ff.; HÜRLIMANN-KAUP/SCHMID, Personenrecht, N 611 ff.

441 Urteilsfähig ist, wer vernunftgemäss handeln kann, d.h. wer nicht wegen Kindesalters, infolge geistiger Behinderung, psychischer Störung, Rausch oder ähnlicher Zustände in seinem vernunftgemässen Handeln eingeschränkt ist (Art. 16 ZGB); FANKHAUSER, BSK ZGB I, Art. 16 N 1 ff.; HÜRLIMANN-KAUP/SCHMID, Personenrecht, N 601 ff.

442 Vgl. FANKHAUSER, BSK ZGB I, Art. 17 N 4.

Gesetz und Statuten die erforderlichen Organe bestellt sind (Art. 54 ZGB).[443] Die Handlungsfähigkeit (resp. Geschäftsfähigkeit) wird vermutet, die Handlungsunfähigkeit muss von der Partei bewiesen werden, die diese behauptet.[444] Auch beschränkt Handlungsunfähige (bspw. urteilsfähige handlungsunfähige Personen, Art. 19-19c ZGB) können teilweise geschäftsfähig sein und rechtswirksam gewisse Rechtsgeschäfte abschliessen (Art. 19 Abs. 1 und 2 ZGB).[445] Die fehlende Geschäftsfähigkeit als Folge der fehlenden Urteilsfähigkeit bewirkt die Nichtigkeit des Vertrages (Art. 18 ZGB).[446] Fehlt es hingegen einem Urteilsfähigen an der vorausgesetzten Handlungsfähigkeit, so ist der Vertrag ohne Zustimmung des gesetzlichen Vertreters für ihn einseitig unverbindlich.[447]

3. Rechts- und Geschäftsfähigkeit bei Smart Contracts

280 Wie bereits dargelegt, kann ein Smart Contract grundsätzlich auf einer öffentlichen oder einer privaten Blockchain-Plattform implementiert sein (vgl. N 80, 84, 251 ff.). Dabei stellt sich die Frage, ob die Teilnehmer in irgendeiner

---

443 Vgl. BERGER, Allgemeines Schuldrecht, N 391; HUGUENIN/REITZE, BSK ZGB I, Art. 54 N 2.

444 FANKHAUSER, BKS ZGB I, Art. 12 N 40; HÜRLIMANN/SCHMID, Personenrecht, N 595.
Der gute Glaube an die Handlungsfähigkeit wird jedoch nicht geschützt: BGE 107 II 105 E. 6a S. 116, 89 II 387 E. 2 S. 389; BERGER, Allgemeines Schuldrecht, N 319; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 301.

445 Vgl. BERGER, Allgemeines Schuldrecht, N 322; HOFER/HRUBESCH-MILLAUER, Personenrecht, N 10.26 ff.; HÜRLIMANN-KAUP/SCHMID, Personenrecht, N 597 ff.

446 FANKHAUSER, BSK ZGB I, Art. 18 N 3, 6 ff.; HOFER/HRUBESCH-MILLAUER, Personenrecht, N 10.43.

447 BERGER, Allgemeines Schuldrecht, N 311 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 302; HOFER/HRUBESCH-MILLAUER, Personenrecht, N 10.40.

Weise zwecks Feststellung der Rechts- und Geschäftsfähigkeit identifiziert werden (können).

a) Öffentliche Blockchain

281 Das Prinzip der öffentlichen Blockchain ist, dass sie jedermann zugänglich ist (vgl. N 33). Es ist fraglich, wie die Parteien bei einem Vertragsschluss auf einer öffentlichen Blockchain die Rechts- und Geschäftsfähigkeit der potentiellen Vertragspartei sicherstellen. Da die öffentliche Blockchain grundsätzlich jedermann zugänglich ist und ohne Zentralinstanz auskommt, ist eine wie auch immer geartete Form der Zulassungskontrolle (z.B. zugelassen wird nur, wer sich identifiziert) nicht realistisch und widerspricht der Grundkonzeption. Es ist daher in der Verantwortung der potentiellen Vertragsparteien, die Rechts- und Geschäftsfähigkeit ihrer Vertragspartner zu überprüfen oder einen entsprechenden Nachweis zu verlangen. Eine Möglichkeit würde darin bestehen, dass eine Applikation für den Vertragsschluss genutzt wird, welche die Identifizierung der Parteien übernimmt, resp. die Rechts- und Geschäftsfähigkeit der Vertragspartner überprüft oder nachweist.

b) Private Blockchain

282 Werden Verträge auf einer privaten Blockchain (vgl. N 35 f.) geschlossen, kann von Anfang an eine Identifizierung der Teilnehmer vorgesehen werden. So können nur Teilnehmer zur Blockchain zugelassen werden, die vorgängig ihre Rechts- und Geschäftsfähigkeit nachweisen, resp. sich identifizieren können. In der Regel sind sich die Teilnehmer eines geschlossenen Netzwerkes bereits bekannt oder können sich gegenseitig identifizieren. Die Ausgestaltung des Identitätsnachweises richtet sich nach den Regeln der Blockchain oder der Applikation. Aber auch bei einer privaten Blockchain gilt, dass es dem einzelnen Nutzer obliegt, ob und wie er den Nachweis der Rechts- und Geschäftsfähigkeit seines Vertragspartners einholt.

4. Fazit

283 Der Nachweis der Rechts- und Geschäftsfähigkeit von Vertragsparteien kommt bei der Anwendung von Smart Contracts einer Identifizierung der Teilnehmer gleich. Entweder verwenden die Nutzer einer öffentlichen Blockchain eine Applikation, auf der Identifizierungen vorgenommen werden oder sie stellen auf anderem Wege sicher, dass ihre Vertragspartei rechtsgültig Geschäfte abschliessen darf. Das Gleiche gilt für Smart Contracts auf privaten Blockchains, wobei bei diesen eher davon ausgegangen werden kann, dass die Parteien ihre Identität offengelegt haben oder diese nachvollziehbar ist.

III. Rechtsbindungswille und Willenserklärung: Antrag und Annahme

284 Für den Abschluss eines Vertrages braucht es einen Antrag sowie eine Annahme der Parteien. Die Parteien benötigen einen Rechtsbindungswillen, ein vertragliches Verhältnis eingehen zu wollen.

285 Auch für elektronische Willenserklärungen gelten die Grundsätze des Obligationenrechts.[448] Im elektronischen Geschäftsverkehr wird die Willenserklärung oftmals nur durch einen Mausklick kundgetan,[449] kann aber auch als individuell verfasste Erklärung elektronisch versendet werden (z.B. mittels E-Mail oder via Webformular).[450]

286 Die Blockchain eignet sich grundsätzlich als System, um Antrag und Annahme zusammenzufügen.[451] Dabei ist zu unterscheiden, ob bspw. ein Angebot mit einem Smart Contract in eine Blockchain-Plattform gesetzt wird, wonach bei Zustimmung durch eine andere Partei automatisch das vordefinierte Geschäft ausgeführt wird, ob die Parteien einen Vertrag direkt als Smart Contract aufsetzen oder ob ein Smart Contract von den Vertragsparteien dafür benutzt wird, das vorher vereinbarte Grundgeschäft abzubilden und ggf. abzuwickeln.[452] Bei letzterer Variante entscheiden sich die Fragen über Antrag und Annahme nach dem Grundgeschäft ausserhalb des Smart Contract. Sollte der Smart Contract das Grundgeschäft selbst darstellen, so stellen sich nachfolgende Fragen unabhängig davon, ob der Smart Contract auf einer öffentlichen oder auf einer privaten Blockchain eingesetzt wird.

---

448 Vgl. WEBER, E-Commerce, 345.

449 WEBER, E-Commerce, 339.

450 BALSCHEIT, Konsumvertragsrecht, 168.

451 Gem. EGGEN ein “Matchingsystem”: EGGEN, Chain of Contracts, 7.

452 Für letztere Konstellation Vgl. FURRER, Smart Contracts, 111.

1. Rechtsbindungswille

287 Gemäss Art. 1 OR braucht es für das Zustandekommen eines Vertrages eine übereinstimmende gegenseitige Willenserklärung (Abs. 1). Diese Zustimmung kann ausdrücklich oder stillschweigend sein (Abs. 2). Die zeitlich erste Willenserklärung besteht aus dem Antrag, die zweite aus der Annahme.[453]

a) Allgemeine Regeln

288 Mit dem Antrag erklärt der Antragsteller seinen endgültigen Vertragsabschlusswillen.[454] Davon zu unterscheiden ist die Einladung zur Offertenstellung (*invitatio ad offerendum*), die sich an eine oder mehrere Personen richten kann und mit der erst die Bereitschaft zu einem Vertragsabschluss – jedoch ohne endgültigen Abschlusswillen – kundgetan wird.[455]

289 Der (Rechtsbindungs-, Rechtsfolge- oder Geschäfts-) Wille im juristischen Sinne ist das Resultat einer psychischen Leistung, *„des gegenseitigen Abwägens der verschiedenen Strebungen und der Gewinnung eines Standpunktes, bei dem behaftet zu werden man gewillt ist.“*[456] Das Vorliegen eines Bindungswillens ist elementar für die Abgrenzung eines Vertrages von einem Gefälligkeitsgeschäft.[457] Wird der Wille nach dem Vertrauensprinzip ausgelegt, dann wird ein Bindungswille verneint bei *„Gefälligkeitshandlungen*

---

453 BERGER, Allgemeines Schuldrecht, N 647, 668; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 363 ff.; SCHWENZER, OR AT, N 28.01; WEBER, E-Commerce, 340.

454 BERGER, Allgemeines Schuldrecht, N 648; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 363; SCHWENZER, OR AT, N 28.09.

455 BERGER, Allgemeines Schuldrecht, N 648; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 369; vgl. SCHWENZER, OR AT, N 28.09.

456 ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 1 N 3.

457 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 353a; vgl. HÜRLIMANN-KAUP, privatrechtliche Gefälligkeit, N 110.

des täglichen Lebens, bei Zusagen im rein gesellschaftlichen Verkehr oder bei ähnlichen Vorgängen".[458]

290 Die Annahme ist die Kundgabe des Vertragsabschlusswillens und muss als zweite Willenserklärung mit dem Antrag übereinstimmen – weicht sie inhaltlich vom Angebot ab, gilt dies grundsätzlich als Gegenangebot.[459]

b) Im elektronischen Geschäftsverkehr

291 Auch im elektronischen Rechtsverkehr gilt, dass zum gültigen Abschluss eines Vertrages ein Rechtsbindungswille vorliegen muss. In den Anfangszeiten des E-Commerce schien es fraglich, ob ein Nutzer sich aufgrund der unzähligen erforderlichen Mausklicks bewusst ist, wann er mittels Klick einen Vertrag eingeht.[460] Zwischenzeitlich ist anerkannt, dass ein Mausklick dem Absender zugerechnet wird (vgl. N 323).[461] Internetseiten sind u.a. auch aufgrund von regulatorischen Vorgaben so ausgestaltet, dass explizit auf das Eingehen eines Vertragsverhältnisses hingewiesen werden muss.[462] In der Regel müssen die AGB vorgängig akzeptiert werden. Ein zufälliges Eingehen einer rechtlichen Beziehung ohne Rechtsbindungswille im elektronischen Geschäftsverkehr ist daher unwahrscheinlich.

c) Bei Smart Contracts

292 In den Fällen, in denen ein Smart Contract zur Abbildung und/oder zur Durchsetzung eines ausserhalb der Blockchain geschlossenen Vertrages eingesetzt wird, ist der Rechtbindungswille in diesem Grundgeschäft zu verorten. Der Geschäftswille muss sich nur dann auf die Verwendung des Smart Contract (bspw. als Abbildungs- oder Durchsetzungsinstrument)

---

458 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 353b m.w.H; HÜRLIMANN-KAUP, privatrechtliche Gefälligkeit, N 116.

459 BERGER, Allgemeines Schuldrecht, N 670; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 435, 441; SCHWENZER, OR AT, N 28.31.

460 Vgl. WEBER, E-Commerce, 339 f.

461 WEBER, E-Commerce, 340.

462 Z.B. Art. 11 E-Commerce RL.

beziehen, wenn die Verwendung des Smart Contract einen wesentlichen Hauptpunkt des Vertrages darstellt.[463]

293 In den übrigen Fällen ist zu differenzieren, ob es sich bei den beteiligten Parteien um fachkundige Personen handelt, die von den wesentlichen Regelungen im Smart Contract Kenntnis nehmen können (bspw. durch Kenntnis der Programmiersprache), ob es beiden Parteien möglich ist, den Inhalt eines Smart Contract in zumutbarer Weise zu erschliessen oder ob ein Gefälle im Verständnishorizont der Parteien besteht.

aa) Fachkundige Personen

294 Verwenden fachkundige Parteien einen Smart Contract, ohne dabei vorgängig einen anderen Vertrag abzuschliessen, ist zu vermuten, dass die Nutzung des Smart Contract und die darin enthaltenen Bedingungen dem Willen der Parteien entsprechen.[464] Da eine Programmiersprache grundsätzlich Vertragssprache sein kann (N 273 ff.), stellt in dieser Konstellation der Smart Contract direkt den Vertrag dar[465] – unter Voraussetzung der übrigen notwendigen Elemente für einen gültigen Vertragsabschluss. Da sich ein Smart Contract auf Informationen (Ereignisse) bezieht, die bei Vertragsschluss noch nicht vorliegen, handelt es sich dabei i.d.R. um einen (resolutiv oder suspensiv)

---

463 Vgl. FURRER, Smart Contracts, 106.

464 A.A. SCHALLER, blogpost 32, N 6; SCHALLER, blogpost 34, N 8.

465 A.A. SCHALLER, der die Meinung vertritt, dass der Vertrag „eine juristische Sekunde“ zuvor zustande kommt: Die Parteien würden den Vertrag jeweils schriftlich, mündlich oder konkludent im Vorfeld schliessen und erst danach in einen Smart Contract überführen; ausser, die Parteien hätten explizit erklärt, erst gebunden sein zu wollen, wenn der Vertrag als Smart Contract vorliegt (SCHALLER, blogpost 32, N 4, 6.). Dieser Meinung ist im Grundsatz insofern zu widersprechen, als dies konsequenterweise auch für Vertragsschlüsse ohne Smart Contracts gelten müsste: Bei einem schriftlich fixierten Vertrag kommt der Vertrag in der Regel nicht schon im Vorfeld mündlich oder konkludent zustande; vielmehr ist dies das Stadium der vorvertraglichen Verhandlungen.
A.A. auch FURRER, nach dem der Smart Contract kein eigenständiger Vertrag ist, aber den gemeinsamen Willen der Vertragsparteien reflektiert: FURRER, Smart Contracts, 109.

bedingten Vertrag (Art. 151 Abs. 1 OR).[466] Ein bedingter Vertrag kann aufgrund der Privatautonomie für Schuldverhältnisse und auch für Verfügungsgeschäfte eingesetzt werden.[467] Bedingungsfeindlich sind jedoch diejenigen Rechtsgeschäfte, die zu einer unzumutbaren Beeinträchtigung der Rechtssicherheit führen oder eine widerrechtliche oder sittenwidrige Absicht beinhalten.[468]

bb) Fachunkundige Personen

295 Obwohl sich die Blockchain-Technologie immer grösserer Beliebtheit erfreut, ist aus heutiger Sicht das Szenario, dass eine unkundige Person „aus Versehen" einen Smart Contract implementiert, ziemlich unwahrscheinlich. Soll ein Smart Contract auf einer Blockchain initiiert und ein Vermögenswert auf die Adresse des Smart Contract übertragen werden, erfordert dies immer eine aktive Handlung durch mindestens eine Partei. Durch diese aktive Handlung kann der Partei auch ein Handlungswille zugeschrieben werden. Ob diese Handlung jeweils auch einen Geschäftswillen beinhaltet, kann nur im Einzelfall beurteilt werden. Fest steht jedoch, dass durch das Signieren mit dem Private Key die Partei bewusst eine Transaktion auslöst.

296 Sollte dabei den Parteien die Tragweite der signierten Transaktion nicht bewusst sein (resp. sie können aufgrund fehlender Kenntnissen die Inhalte des Smart Contract nicht in zumutbarer Weise erschliessen) und kein Bindungswille mit den damit verbundenen (rechtlichen) Folgen vorhanden sein, dann stellt der Smart Contract selbst keinen Vertrag dar. In dieser Konstellation ist es jedoch fraglich, ob den Parteien bei bewusster Nutzung eines Smart Contract ohne die Kenntnisse des konkreten Inhaltes die Berufung

---

466 Laut Art. 151 Abs. 1 OR ist die Bedingung der Eintritt einer ungewissen Tatsache. Die Bedingung steht für ein objektiv ungewisses zukünftiges Ereignis, von dem nach dem Willen der Parteien die Wirksamkeit des Vertrages abhängt: EHRAT/WIDMER, BSK OR I, Vorbem. Art. 151-157 N 1.

467 EHRAT/WIDMER, BSK OR I, Vorbem. Art. 151-157 N 4; BERGER, Allgemeines Schuldrecht, N 790; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3952.

468 EHRAT/WIDMER, BSK OR I, Vorbem. Art. 151-157 N 5a; BERGER, Allgemeines Schuldrecht, N 794 f.

auf den fehlenden Geschäftswillen aufgrund des Rechtmissbrauchsverbots verwehrt sein soll (vgl. N 412 ff.).[469]

cc) Fachkundige und fachunkundige Personen

297 Wird ein Vertrag mit einem Smart Contract aufgesetzt und sind die involvierten Parteien eine fachkundige Person und eine fachunkundige Person, ist wiederum eine Einzelfallbetrachtung notwendig. Handelt es sich bei der fachunkundigen Person um einen Konsumenten[470] und bei der fachkundigen Person um ein Unternehmen, dann ist aufgrund der fehlenden Übersetzung des Vertrages in natürliche Sprache davon auszugehen, dass der Smart Contract nicht den Vertrag selbst darstellt (vgl. nachfolgend N 306). Handelt es sich nicht um einen Konsumentenvertrag, dann ist zu prüfen, worauf sich der Wille der fachunkundigen Person gerichtet hat. Wenn es der fachunkundigen Person in zumutbarer Weise möglich war, vom Inhalt des Smart Contract Kenntnis zu nehmen (z.B. durch Erkundigung bei der Vertragspartei), dann stellt der Smart Contract direkt den Vertrag dar – unter Vorbehalt der Erfüllung der übrigen Voraussetzungen zum gültigen Vertragsabschluss.

469 KAULARTZ/HECKMANN, Smart Contract, 624 (dt. Recht); vgl. WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 10; ausführlich zum Rechtsmissbrauchsverbot statt vieler HAUSHEER/AEBI-MÜLLER, BK ZGB, Art. 2 N 41 ff.

470 Unter Konsument ist eine natürliche Person zu verstehen, die für den persönlichen oder familiären Gebrauch Waren oder Dienstleistungen erwirbt (KRAMER/PROBST/PERRIG, AGB, 62); vgl. Art. 40a ABS. 1 OR, Art. 32 Abs. 2 ZPO, Art. 120 Abs. 1 IPRG oder Art. 15 Abs. 1 LugÜ.

2. Adressatenkreis und Formvorschriften

298 Der Antrag und die Annahme kann sich an einen bestimmten oder unbestimmten Adressatenkreis richten und unterliegt allenfalls Formvorschriften, wenn das angebotene Geschäft einer Formvorschrift unterliegt.

a) Allgemeine Regeln

299 Der Antrag kann sich an Anwesende (Art. 4 OR)[471] oder Abwesende (Art. 5 OR)[472] richten und ist grundsätzlich formfrei möglich (Art. 11 OR).[473] Ausnahmen bilden diejenigen Verträge, die einer gesetzlichen Formvorschrift unterliegen (Art. 11 und 16 OR); hier unterliegt sowohl der Antrag als auch die Annahme grundsätzlich der entsprechenden Formvorschrift.[474] Der Antragsteller kann sein Angebot an einen einzigen Empfänger oder an einen unbestimmten Personenkreis richten.[475] Die Auslage von Ware inkl. Preisangabe stellt gem. Art. 7 Abs. 3 OR in der Regel einen Antrag dar; diese Regelung gilt jedoch nicht für Dienstleistungen.[476] Keinen Antrag stellt die

---

471 Hier wird davon ausgegangen, dass sich die Parteien am gleichen Ort befinden oder miteinander am Telefon verbunden sind, vgl. BERGER, Allgemeines Schuldrecht, N 655 f.; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 4 N 3.

472 Unter Abwesenden wird verstanden, dass die Parteien in keiner unmittelbaren Kommunikation stehen, vgl. BERGER, Allgemeines Schuldrecht, N 657.

473 Die Willenserklärung kann in Form der reinen Erklärung (Sprache oder nonverbale Ausdrucksmittel, d.h. Handlung bezweckt den Ausdruck des Geschäftswillens), durch konkludentes Verhalten, durch mündliche oder schriftliche Erklärung (z.B. auch via E-Mail), mittelbar oder unmittelbar oder ausdrücklich oder stillschweigend erfolgen: GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, 178 ff.; SCHWENZER, OR AT, N 27.09 f., 27.12.

474 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 385 f.; vgl. SCHWENZER, BSK OR I, Art. 11 N 12 f.

475 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 387 f.

476 ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 7 N 10.

Auskündung gem. Art. 7 Abs. 2 OR dar; betroffen davon ist das Versenden von Tarifen, Preislisten und dergleichen (bspw. Kataloge, Muster etc.).[477]

b) Im elektronischen Geschäftsverkehr

300 Das Angebot von Waren und Dienstleistungen im Internet stellt nach h.L. eine Auskündung gem. Art. 7 Abs. 2 OR dar.[478] Je nach Umstand kann aber auch auf ein konkretes Angebot geschlossen werden, so z.B. in den Fällen, in denen sich die Dienstleistung oder die Ware (darunter sind in diesem Zusammenhang auch unkörperliche Sachen zu verstehen) auf dem Rechner des Anbieters befindet und direkt bezogen werden kann (Bsp. Software, Informationen wie Zeitungsartikel) oder wenn der Kunde direkt mit der Kreditkarte (o.ä. Zahlungsmitteln) bezahlen muss und konkrete Liefertermine abgesprochen sind.[479] Die Fälle, in denen von einem konkreten Angebot im Internet ausgegangen wird, können nicht eng umschrieben werden, sondern bedürfen vielmehr einer Einzelfallbetrachtung.[480]

301 Stellt die online dargebotene Ware oder Dienstleistung eine Einladung zur Offertenstellung dar, dann unterbreitet der Kunde mittels E-Mail oder Webformular ein verbindliches Angebot und der Vertrag kommt dann zustande, wenn der Anbieter der Ware oder der Dienstleistung das Angebot unverändert annimmt.[481]

302 Sollte das Rechtsgeschäft Formvorschriften unterliegen, dann sind diese auch im elektronischen Geschäftsverkehr zu beachten. Hierzu ist die Regelung in Art. 14 Abs. 2bis OR zu erwähnen, die die qualifizierte elektronische Unterschrift der eigenhändigen Unterschrift gleichstellt (vgl. nachfolgend N 390 ff.).

---

477 BERGER, Allgemeines Schuldrecht, N 663; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 373 ff.; SCHWENZER, OR AT, N 28.10.

478 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 374, 377; WEBER, E-Commerce, 341 f.

479 WEBER, E-Commerce, 342.

480 WEBER, E-Commerce, 342.

481 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 441; WEBER, E-Commerce, 342.

c) Bei Smart Contracts

303 Ein Angebot mittels Smart Contract kann sich sowohl in einer öffentlichen als auch in einer privaten Blockchain an einen bestimmten oder unbestimmten Personenkreis richten.

304 Onlineangebote von Waren oder Dienstleistungen werden nicht als Angebote qualifiziert, sondern als eine invitatio ad offerendum (vgl. N 300). Smart Contracts, die eine Ware oder Dienstleistung (an einen bestimmten oder unbestimmten Personenkreis) anbieten, sind daher ebenfalls grundsätzlich nicht als Angebot, sondern als Einladung zur Offertenstellung zu betrachten. Dies gilt unabhängig davon, ob der Smart Contract auf einer öffentlichen oder auf einer privaten Blockchain-Plattform implementiert ist.

305 Wie bei jedem Onlineangebot, kann auch mit einem Smart Contract ein verbindliches Angebot übermittelt werden; nämlich dann, wenn die Ware oder Dienstleistung direkt bezogen werden kann (z.B. Benutzung einer Plattform, Zugang zu Informationen etc.) oder wenn der Kunde direkt eine Gegenleistung (z.B. Zahlung mit einer Kryptowährung) tätigen muss und konkrete Liefertermine vorliegen (vgl. N 300).

306 Beschlägt das mit einem Smart Contract übermittelte Angebot ein Rechtsgeschäft, das einer Formvorschrift unterliegt, dann ist auch der Antrag und die Annahme von dieser Formvorschrift betroffen (zur Formvorschrift vgl. nachfolgend N 364 ff.).

307 Richtet sich das in einem Smart Contract verankerte Angebot an Konsumenten, dann ist jeweils eine Verschriftlichung der im Smart Contract hinterlegten Regeln (z.B. in Form von Allgemeinen Geschäftsbedingungen, AGB[482]) von Nöten, um aus konsumentenschützerischer Sicht eine Übervorteilung von Verbrauchern zu verhindern. Es sind dabei die jeweils spezialgesetzlichen

[482] AGB sind generell vorformulierte Vertragsbestimmungen, die auf eine Vielzahl von Verträgen angewendet werden können; Zweck ist eine Rationalisierung im Geschäftsverkehr im Sinne einer effizienten Abwicklung von Verträgen: GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1117 f.; KRAMER/PROBST/PERRIG, AGB, N 2, 73.

Regelungen (z.B. im Konsumkreditgesetz[483] oder bei Haustürgeschäften) zu beachten. Rechtssicherheit besteht in diesen Fällen erst dann, wenn eine Übersetzung in eine natürliche Sprache vorliegt.[484] Sind Smart Contracts als AGB ausgestaltet, so ist eine Textform erforderlich; mündliche AGBs sind nicht zulässig.[485] Das Texterfordernis kann auch in elektronischer Form (bspw. USB-Speicher, PDF, E-Mail, SMS) erfüllt werden; es braucht hierzu keinen traditionellen Erklärungsträger. Erforderlich ist einzig, dass die elektronische Datei einfach zu finden und gut lesbar ist.[486] AGB müssen von den Vertragsparteien angenommen werden, ansonsten sie nicht Teil des Vertrages werden.[487] Die Übernahme erfolgt dann, wenn die Vertragspartei deutlich darauf hingewiesen wurde und die Möglichkeit besteht, sich in zumutbarer Weise Kenntnis des Inhaltes zu verschaffen.[488] Für elektronische Verträge gilt ebenfalls die Pflicht eines deutlichen Hinweises auf die AGB; eine blosse Veröffentlichung der AGB im Internet reicht hierfür nicht.[489] Erforderlich ist vielmehr ein ohne grossen Aufwand möglicher Direktzugriff auf die AGB vor Vertragsschluss, resp. spätestens bei Abgabe der Willenserklärung.[490] Nach erfolgter Übernahme durch die Parteien können AGB einer richterlichen

---

483 Bundesgesetz über den Konsumkredit (KKG) vom 23. März 2001, SR 221.214.1.

484 WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 9.

485 KRAMER/PROBST/PERRIG, AGB, N 75.

486 KRAMER/PROBST/PERRIG, AGB, N 75.

487 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1124; vgl. KRAMER/PROBST/PERRIG, AGB, N 112 ff.

488 KRAMER/PROBST/PERRIG, AGB, N 161.

489 KRAMER/PROBST/PERRIG, AGB, N 163.

490 KRAMER/PROBST/PERRIG, AGB, N 120.

Kontrolle bezüglich Konsens,[491] Auslegung[492] und Inhalt[493] unterzogen werden.[494]

3. Zugang der Willenserklärung und Frist

308 Der Offerent ist grundsätzlich eine bestimmte Zeit an seinen Antrag gebunden. Die Willenserklärungen müssen bei der jeweils anderen Partei zugehen, ansonsten kein Vertrag gültig zustande kommen kann.

a) Allgemeine Regeln

309 Der Antrag wie auch die Annahme sind in der Regel empfangsbedürftig.[495] Die Erklärung muss hierzu beim Empfänger eingehen, d.h. sie wird erst wirksam, wenn sie beim Empfänger zugegangen ist.[496] Während bei unmittelbaren Erklärungen (Antrag an Anwesende) der Zugang und die Kenntnisnahme durch den Empfänger zusammenfallen, fällt dies bei mittelbaren Erklärungen (Antrag an Abwesende) auseinander.[497] Die Erklärung wird bei mittelbaren Willenserklärungen dann wirksam, wenn sie beim Empfänger eintrifft

---

491 Ausführlich zur Konsenskontrolle KRAMER/PROBST/PERRIG, AGB, N 109 ff.

492 Ausführlich zur Auslegungskontrolle KRAMER/PROBST/PERRIG, AGB, N 235 ff.

493 Ausführlich zur Inhaltskontrolle KRAMER/PROBST/PERRIG, AGB, N 290 ff.

494 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1124 ff.; KRAMER/PROBST/PERRIG, AGB, N 18 ff.

495 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 194; vgl. SCHWENZER, OR AT, N 28.10.

496 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 196 f.; SCHWENZER, OR AT, N 27.22.

497 BERGER, Allgemeines Schuldrecht, N 684; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 196; SCHWENZER, OR AT, N 27.23.

(Empfangstheorie).[498] Nicht empfangsbedürftige Willenserklärungen entfalten ihre Wirkung mit der Äusserung.[499]

310 Stellt der Antragsteller eine Frist, dann ist er bis zum Ablauf dieser Frist an sein Angebot gebunden (Art. 3 OR). Bei einem Antrag an Abwesende ist der Antragsteller so lange gebunden, wie eine Antwort des Antragempfängers bei ordnungsgemässer und rechtzeitiger Absendung erwartet werden darf (Art. 5 Abs. 1 OR), d.h. es besteht eine Frist, die sich aus der Dauer der Übermittlungen (Angebot und Annahme) sowie einer Bedenkfrist des Offertenempfängers zusammensetzt.[500]

b) Im elektronischen Geschäftsverkehr

311 Elektronische Willenserklärungen sind i.d.R. mittelbar,[501] weshalb auch die Empfangstheorie zur Anwendung kommt. Bei elektronischen Willenserklärungen gilt die Mitteilung mit der Speicherung auf einem Rechner des Empfängers oder mit der Speicherung auf einem fremden Rechner, sobald er diese abrufen kann (z.B. elektronisches Postfach, Zugang durch Passwort), als zugegangen.[502]

312 In den Fällen, in denen die Onlineanpreisung als direktes Angebot qualifiziert werden kann, ist der Anbieter solange an sein Angebot gebunden, bis die angemessene Übermittlungs- und Bedenkfrist des Empfängers abgelaufen ist (vgl. N 310). Im elektronischen Geschäftsverkehr dürften insbesondere die Übermittlungsfristen von Angebot und Akzept sehr kurz sein.[503] Für die

---

498 BERGER, Allgemeines Schuldrecht, N 242; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 196 f..

499 BERGER, Allgemeines Schuldrecht, N 682; SCHWENZER, OR AT, N 27.18.

500 ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 5 N 5.

501 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 186; WEBER/JÖHRI, Vertragsschluss im Internet, 45.

502 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, 202; SCHWENZER, OR AT, N 27.23; WEBER/JÖHRI, Vertragsschluss im Internet, 45; vgl. auch Art. 11 E-Commerce RL.

503 Für die Kenntnisnahme kann gemäss WEBER der Absender aber davon ausgehen, dass min. einmal pro Tag eine Mailbox geleert wird: WEBER, E-Commerce, 344.

Bemessung der angemessenen Bedenkfrist des Empfängers ist jeweils eine Einzelfallbetrachtung notwendig (wobei objektive Kriterien, wie die Art des Geschäftes oder die Usanz, sowie subjektive Kriterien, wie die Dauer der Ermittlung notwendiger Informationen, Kenntnis der Interessenlage der anderen Partei etc. zu berücksichtigen sind).[504]

c) Bei Smart Contracts

313 Auch bei einem Smart Contract gilt, dass der Antrag und die Annahme beim Empfänger zugegangen sein müssen (vgl. N 309).

314 Für die Bemessung der Frist, in der der Antragssteller an seine Offerte gebunden ist, muss ebenfalls eine Einzelfallbetrachtung vorgenommen werden (vgl. N 312).

315 Für die Verbindlichkeit einer Offerte ist die Ausgestaltung eines Smart Contract von Bedeutung. Stellt ein Smart Contract initial das Grundgeschäft dar und enthält er ein Angebot an einen bestimmten oder unbestimmten Personenkreis, dann muss er entweder zeitlich terminiert oder so programmiert sein, dass dieses Angebot entweder deaktiviert oder abgeändert werden kann. Ansonsten ist das Angebot unveränderbar und für „immer“ (solange jedenfalls, wie die entsprechende Blockchain-Plattform besteht) veröffentlicht. In den Fällen, in denen das Angebot als Einladung zur Offertenstellung qualifiziert würde, wäre das Problem insofern entschärft, als die darauf eingegangene Offerte jeweils akzeptiert werden müsste und dies unterlassen werden kann. Enthält das Angebot jedoch eine Leistung oder Ware, die direkt bezogen wird oder werden gegen direkte Bezahlung (automatisch) konkrete Liefertermine vereinbart, dann muss der Angebotsteller dafür besorgt sein, diesen Smart Contract ggf. terminiert oder deaktivierbar auszugestalten, da er ansonsten allenfalls schadenersatzpflichtig wird (vgl. nachfolgend N 412 ff.).

504 ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 5 N 5 ff.

4. Zeitpunkt des Vertragsabschlusses

316 Je nachdem, ob der Vertrag unter Anwesenden oder Abwesenden zustande kommt, unterscheidet sich der Zeitpunkt des Zustandekommens des Vertrages. Beim elektronischen Geschäftsverkehr ist von einem Vertragsschluss unter Abwesenden auszugehen.

a) Allgemeine Regeln

317 Der Vertrag kommt unter Anwesenden sofort zustande, falls keine Frist vereinbart wurde (Art. 4 Abs. 1 OR).[505] Unter Abwesenden kommt der Vertrag mit Zugang der Annahmeerklärung beim Offerenten zustande, wobei der Antragsteller bei einem Antrag ohne Frist zur Annahme so lange an seine Offerte gebunden ist, bis der Eingang der Annahmeerklärung bei ordnungsgemässer und rechtzeitiger Absendung durch den Akzeptanten erwartet werden darf (Art. 5 Abs. 1 OR).[506] Die Gestaltungswirkung dieses Vertrages kann jedoch bereits zum Zeitpunkt der Absendung der Annahmeerklärung zurückbezogen werden (Art. 10 Abs. 1 OR).[507]

b) Im elektronischen Geschäftsverkehr

318 Auch beim elektronischen Geschäftsverkehr gilt, dass der Vertrag zu dem Zeitpunkt entsteht, zu dem die Annahmeerklärung beim Offerenten eintrifft (N 317). Durch die stark verkürzte, resp. kaum mehr vorhandene Übermittlungsfrist beim elektronischen Geschäftsverkehr kann die Absendung einer Annahmeerklärung mit dem Zugang der Annahme beim Empfänger

---

505 BERGER, Allgemeines Schuldrecht, N 682; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 460; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 4 N 3 ff.

506 Vgl. ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 5 N 1 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 410; SCHWENZER, ORT AT, 28.20.

507 BERGER, Allgemeines Schuldrecht, N 683; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 461 f.; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 10 N 3.

zusammenfallen.[508] Somit gilt aufgrund des faktischen Wegfalls der Übermittlungsfrist der Zeitpunkt der Versendung als Zeitpunkt des Vertragsschlusses.[509]

c) Bei Smart Contracts

319 Bei einem Vertragsschluss mit Smart Contracts stellt sich die Frage, mit welcher Handlung die Annahme erklärt wird und zu welchem Zeitpunkt der Vertrag zustande kommt. Wird das Grundgeschäft ausserhalb des Smart Contract geschlossen, dann ist in diesem Verhältnis zu prüfen, wie die Annahme erklärt und wann die Annahme versendet wurde. Kommt der Vertrag direkt mit einem Smart Contract zustande, dann ist zu bestimmen, mit welchem konkreten Vorgang die Annahme erklärt wird. In Frage kommen zwei Zeitpunkte: Entweder geschieht dies durch die Signierung des Angebots durch den Empfänger mit seinem Private Key (= Akzept) oder erst durch den Validierungsmechanismus der Transaktion (gem. Konsensprotokoll, vgl. N 61 ff.) der entsprechenden Blockchain-Plattform, in der der Smart Contract implementiert ist. Für Letzteres würde sprechen, dass eine Transaktion erst dann in einer Blockchain als gültig gilt, wenn sie gemäss Konsensprotokoll validiert ist.[510] Jedoch haben die Parteien keinen Einfluss auf den Validierungsmechanismus und die tatsächliche Willensäusserung des Akzeptanten wird mit der Signierung mit dem Private Key kundgetan. Daher erfolgt die Annahmeerklärung durch die Signierung mit dem Private Key. Dies ist gleichzeitig auch der Zeitpunkt des Vertragsschlusses, da die Signierung mit dem Private Key unmittelbar die automatisierte Ausführung auslöst.

---

508 Vgl. WEBER, E-Commerce, 345.

509 Vgl. WEBER, E-Commerce, N 345.

510 Aufgrund der unterschiedlichen Ausgestaltung der Konsensprotokolle ist die Validierung von Transaktionen bei jeder Blockchain-Plattform jeweils separat zu betrachten. Bei der Bitcoin- und (derzeit noch) Ethereum-Blockchain wird das PoW-Konzept verwendet (vgl. N 65 ff.). Hier gilt eine Transaktion dann als sicher, wenn sie min. sechs weitere Blöcke vor sich hat (vgl. N 69).

320 Vom Zeitpunkt des Vertragsschlusses ist der Beginn der Wirkung zu unterscheiden, der bei bedingten Verträgen (N 294) im Zeitpunkt der Erfüllung der Bedingung liegt (Art. 151 Abs. 1 OR), wobei die Parteien eine anderslautende Vereinbarung treffen können (Art. 151 Abs. 2 OR). Eine solche wird bei einer Suspensivbedingung insbesondere dann angenommen, wenn die Sache schon vor Eintritt der Bedingung übergeben wird.[511] Entsprechend fällt die Wirkung *ex tunc* mit dem Zeitpunkt des Vertragsschlusses zusammen.[512] Bei einer Resolutivbedingung wird das Rechtsgeschäft zu dem Zeitpunkt ungültig, zu dem die Bedingung eintritt (Art. 154 Abs. 1 OR). Eine Rückwirkung (der Unwirksamkeit) auf den Abschlusszeitpunkt findet in der Regel nicht statt (Art. 154 Abs. 2 OR).[513]

5. Zurechenbarkeit der Willenserklärung

321 Eine Willenserklärung muss jeweils einer Partei zurechenbar sein; diese Frage ist besonders im elektronischen Geschäftsverkehr von Bedeutung.

a) Allgemeine Regeln

322 Die Frage der Zurechenbarkeit einer Willenserklärung spielt bei den allgemeinen Prinzipien keine bedeutende Rolle, da die Regeln nicht in einer anonymen und virtuellen Umgebung entwickelt wurden. Die Zurechenbarkeit von Willenserklärungen spielen jedoch dort eine Rolle, wo eine andere Person als die Vertragspartei selbst beim Vertragsschluss involviert ist, wie bspw. beim Einsatz eines Boten oder eines Stellvertreters. Auf die allgemeinen

---

511 EHRAT/WIDMER, Art. 151 N 12; BERGER, Allgemeines Schuldrecht, N 817.

512 Berger, Allgemeines Schuldrecht, N 817; Erhard/Widmer, Art. 151 N 12.

513 D.h. Leistungen, die vor Eintritt der Bedingung erbracht wurden, sind nicht zurückzuerstatten; das Rechtsgeschäft wird durch den Nichteintritt der Bedingung zu einem unbedingten (vgl. EHRHARD/WIDMER, Art. 154 N 7; BERGER, Allgemeines Schuldrecht, N 822 f.; vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 4007.

Regeln zur Boten- und Stellvertreterfunktion wird an dieser Stelle aber nicht näher eingegangen (vgl. jedoch nachfolgend N 415, 426 f).

b) Im elektronischen Geschäftsverkehr

323 Bei elektronischen Willenserklärungen ist grundsätzlich zwischen denjenigen Erklärungen zu unterscheiden, die von einem Menschen mittels Computer abgegeben werden (z.B. durch einen Klick) und denjenigen, die automatisch durch ein Computerprogramm generiert werden.[514] Erstere können dem Absender direkt zugerechnet werden.[515] Die durch ein Computerprogramm generierten Erklärungen sind im Voraus festgelegt; im Gegensatz zur ersten Fallgruppe werden die Erklärungen jedoch nicht direkt durch menschliches Handeln ausgelöst; eine Maschine nimmt die rechtlich relevante Handlung vor.[516] Diese Handlung wird jedoch dem Betreiber der entsprechenden Datenverarbeitungsanlage zugerechnet.[517] Computererklärungen gelten daher grundsätzlich ebenfalls als Willenserklärungen.[518]

c) Bei Smart Contracts

324 Ein Smart Contract wird immer durch min. eine Partei initialisiert.[519] Dabei führt ein Smart Contract diejenigen Schritte aus, die vorprogrammiert wurden.

---

514 BALSCHEIT, Konsumvertragsrecht, 168; WEBER/JÖHRI, Vertragsschluss im Internet, 48.

515 BALSCHEIT, Konsumvertragsrecht, 168; WEBER/JÖHRI, Vertragsschluss im Internet, 48.

516 BALSCHEIT, Konsumvertragsrecht, 168; WEBER, E-Commerce, 340; WEBER/JÖHRI, Vertragsschluss im Internet, 49.

517 BALSCHEIT, Konsumvertragsrecht, 168 f.; WEBER, E-Commerce, 340. vgl. HOEREN, Internetrecht, N 737.

518 SCHMIDLIN, BK OR, Art. 27 N 22.

519 Dieser Grundsatz gilt auch für komplexe Smart-Contract-Gebilde. Wenn ein Smart Contract dazu programmiert wurde, selbst weitere Smart Contracts zu initiieren, dann ist diese „Handlung“ originär auf die Programmierung des ersten Smart Contract zurückzuführen. Es ist aufgrund der Transaktionshistorie eine Rückverfolgung zu der initiierenden Person möglich. Vgl. zur privatrechtlichen Einordnung eines

Diese „Handlungen“ können also wie bei jeder anderen Computererklärung denjenigen Parteien zugeordnet werden, denen die Initialisierung oder die dazugehörige Datenverarbeitungsanlage zugerechnet werden kann (vgl. N 323).[520]

325 Die Zurechenbarkeit eines Smart Contract zu einer Partei kann auch durch die Überprüfung der Transaktionen erfolgen: Wird an die Adresse des Smart Contract durch die Parteien bspw. ein Vermögenswert übertragen, ist diese Transaktion in der Blockchain (öffentlich, wenn es sich um eine öffentliche Blockchain handelt) registriert; mittels Signatur kann diese Transaktion einer Partei zugeordnet werden (vgl. N 28 ff., 56 ff.).[521]

6. Auslegung der Willenserklärung

326 Besteht bezüglich einer Willenserklärung eine Unklarheit, resp. besteht die Gefahr eines Dissenses, dann muss die Willenserklärung ausgelegt werden.

---

komplexen Smart-Contract Gebildes einer dezentralen autonomen Organisation, „The DAO“, GYR, DAO, N 17 ff.

520 A.A. FURRER, der dem Smart Contract eine Art Stellvertreterfunktion zukommen lässt, da bei den betroffenen Parteien bei Vertragsschluss noch kein konkreter, sich auf einzelne Handlungen des Smart Contract beziehender Wille bestehe; die Handlungen des Smart Contract würden einzig nach dem vorprogrammierten Algorithmus bestimmt. Daher komme dem Smart Contract auch keine Botenfunktion zu, da dieser einen bereits bestehenden Willen transportiere: FURRER, Smart Contracts, 108. Dieser Meinung ist insofern zu widersprechen, als es in der Natur eines bedingten Vertrages liegt, dass die Parteien die Wirksamkeit des Vertrages von einer ungewissen zukünftigen Tatsache abhängig machen (vgl. Art. 151 Abs. 1 OR). Der Wille wird bereits bei Vertragsschluss kundgetan und erstreckt sich auch auf das zukünftige, ungewisse Ereignis (vgl. BERGER, Allgemeines Schuldrecht, N 815).

521 Vgl. FURRER, Smart Contracts, 104.

a) Allgemeine Regeln

327 Sollte der Empfänger den Erklärenden nicht richtig verstanden und dessen Willen nicht erkannt haben, dann wird die Willenserklärung nach dem Vertrauensprinzip ausgelegt.[522] Dabei wird die Willenserklärung so ausgelegt, wie sie vom Empfänger nach Treu und Glauben verstanden werden durfte und musste; ermittelt wird folglich der objektive Sinn der Erklärung.[523] Bei der Auslegung wird auf den Wortlaut, den Zusammenhang sowie auf die Gesamtumstände abgestellt.[524]

b) Im elektronischen Geschäftsverkehr

328 Mangels spezieller Regelungen wird auch im elektronischen Verkehr ein unbewiesener wirklicher Wille nach dem Vertrauensprinzip ausgelegt (vgl. N 327).

c) Bei Smart Contracts

329 Für Verträge mit Smart Contracts gilt ebenfalls, dass bei Bedarf die Willenserklärungen nach dem Vertrauensprinzip ausgelegt werden müssen (vgl. N 327). Da ein Smart Contract als Software nur deterministische Handlungen vornehmen kann, bedürfen diese grundsätzlich keiner Auslegung.[525]

7. Fazit

330 Nutzen fachkundige Personen einen Smart Contract, dann kann dieser direkt den Vertrag darstellen. Es wird vermutet, dass bei Einsatz eines Smart Contract

---

522 BERGER, Allgemeines Schuldrecht, N 710; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 212; SCHWENZER, OR AT, N 29.02.

523 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 207, 211. BGE 138 III 659 E. 4.2.1 S. 666, 136 III 186 E. 3.2.1 S. 188, 135 III 259 E. 5.2 S. 302.

524 BGE 138 III 659 E. 4.2.1 S. 666.

525 Vgl. KAULARTZ, Gestaltung von Smart Contracts, 204.

sein Inhalt dem Willen der beiden fachkundigen Personen entspricht. Anders verhält es sich bei unkundigen Personen. Hier ist nicht zu vermuten, dass sich der Rechtsbindungswille auf den Smart Contract bezieht, da sich der Inhalt eines Smart Contract durch diese nicht in zumutbarer Weise eruieren lässt. Eine Berufung auf einen fehlenden Rechtsbindungswillen bei wissentlicher Nutzung einer nicht bekannten Technologie kann jedoch rechtsmissbräuchlich sein. Sind eine fachkundige und eine fachunkundige Partei involviert, so ist eine Einzelfallbetrachtung von Nöten. Handelt es sich nicht um einen Konsumentenvertrag und kann die fachunkundige Person in zumutbarer Weise Kenntnis des Inhalts des Smart Contract nehmen, dann kann in diesen Fällen der Smart Contract direkt den Vertrag darstellen.

331 Ein Smart Contract kann, je nach konkreter Ausgestaltung, ein konkretes Angebot oder auch eine invitatio ad offerendum enthalten. Stellt der Smart Contract ein Angebot unter Abwesenden dar, dann ist von praktischer Bedeutung, dass der Smart Contract zeitlich terminiert ist oder deaktiviert werden kann, sollte der Antragsteller nicht mehr gebunden sein wollen. Enthält ein Smart Contract ein Angebot für Konsumenten, dann stellt er selbst nie den Vertrag dar; es müssen diesbezüglich die Regelungen zu den einzelnen Konsumentenverträgen eingehalten werden.

332 Der Vertrag mittels Smart Contract kommt zu dem Zeitpunkt zustande, zu dem die akzeptierende Partei ihr Einverständnis mit der Signierung, resp. der Übertragung eines Wertes an den Smart Contract zum Ausdruck bringt, welcher durch die automatisierte Abwicklung unmittelbare Wirkung entfaltet. Durch diese Signierung ist die Willenserklärung jeweils einer Partei zurechenbar. Die Handlungen eines Smart Contract sind grundsätzlich der/den initialisierenden Partei(en) zuzurechnen. Da Smart Contracts deterministisch sind, bedarf es theoretisch keiner Auslegung der darin verankerten Willenserklärungen.

IV. Übereinstimmende Willenserklärung

Die Willenserklärungen der Partien müssen übereinstimmen, das heisst es muss Konsens bezüglich der wesentlichen Vertragsbestandteile bestehen. 333

1. Allgemeine Regeln

Ein Vertrag gilt dann als zustande gekommen, wenn sich die Parteien über die wesentlichen Vertragsbestandteile (*essentialia negotii*) geeinigt haben (Art. 2 Abs. 1 OR).[526] Der Konsens beschreibt den Zustand, der vorliegt, wenn die übereinstimmenden Willenserklärungen der Parteien ausgetauscht wurden.[527] 334

a) Natürlicher und normativer Konsens

Im Regelfall ist davon auszugehen, dass sich die Parteien richtig verstanden haben und die Erklärungen so gelten, wie die Parteien sie tatsächlich (übereinstimmend) verstanden haben. In diesem Fall liegt ein natürlicher Konsens vor.[528] Davon zu unterscheiden sind diejenigen Fälle, in denen mindestens eine der Parteien die andere nicht richtig verstanden hat. In diesen Fällen wird die Erklärung nach dem Vertrauensprinzip eruiert, d.h. die Erklärung wird so, wie sie vom Empfänger nach Treu und Glauben verstanden werden durfte, ausgelegt.[529] Der durch das Vertrauensprinzip ermittelte Konsens wird *rechtlicher* oder *normativer Konsens* genannt.[530] 335

---

526 SCHWENZER, OR AT, N 6.02; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 1 N20.

527 BERGER, Allgemeines Schuldrecht, N 691; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 309; vgl. SCHWENZER, OR AT, N 6.02.

528 BERGER, Allgemeines Schuldrecht, N 694; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 310 ff.; SCHWENZER, OR AT, N 29.02.

529 BERGER, Allgemeines Schuldrecht, N 710; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 316; SCHWENZER, OR AT, N 29.02.

530 BERGER, Allgemeines Schuldrecht, N 697; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 317; SCHWENZER, OR AT, N 29.02.

b) Dissens

336 Dissens liegt vor, wenn sich die Parteien nicht über die wesentlichen Vertragsbestandteile geeinigt haben – der Vertrag kommt in diesen Fällen nicht zustande.[531] Davon ist zu unterscheiden, wenn die Erklärungen der Parteien nicht übereinstimmen, diese sich jedoch dieser Nichtübereinstimmung bewusst sind, weil sie sich tatsächlich richtig verstanden haben (offener Dissens) oder sie sich dieser Nichtübereinstimmung nicht bewusst sind (versteckter Dissens).[532] Bei einem versteckten Dissens fragt sich, ob mittels Auslegung gemäss Vertrauensprinzip nicht ein normativer Konsens bestehen kann.[533]

c) Wesentliche Vertragsbestandteile

337 Der Konsens muss sich auf die wesentlichen Vertragsbestandteile beziehen. Über die Merkmale der wesentlichen Vertragsbestandteile schweigt Art. 2 Abs. 1 OR. Es finden sich jedoch in den jeweiligen Bestimmungen der gesetzlich geregelten Vertragstypen Hinweise zu den wesentlichen Vertragsbestandteilen.[534] Es können daher keine allgemeingültigen Aussagen über den inhaltlich notwendigen Konsens gemacht werden, da diesbezüglich eine Einzelfallbetrachtung erforderlich ist.[535] Liegt ein Dissens vor und bezieht sich dieser auf die wesentlichen Vertragsbestandteile, dann kommt der Vertrag nicht zustande.[536]

338 Es ist zwischen objektiv und subjektiv wesentlichen Vertragspunkten zu unterscheiden. Die objektiv wesentlichen Vertragsbestanteile umfassen den *„unentbehrlichen Geschäftskern“* (d.h. die vertragstypenbestimmenden

---

531 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 326; SCHWENZER, OR AT, N 29.07.

532 BERGER, Allgemeines Schuldrecht, N 721, 723; GAUCH/SCHLUEP/SCHMID/ EMMENEGGER, OR AT, N 327; SCHWENZER, OR AT, N 29.08.

533 BERGER, Allgemeines Schuldrecht, N 726; GAUCH/SCHLUEP/SCHMID/ EMMENEGGER, OR AT, N 328.

534 ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 1 N23.

535 Vgl. ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 1 N 23.

536 BERGER, Allgemeines Schuldrecht, N 721; GAUCH/SCHLUEP/SCHMID/ EMMENEGGER, OR AT, N 328; SCHWENZER, OR AT, N 29.09.

Merkmale des Vertrages), die Parteien sowie die jeweilige Leistung und Gegenleistung.[537] Die subjektiv wesentlichen Vertragspunkte sind zumindest für eine Partei unabdingbare Voraussetzung (*conditio sine qua non*) für den Vertragsschluss.[538]

2. Konsens im elektronischen Geschäftsverkehr

339 Im elektronischen Geschäftsverkehr gelten ebenfalls die allgemeinen Regeln bezgl. Konsens und Dissens. Hier liegt in der Regel eine Verschriftlichung von Angebot und Annahme vor, was bei der Eruierung des Konsenses hilfreich ist. Sollte bei der Übermittlung der Willenserklärung ein Fehler (Bedienungs- oder Eingabefehler, Übermittlungsfehler etc.) unterlaufen, dann liegt allenfalls ein Dissens vor (zur Anfechtung mangelhafter Willenserklärungen siehe nachfolgend N 412 ff.).

3. Konsens bei Smart Contracts

340 Auch bezüglich Smart Contracts muss ein übereinstimmender Konsens bzgl. der wesentlichen Vertragsbestandteile vorliegen (vgl. N 337 f.)

537 BERGER, Allgemeines Schuldrecht, N 639; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 333; SCHWENZER, OR AT, N 29.03.

538 BERGER, Allgemeines Schuldrecht, N 641; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 341; SCHWENZER, OR AT, N 29.03.

V. Widerruf

341 Angebot und Annahme können unter gewissen Umständen widerrufen werden. Die Geschwindigkeit der Übertragung von Willensäusserungen im elektronischen Geschäftsverkehr erschwert die Widerrufsmöglichkeit allerdings.

1. Allgemeine Regeln

342 Grundsätzlich sind Antrag und Annahme unwiderruflich.[539] Ausgenommen davon sind die Ausnahmentatbestände von Art. 9 OR, das Widerrufsrecht bei Konsumentenverträgen (N 343) sowie ein Widerrufsvorbehalt. In letzterem Fall kann der Antrag oder die Annahme gültig widerrufen werden, wenn der Widerruf vor oder mit der (ersten) Erklärung beim Empfänger eintrifft oder wenn er später als die Erklärung beim Empfänger eintrifft, er aber vor der widerrufenen Erklärung dem Empfänger zur Kenntnis gebracht wird.[540] Zu beachten ist, dass gemäss neuerer Lehre ein verspäteter Widerruf trotzdem seine Wirkung entfaltet, wenn der Empfänger des Widerrufs diesen zwar später als die Ersterklärung zur Kenntnis nimmt, ihn aber unbeantwortet lässt (Anwendung von Art. 5 Abs. 3 OR).[541]

343 Nach Art. 40b OR gilt ein Widerrufsrecht für Kunden, wenn ihnen ein Angebot am Arbeitsplatz, in Wohnräumen oder deren unmittelbarer Umgebung (lit. a), in öffentlichen Verkehrsmitteln oder auf öffentlichen Strassen und Plätzen (lit. b), an Werbeveranstaltungen, die mit einer Ausflugsfahrt o.ä. verbunden sind (lit. c) oder am Telefon oder über vergleichbare Mittel der gleichzeitigen

---

539 BERGER, Allgemeines Schuldrecht, N 649; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 468; SCHWENZER, OR AT, N 28.15.

540 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 471 ff.; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 10 N 10 f.; vgl. SCHWENZER, OR AT, N 28.27.

541 BERGER, Allgemeines Schuldrecht, N 689; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 474; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 9 N 13.

mündlichen Telekommunikation (lit. d) unterbreitet wurden. Dabei muss es sich um Verträge über bewegliche Sachen und Dienstleistungen handeln, die für den persönlichen oder familiären Gebrauch des Verbrauchers bestimmt sind (= Konsumentenverträge, Art. 40a Abs. 1 OR).[542] Darunter fallen beispielsweise Verträge über Wertpapiere, Werkverträge, Heiratsvermittlung oder Kreditvermittlungsverträge.[543] Ausnahmen vom Grundsatz des Widerrufsrechts bei Haustürgeschäften und ähnlichen Verträgen sind einerseits eine Leistung von unter CHF 100 des Konsumenten und andererseits Versicherungsverträge, die gänzlich ausgeschlossen sind (Art. 40a Abs. 1 lit. b und Abs. 2 OR).[544] Das Widerrufsrecht entfällt auch, wenn der Kunde die Vertragsverhandlungen ausdrücklich gewünscht hat oder er seine Erklärung an einem Markt- oder Messestand abgegeben hat (Art. 40c OR).[545] Nicht vom Widerrufsrecht gedeckt sind überdies Verträge, die auf dem schriftlichen Weg unterbreitet wurden, da in solchen Fällen das Überrumplungspotential bei einem persönlichen Kontakt fehlt.[546] Das Widerrufsrecht bei Konsumentenverträgen ist für Internetgeschäfte nicht anwendbar (das Parlament hat bei dem per 1. Januar 2016 angepassten Widerrufsrecht auf eine Regelung von Internetgeschäften verzichtet).[547]

---

542 KOLLER-TUMLER, BSK OR I, Art. 40a N 2; SCHWENZER, OR AT, N 28.65.

543 KOLLER-TUMLER, BSK OR I, Art. 40a N 2 mit weiteren Beispielen.

544 KOLLER-TUMLER, BSK OR I, Art. 40a N 5 f.; SCHWENZER, OR AT, N 28.65 f.
Mit Inkrafttreten am 1. Januar 2020 des Bundesgesetzes über Finanzdienstleistungen (Finanzdienstleistungs-gesetz, FIDLEG) vom 15. Juni 2018 (BBL 2018, 3615-3656) wird Art. 40a Abs. 2 OR dahingehend ergänzt, dass auch Verträge über Finanzdienstleistungen ausgenommen werden (vgl. FIDLEG, Anhang Änderung anderer Erlasse, 35).

545 KOLLER-TUMLER, BSK OR I, Art. 40c N 2 ff.; SCHWENZER, OR AT, N 28.68 f.

546 KOLLER-TUMLER, BSK OR I, Art. 40b N 9; vgl. SCHWENZER, OR AT, N 28.67.

547 KOLLER-TUMLER, BSK OR I, Art. 40b N 8; WEBER, E-Commerce, 32; vgl. BOTSCHAFT ZertES, BBl 2014 921, 2999.

2. Widerruf im elektronischen Geschäftsverkehr

344 Da der Widerruf vor oder gleichzeitig mit der vorgehenden Erklärung beim Empfänger eingehen muss (vgl. vorstehend N 342), stellt dieser beim elektronischen Geschäftsverkehr eine besondere Herausforderung dar, weil dies technisch kaum möglich ist.[548] Es besteht jedoch immerhin die Möglichkeit, dass der Widerruf vom Empfänger vor der (ersten) Erklärung wahrgenommen wird und er so seine Wirkung entfaltet. Laut SCHWENZER kommt es im elektronischen Geschäftsverkehr nicht auf den zeitlichen Eingang von Widerruf und Erklärung an, sondern vielmehr auf die Gleichzeitigkeit der Kenntnisnahme.[549]

3. Widerruf bei Smart Contracts

345 Der Smart Contract führt aus, was vorgängig programmiert wurde. Die Möglichkeit des Widerrufs ist in der Konzeption eines Smart Contract nicht vorgesehen. Ist ein Smart Contract auf einer öffentlichen Blockchain direkt abgespeichert, dann ist er grundsätzlich unwiderruflich (vgl. N 250 ff.). Eine Widerrufsmöglichkeit ist demgemäss nur bei einem Smart Contract umsetzbar, der in einem virtuellen Container ausserhalb der Blockchain abgespeichert ist. Ist eine Widerrufsmöglichkeit vorgesehen, müsste dies jedoch zur Anwendung gelangen, bevor das Vorprogrammierte ausgeführt wird. Wurde eine solche Funktion vorgesehen, dann kommen die allgemeinen Regeln sowie diejenigen für den elektronischen Geschäftsverkehr zur Anwendung (vgl. hiervor N 342 f., 344).

346 Wird ein Smart Contract im Zusammenhang mit Konsumentenverträgen eingesetzt, ist fraglich, ob auch hier das speziell geregelte Widerrufsrecht gem. Art. 40a ff. OR gilt. Das Widerrufsrecht gilt nicht für Verträge, die auf schriftlichem Weg geschlossen wurden und auch nicht für Internetverträge (vgl. hiervor N 343). Elektronische Vertragsschlüsse sind in der Regel schriftlich und fallen daher nicht unter das Widerrufsrecht von

---

548 BALSCHEIT, Konsumvertragsrecht, 175; WEBER, E-Commerce, 344.

549 SCHWENZER, OR AT, N 27.25.

Haustürgeschäften gem. Art. 40a ff. OR. Sofern ein Smart Contract einen Konsumentenvertrag betrifft, muss eine Umschreibung in einer natürlichen Sprache vorliegen; der Smart Contract kann in diesen Fällen nicht den Vertrag darstellen (vgl. N 305 ff.).[550]

[550] Ob die Begründung, dass nur bei mündlich vorgetragenen Angeboten ein Überraschungsmoment vorhanden sei zutrifft, kann hier offengelassen werden. Dies ist eine politische Frage, deren Beantwortung durch das Schweizer Parlament vorgenommen werden muss. Zur rechtspolitischen Ausgangslage in der Schweiz und der EU vgl. BALSCHEIT, Konsumvertragsrecht, 36 ff.; KRAMER/PROBST/PERRIG, AGB, N 1 ff., 25 ff.

VI. Inhalt des Vertrages

347 Grundsätzlich besteht im Schweizer Vertragsrecht das Prinzip der Inhaltsfreiheit. Trotzdem bestehen gewisse Inhaltsschranken, deren Nichtbeachtung die Nichtigkeit des Vertrages nach sich zieht.

1. Grundsatz der Inhaltsfreiheit

348 Ein zentraler Aspekt der Vertragsfreiheit[551] ist die explizit in Art. 19 Abs. 1 OR verankerte Inhaltsfreiheit.[552] Eingeschränkt wird die Inhaltsfreiheit durch „die Schranken des Gesetzes“ (Art. 19 Abs. 1 OR). Das Gesetz selbst nennt die für die Inhaltskontrolle geltenden Kriterien; es sind einerseits die in Art. 19 Abs. 2 OR verankerten zwingenden Gesetzesvorschriften, die öffentliche Ordnung, die guten Sitten und das Persönlichkeitsrecht und andererseits die in Art. 20 Abs. 1 OR aufgezählten Kriterien der Leistungsunmöglichkeit, der Widerrechtlichkeit sowie der Sittenwidrigkeit.

2. Inhaltsschranken

349 Die gesetzlich vorgesehenen Inhaltsschranken des widerrechtlichen, unmöglichen, oder sittenwidrigen Inhalts können sich teilweise überschneiden. Sie können in drei Gruppen zusammengefasst werden: Sittenwidrigkeit (schliesst Persönlichkeitsverletzung mit ein), Leistungsunmöglichkeit sowie Widerrechtlichkeit (schliesst die Verletzung der öffentlichen Ordnung ein).[553]

---

551 Die Vertragsfreiheit umfasst mehrere Aspekte, darunter die Abschlussfreiheit, Partnerwahlfreiheit, Aufhebungsfreiheit, Formfreiheit und die Inhaltsfreiheit, vgl. BERGER, Allgemeines Schuldrecht, N 167 ff.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 613 ff.

552 BERGER, Allgemeines Schuldrecht, N 170; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 618; SCHWENZER, OR AT, N 32.01.

553 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 629; HUGUENIN/MEISE, BSK OR I, Art.19/20 OR N 13; SCHWENZER, OR AT, N 32.04.

a) Sittenwidrigkeit

350 Die Sittenwidrigkeit stellt eine Generalklausel dar; sie widerspiegelt die „herrschende Moral".[554] Die guten Sitten sind als Spiegel der gesellschaftlichen Wertvorstellungen einem Wandel unterworfen, doch können sie auch die Prinzipien der Rechtsordnung selbst (z.B. Grundrechte) widerspiegeln.[555] Dem Gericht kommt bei der Beurteilung der Sittenwidrigkeit ein grosser Ermessenspielraum zu.[556]

b) Unmöglichkeit

351 Unmöglichkeit liegt dann vor, wenn die versprochene Leistung objektiv nicht erbringbar ist.[557]

c) Widerrechtlichkeit

352 Ein Vertragsinhalt ist dann widerrechtlich, wenn er gegen eine objektive Norm des Schweizer Rechts verstösst; die Widerrechtlichkeit kann den Inhalt oder aber den Vertragsabschluss (mit entsprechendem Inhalt) selbst betreffen.[558] Die Widerrechtlichkeit kann sich also direkt aus einer (zwingenden) Norm des Privatrechts oder des öffentlichen Rechts ergeben.[559]

---

554 BGE 136 III 474 E.3, 132 III 458.

555 Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 668.

556 Ausführlich und mit Beispielen GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 669 ff.

557 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 631; HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 46; SCHWENZER, OR AT, N 32.34, 63.02.

558 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 639 ff.; HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 17; SCHWENZER, OR AT, N 32.06.

559 Ausführlich und mit Beispielen GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 646 ff.

3. Inhaltsschranken im elektronischen Geschäftsverkehr und bei Smart Contracts

353 Wie bei herkömmlichen Verträgen gelten auch im elektronischen Geschäftsverkehr und für Smart Contracts die Inhaltsschranken gem. Art. 19 Abs. 1 OR.[560]

4. Rechtsfolgen

354 Die Rechtsfolge eines Vertrages mit unerlaubtem Inhalt ist die Nichtigkeit oder Teilnichtigkeit des Vertrages.

a) Nichtigkeit

355 Verstösst ein Vertrag gegen die Inhaltsschranken des OR, d.h. hat er einen unmöglichen oder widerrechtlichen Inhalt oder verstösst er gegen die guten Sitten, ist er nichtig (Art. 20 Abs. 1 OR). Nichtigkeit ist im Gesetz nicht definiert. Negativ umschrieben bedeutet Nichtigkeit, dass keine Vertragswirkung eintritt.[561] Nach herrschender Lehre ist der Vertrag ex tunc unwirksam; allfällige Leistungen aus dem nichtigen Vertrag erfolgen daher ohne gültigen Rechtsgrund.[562] Die Nichtigkeit kann demgemäss von jedermann geltend gemacht werden und das Gericht hat die Nichtigkeit von Amtes wegen

---

560 Wie auch bei konventionellen Verträgen sind die Schwierigkeiten bezgl. Inhaltsschranken eher praktischer Natur: Sie müssen erst geltend gemacht werden, resp. eine Partei muss einen Anspruch daraus ableiten und ein Gericht muss über das Vorliegen eines solchen Vertragsinhalts befinden.

561 BGer Urteil 4C.163/2002 vom 9. Juli 2003 E. 1.3; BGE 134 III 438 E. 2.3 S. 442 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 681.

562 BERGER, Allgemeines Schuldrecht, N 1103; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 681; HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 53; SCHWENZER, OR AT, N 32.35; BGE 134 III 438 E. 2.3 S. 442 f.

zu beachten, sofern sich aus dem Parteivortrag ein Nichtigkeitsgrund ergibt.[563] Wurde bereits geleistet, dann besteht nach Massgabe der unter den gegebenen Voraussetzungen anzuwendenden Bestimmungen die Möglichkeit einer Vindikation (Art. 641 Abs. 2 ZGB) oder es besteht ein Anspruch aus ungerechtfertigter Bereicherung (Art. 62 ff. OR), wobei die Vindikation den Anspruch aus ungerechtfertigter Bereicherung verdrängt.[564] In Betracht kommt allenfalls auch eine Grundbuchberichtigungsklage (Art. 975 ZGB).[565]

356 Das Rückforderungsrecht bei Nichtigkeit ist gewissen Einschränkungen unterworfen. Zu beachten ist Art. 66 OR, in dessen Rahmen bei unsittlichen oder widerrechtlichen Verträgen eine Rückforderung aus Bereicherungsrecht (unklar jedoch beim Vindikationsanspruch) ausgeschlossen ist.[566]

357 Verstösst ein Vertrag gegen eine Norm des öffentlichen Rechts, dann ist der Vertrag nur dann nichtig, wenn dies in der entsprechenden Norm vorgesehen ist.[567] Nicht unumstritten ist, was bei Verträgen nach Art. 27 Abs. 2 ZGB (Schutz der Persönlichkeit vor übermässiger Bindung) passiert. Das Bundesgericht und ein Teil der Lehre gehen davon aus, dass die Nichtigkeitsfolge von Art. 20 OR nicht anzuwenden sei, um den von Art. 27 ZGB Geschützten vor einer Berufung auf die Nichtigkeit durch die Gegenpartei zu bewahren.[568] Die h.L. subsumiert die Persönlichkeitsverletzung aus Art. 27 Abs. 2 ZGB jedoch ebenfalls unter Art. 20 OR mit der daraus resultierenden Nichtigkeitsfolge.[569]

---

563 BUCHER, OR AT, 241 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 681; HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 53; KRAMER, BK OR, Art. 19-20 N 308 ff.

564 BERGER, Allgemeines Schuldrecht, N 1103, 1120; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 681.

565 Vgl. SCHMID, BSK ZGB II, Art. 975 N 1 ff.

566 Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 683, 1553; SCHULIN, BSK OR I, Art. 66 N 6 ff; SCHWENZER, OR AT, .

567 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 684.

568 BGE 129 III 209 E. 2.2 S. 213 f.; SCHWENZER, OR AT, N 32.21.

569 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 685; HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 43; vgl. KRAMER, BK OR, Art. 19 N 370 ff.

358 In der Lehre wird teilweise von einem flexiblen Nichtigkeitsbegriff gesprochen, als Alternative zu dem Modell des traditionellen Nichtigkeitsbegriffes in Art. 20 OR und dessen Konsequenzen (abweichende Formen der Nichtigkeit werden aus dem Anwendungsbereich von Art. 20 OR ausgeklammert oder als Einschränkung des restriktiven Nichtigkeitsbegriffes verstanden).[570] Sinn des flexiblen Nichtigkeitsbegriffes sei es, nicht generell festzulegen, wie die Nichtigkeit wirken soll oder wer sich auf sie berufen darf, um dem Ziel von Art. 20 OR – der Beseitigung des dem Vertrag anhaftenden Mangels und nicht generell der Sanktion des Dahinfallens des Vertrages – nicht im Wege zu stehen.[571]

b) Teilnichtigkeit

359 Betrifft der unmögliche, widerrechtliche oder sittenwidrige Inhalt nur einzelne Teile des Vertrages, dann gilt als Grundregel, dass nur die vom Mangel betroffenen Teile nichtig sind, sofern der Vertrag nicht ohne diese Teile des Vertrages geschlossen worden wäre (Art. 20 Abs. 2 OR).[572] Dies setzt voraus, dass der Vertrag teilbar ist, d.h. der nicht vom Mangel betroffene Rest als eigenständiger Vertrag Bestand hat (d.h. obj. wesentliche Vertragspunkte sind nicht betroffen).[573] Bei der Beurteilung der subjektiven Vertragsvoraussetzungen kommt es auf den hypothetischen Parteiwillen an, d.h. es wird darauf abgestellt, was die Parteien als nach Treu und Glauben handelnde Vertragspartner vereinbart hätten.[574] Der Vertrag kann dann entweder ohne die mangelhaften Teile weiterbestehen (schlichte Teilnichtigkeit), mit einer neuen Regel ergänzt werden (modifizierte

---

570 HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 55.

571 HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 55.

572 BERGER, Allgemeines Schuldrecht, N 1107; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 693; vgl. HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 61.

573 BERGER, Allgemeines Schuldrecht, N 1108; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 694; SCHWENZER, OR AT, N 32.40.

574 BERGER, Allgemeines Schuldrecht, N 1108; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 700.

Teilnichtigkeit) oder bei einer übermässigen Bindung auf das erlaubte Mass reduziert werden (geltungserhaltende Reduktion).[575]

c) Nichtigkeit und Teilnichtigkeit im elektronischen Geschäftsverkehr

360 Die Rechtsfolgen eines inhaltswidrigen Vertrages sind beim elektronischen Rechtsverkehr die gleichen wie im klassischen Vertragsrecht (N 355 ff.).

d) Nichtigkeit und Teilnichtigkeit bei Smart Contracts

361 Die obenstehend ausgeführten allgemeinen Grundsätze (N 355 ff.) gelten auch für allfällige Verträge mit rechtswidrigem Inhalt in Gestalt eines Smart Contract.

362 Hier kommen jedoch erschwerende Elemente hinzu: Wenn der Smart Contract direkt auf der Blockchain gespeichert ist, dann ist der Smart Contract selbst als auch das Ergebnis (Transaktion) des Smart Contract grundsätzlich unwiderruflich und unabänderlich abgespeichert (vgl. N 249 ff.). Die Nichtigkeit eines Smart Contract oder einer Transaktion kann nicht festgehalten werden. Allenfalls wenn der Smart Contract in einem virtuellen Container ausserhalb der Blockchain gespeichert ist und das Ergebnis noch nicht in der Blockchain abgelegt wurde, könnte die Nichtigkeit eines Smart Contract erwirkt werden, indem der Smart Contract gelöscht wird – sofern er noch nicht ausgeführt wurde. In einem geschlossenen System könnte zwar theoretisch vorgesehen werden, dass eine Transaktion im Nachhinein als ungültig markiert werden kann, dies würde jedoch eine hohe Rechtsunsicherheit des gesamten Systems verursachen und die Grundkonzeption der Blockchain-Technologie ad absurdum führen.

363 Faktisch kann also ein als nichtig deklarierter Vertrag in einer Blockchain nicht entsprechend markiert werden, wenn er direkt auf der Blockchain abgespeichert wurde oder das Ergebnis, die Transaktion, bereits in die Blockchain aufgenommen wurde. In dieser Hinsicht hebelt die Technologie

575 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 703 ff.; HUGUENIN/MEISE, BSK OR I, Art. 19/20 N 64 ff.; SCHWENZER, OR AT, N 32.41 ff.

das Recht aus. Dies ändert jedoch nichts an der Tatsache, dass der Vertrag nichtig ist.

VII. Formvorschriften

364 Es gilt der Grundsatz der Formfreiheit (Art. 11 OR), wobei jedoch für einzelne Vertragsverhältnisse gesetzliche Formvorschriften vorgesehen sind. Zweck der Formvorschriften ist der Schutz der Parteien vor Übereilung, die Sicherheit im Rechtsverkehr sowie die Schaffung klarer Verhältnisse.[576] Es bestehen im Schweizer Recht folgende Arten von Formvorschriften: die einfache und qualifizierte Schriftlichkeit sowie die öffentliche Beurkundung. Die Folge der Nichteinhaltung der Formvorschriften ist die Nichtigkeit des Vertrages (Art. 11 Abs. 2 OR). Für den digitalen Rechtsverkehr ist insbesondere die einfache Schriftlichkeit von Bedeutung, da seit Einführung der qualifizierten elektronischen Unterschrift die einfache Schriftlichkeit auch digital gewährleistet werden kann.

1. Grundsatz der Formfreiheit

365 Der Grundsatz der Formfreiheit ist in Art. 11 Abs. 1 OR verankert.[577] Das heisst, Verträge dürfen grundsätzlich formfrei abgeschlossen werden und entfalten Rechtswirkung.[578] Formfreiheit bedeutet aber auch, dass eine strengere Form vertraglich vereinbart werden kann (Art. 16 Abs. 1 OR).[579] Für

576 BERGER, Allgemeines Schuldrecht, N 746; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 497 ff.; SCHWENZER, BSK OR I, Art. 11 N 2; SCHWENZER, OR AT, N 31.02.

577 BERGER, Allgemeines Schuldrecht, N 743; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 490 ff.; HUGUENIN, OR, N 337; SCHWENZER, OR AT, N 31.01.

578 BERGER, Allgemeines Schuldrecht, N 743; SCHWENZER, BSK OR I, Art. 11 N 1; ZELLWEGER-GUTKNECHT/BUCHER, BSK OR I, Art. 1 N 33.

579 BERGER, Allgemeines Schuldrecht, N 778; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 490 ff.; SCHWENZER, BSK OR I, Art. 16 N 1.

Rechtsgeschäfte von Todes wegen (z.B. letztwillige Verfügung) ist immer eine besondere Form vorgesehen; der Grundsatz der Formfreiheit bezieht sich daher ausschliesslich auf Rechtsgeschäfte unter Lebenden.[580] Ausgenommen vom Grundsatz der Formfreiheit sind ebenfalls Verträge, für die ein Bundesgesetz explizit eine Formvorschrift vorsieht; so ist bspw. der Kaufvertrag über ein Grundstück nur gültig, wenn er öffentlich beurkundet ist (Art. 216 OR).

366 Die Formfreiheit gilt auch für den elektronischen Rechtsverkehr und folglich auch für Vertragsschlüsse mit Smart Contracts.[581]

2. Einfache Schriftlichkeit

367 Die einfache Schriftlichkeit verlangt die Unterschrift sämtlicher Vertragsparteien (Art. 13 OR). Der Begriff *Schriftlichkeit* ist im Gesetz selbst nicht definiert. Nach Lehre und Rechtsprechung umfasst die Schriftlichkeit einen Erklärungsinhalt in Schriftzeichen (Schriftform), der auf einem Erklärungsträger aufgezeichnet und dauerhaft festgehalten wird.[582] Einfache Schriftlichkeit wird beispielsweise für den Abtretungsvertrag (Zession) gem. Art. 165 Abs. 1 OR verlangt. Nachfolgend werden die einzelnen Elemente der einfachen Schriftlichkeit erörtert, wobei insbesondere auf die digitale Ausgestaltung der einzelnen Elemente eingegangen wird. Dabei wird auch die neuere Lehre zu der in der Zivilprozessordnung und im Internationalen Privatrechtsgesetz (IPRG)[583] verankerten Textform miteinbezogen.

---

580 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 495.

581 Zu den übrigen Voraussetzungen zum gültigen Abschluss eines Vertrages siehe vorangegangene Ausführungen, Kapitel E., N 266 ff.

582 BGE 120 V 74 E.3a S. 77; vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 504; vgl. KRAMER/SCHMIDLIN, BK OR, Allg. Erläuterungen zu Art.12-15, N 3; SCHWENZER, OR AT, N 31.06.

583 Bundesgesetz über das Internationale Privatrecht (IPRG) vom 18. Dezember 1987, SR 291.

a) Erklärungsinhalt in Schriftzeichen

368 In der Lehre wird das Schriftlichkeitserfordernis immer mit der Unterschriftsfrage verbunden, was sich direkt aus dem Wortlaut von Art. 13 OR ergibt.[584] Demnach genügten Brief und Telegramm dem Schriftlichkeitserfordernis, wenn der Brief oder die Aufgabendepesche die Unterschrift des Absenders trug.[585] Dies alleine sagt jedoch noch nichts über den Erklärungsinhalt in Schriftzeichen aus.

369 Einigkeit herrscht in der Lehre darüber, dass die Schrifttechnik und das verwendete Schreibgerät unbeachtlich sind, sofern eine dauerhafte Verkörperung gewährleistet ist.[586] Der Erklärungsinhalt muss also auf dem Erklärungsträger dauerhaft festgehalten werden können.[587] Die Dauerhaftigkeit bezieht sich jedoch auf den geeigneten Erklärungsträger (vgl. nachfolgend N 376 ff.) und weniger auf den Erklärungsinhalt in Schriftzeichen.

370 Die für den Erklärungsinhalt verwendete Schrift und Sprache müssen laut KRAMER/SCHMIDLIN mindestens für diejenigen Personen verständlich sein, die durch die Formvorschrift geschützt werden sollen; sind Drittinteressen betroffen, muss der Schrifttext allgemein zugänglich sein und Geheimsprachen oder -schriften sind nicht ausreichend, um dem Schriftzeichenerfordernis zu genügen.[588] Als Schriftzeichen anerkannt sind auch die Blindenschrift, Kurzschrift oder Maschinenschrift.[589] Nach älterer Lehrmeinung genügte bspw. ein Magnetband oder ein Lochstreifen dem Schriftlichkeitserfordernis

---

584 Art. 13 OR: "Ein Vertrag, für den die schriftliche Form gesetzlich vorgeschrieben ist, muss die Unterschrift aller Personen tragen, die durch ihn verpflichtet werden sollen."

585 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 507.

586 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 509; HUGUENIN, OR, N 349; SCHWENZER, BSK OR I, Art. 13 N 4; vgl. KRAMER/SCHMIDLIN, BK OR, Allg. Erläuterungen zu Art.12-15 N 5;
Gleiches gilt für das Schrifterfordernis im Urkundenstrafrecht: BOOG, BSK StGB I, Art. 110 Abs. 4 N 10.

587 SCHWENZER, OR AT, N 31.06.

588 KRAMER/SCHMIDLIN, BK OR, Allg. Erläuterungen zu Art.12-15 N 5.

589 BUCHER, OR AT, 164.

nicht, da einerseits bei diesen Trägern keine Unterschrift gesetzt und andererseits die Erklärung nur mit technischen Hilfsmitteln gelesen werden könne.[590]

371 Die ZPO und das IPRG kennen im Gegensatz zum OR die sog. Textform.[591] Diese ist weniger streng als die einfache Schriftlichkeit ausgestaltet, da keine Unterschrift erforderlich ist.[592] Voraussetzung für die Textform ist ein schriftlicher Ausdruck, der einen dauerhaften Nachweis der Erklärung ermöglicht.[593] Der Text muss visuell wahrnehmbar und körperlich reproduzierbar sein; auf einzelne Technologien kommt es nicht an.[594] In diesem Sinne genügen Voice-Mails oder Videokonferenzen dem Texterfordernis nicht, da der Absender keinen Text versendet (dieser aber dem Empfänger dank Spracherkennung als Text vorliegen kann).[595] Dies ist in Übereinstimmung mit der herrschenden Lehre, die Tonaufnahmen dem Schrifterfordernis nicht genügen lässt.[596]

372 Ergänzt man die Textform mit einer Unterschrift, lässt sich kein Unterschied zur einfachen Schriftlichkeit erkennen. Es bietet sich daher an, die Lehre zur neueren Textform für die Auslegung der Erfordernisse des Erklärungsinhalts in Schriftzeichen heranzuziehen. So ist das Erfordernis der visuellen

---

590 BUCHER, OR AT, 164; KRAMER/SCHMIDLIN, BK OR, Allg. Erläuterungen zu Art. 12-15 N 4.
Weniger streng bezüglich technischen Hilfsmittel ist das Strafrecht für den Urkundenbegriff in Art. 110 Abs. 4 StGB, siehe BOOG, BSK StGB I, Art. 110 Abs. 4 N 10.

591 Art. 178 IPRG (Schiedsvereinbarung), Art. 17 ZPO (Gerichtsstandsvereinbarung) und Art. 358 ZPO (Schiedsvereinbarung).

592 GIRSBERGER, BSK ZPO, Art. 358 N 10; GRÄNICHER, BSK IPRG, Art. 178 N 11.

593 HUGUENIN, OR, N 347.

594 GIRSBERGER, BSK ZPO, Art. 358 N 7; GRÄNICHER, BSK IPRG, Art. 178 N 11.

595 DASSER, KUKO ZPO, Art. 358 N 2; GRÄNICHER, BSK IPRG, Art. 178 N 13.

596 HUGUENIN, OR, N 349; KRAMER/SCHMIDLIN, BK OR, Allg. Erläuterungen zu Art. 12-15 N 4.

Wahrnehmbarkeit bei der Beurteilung des Erklärungsinhaltes in Schriftzeichen ebenfalls miteinzubeziehen. Es ist einerseits ein technologieneutrales Merkmal und andererseits entspricht es dem unbestrittenen Grundsatz, dass es auf die Art der Sprache, Schrifttechnik und des Schreibgerätes nicht ankommt (vgl. vorgehend N 369).

aa) Erklärungsinhalt in Schriftzeichen im elektronischen Geschäftsverkehr

373 E-Mails, Webformulare oder andere digitale Schriftstücke, wie sie im elektronischen Geschäftsverkehr eingesetzt werden, sind in der Regel in einer der Allgemeinheit zugänglichen Sprache und Schrift gefertigt; sie sind visuell wahrnehmbar. Die visuelle Wahrnehmbarkeit wird durch technische Hilfsmittel hergestellt, was zwar gemäss älterer Lehrmeinung dem Schriftlichkeitserfordernis nicht zu genügen vermag (vgl. N 370). Diese Meinung ist aufgrund der wirtschaftlichen Realität des elektronischen Geschäftsverkehrs und der heute eingesetzten technologischen Hilfsmittel im Alltag aber nicht mehr sachgerecht. Die Sichtbarmachung von Informationen (Daten aller Art) durch technische Hilfsmittel ist heute im Geschäftsalltag wie auch im Privatleben Standard. Die digitale Transformation betrifft die Geschäftswelt sowie das Private gleichermassen. Daher vermag ein Erklärungsinhalt, der zwar nur mit technischen Hilfsmitteln wahrnehmbar gemacht werden kann aber visuell wahrnehmbar ist, dem Erfordernis des Erklärungsinhalts in Schriftzeichen durchaus zu genügen.

bb) Erklärungsinhalt in Schriftzeichen bei Smart Contracts

374 Wenn davon ausgegangen wird, dass Smart Contracts direkt ein vertragliches Verhältnis begründen können, dann muss auch bei Smart Contracts gelten, dass der Erklärungsinhalt in Schriftzeichen ein visuell wahrnehmbarer Text sein muss (N 372 f.), wobei es nicht darauf ankommt, dass zur visuellen Wahrnehmbarkeit technische Hilfsmittel eingesetzt werden müssen (N 373)

375 Wird ein Vertrag direkt als Smart Contract aufgesetzt, dann ist die Vertragssprache eine Programmiersprache.[597] Es ist fraglich, ob eine Programmiersprache dem Erfordernis des Erklärungsinhalts in Schriftzeichen

[597] Zur Frage, ob eine Programmiersprache Vertragssprache sein kann vgl. Kapitel E.I., N 269 ff.

genügt. Eine Programmiersprache ist zwar visuell wahrnehmbar, jedoch nicht eine der Allgemeinheit zugängliche, resp. verständliche Textform. Nach der Lehre genügt es jedoch, wenn die Schrift und Sprache den sich erklärenden Parteien zugänglich ist; nur wenn Drittinteressen betroffen sind, muss die Sprache der Allgemeinheit zugänglich sein.[598] Daraus schliesst sich, dass eine direkt mittels Programmiersprache aufgesetzte Erklärung allenfalls dann dem Kriterium der einfachen Schriftlichkeit genügen könnte, wenn der Text von den betroffenen Parteien verstanden wird (sie also die entsprechende Programmiersprache verstehen, d.h. fachkundige Personen sind), keine Drittinteressen betroffen sind und ein gültiger Erklärungsträger (vgl. nachfolgend N 376 ff.) sowie gültige Unterschriften (vgl. nachfolgend N 390 ff.) vorliegen. Es ist im Einzelfall zu beurteilen, ob diese kumulierten Erfordernisse erfüllt sind. So dürfte dies bspw. bei Forderungsabtretungen gem. Art. 165 Abs. 1 OR nie der Fall sein, da hier immer Drittinteressen betroffen sind.[599]

b) Erklärungsträger

376 Der Erklärungsträger ist gemäss klassischem Verständnis körperlich vorhanden und wird als eine Urkunde klassifiziert; dabei wird von der Urkunde in Papierform ausgegangen.[600] Die Urkunde verkörpert eine veränderungsresistente Speicherung des Erklärungsinhaltes. Modernen Kommunikationsmitteln und elektronischen Datenträgern wurde dieses Merkmal regelmässig abgesprochen; nicht zuletzt auch deshalb, weil unter den

598 KRAMER/SCHMIDLIN, BK OR, Allg. Erläuterungen zu Art.12-15 N 5.

599 Eine Forderung kann ohne Einwilligung und Kenntnis der Schuldnerin abgetreten werden, Art. 164 Abs. 1 OR, vgl. GIRSBERGER/HERRMANN, BSK OR I, Art. 164 N 5 ff.

600 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 504 ff.; SCHWENZER, BSK OR I, Art. 13 N 3; SCHWENZER, OR AT, N 31.06; BUCHER, OR AT, 164; HUGUENIN, OR, N 349; KRAMER/SCHMIDLIN, BK OR, Allg. Erläuterungen zu Art. 12-15 N 4.

Erklärungsinhalt keine Unterschrift gesetzt werden konnte, resp. die elektronische Unterschrift der eigenhändigen noch nicht gleichgestellt war.[601]

377 Bei der in der ZPO und im IPRG verankerten Textform muss der Erklärungsinhalt physisch reproduzierbar sein; hier besteht jedoch keine Einschränkung auf eine Urkunde als Erklärungsträger.[602] Elektronische Speicherung und Übermittlung ist in Bezug auf die Textform erlaubt, sofern der Empfänger die Möglichkeit zur Speicherung hat und der Text nicht alleine beim Absender verbleibt (z.B. nur auf dem Server des Absenders oder einem Drittserver, auf den nur der Absender Zugriff hat).[603]

378 Fasst man die Lehre zum Erklärungsträger i.S. von Art. 13 OR sowie die neuere Lehre zur Textform zusammen, kann festgehalten werden, dass der Erklärungsträger den Erklärungsinhalt veränderungsresistent und dauerhaft speichern und die Möglichkeit bestehen muss, den Erklärungsinhalt jederzeit physisch zu reproduzieren. Wird der neueren Lehre zur Textform gefolgt, dann muss der Erklärungsinhalt nicht zwingend in Papierform verurkundet sein, sondern kann auch auf einem elektronischen Datenträger gespeichert sein oder mittels moderner Kommunikationsmittel übertragen werden, sofern die Authentizität und Integrität des Inhalts garantiert werden kann; für letzteres wird das zusätzliche Erfordernis der Unterschrift benötigt (vgl. nachfolgend N 390 ff.).

aa) Erklärungsträger im elektronischen Geschäftsverkehr

379 Neuere Lehrmeinungen wollen elektronische Aufzeichnungen als Erklärungsträger i.S. von Art. 13 OR genügen lassen, da zwischenzeitlich technologisch sichergestellt werden kann, dass Daten nicht nachträglich abgeändert werden können.[604] Für diese Ansicht spricht auch, dass die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichgestellt ist (Art. 14 Abs. 2bis OR). Eine elektronische Signatur ergäbe

601 Vgl. Übersicht über die modernen Kommunikationsmittel und Lehrmeinungen bei SCHWENZER, BSK OR I, Art. 13 N 14-14e.

602 Vgl. GRÄNICHER, BSK IPRG, Art. 178 N 11.

603 GRÄNICHER, BSK IPRG, Art. 178 N 13.

604 SCHWENZER, BSK OR I, Art. 13 N 14c; XOUDIS, CR CO I, Art. 13 N 6.

keinen Sinn, wenn man die dazugehörige Erklärung und den Erklärungsträger in digitaler Form nicht genügen liesse.[605]

380 Grundsätzlich ist bei der Frage des Erklärungsträgers zwischen dem Erklärungsträger selbst und der Form der Übermittlung zu unterscheiden. Dabei gibt es jeweils zwei Fallgruppen. Beim Erklärungsträger ist zu differenzieren, ob der Text originär körperlich vorliegt und zusätzlich auf einen elektronischen Träger abgespeichert wird oder unkörperlich, d.h. rein digital vorliegt.[606] Bei der Übermittlung ist zwischen der physischen Übermittlung des Erklärungsträgers (z.B. Postversand von Papier, USB-Stick etc.) und der rein virtuellen Übermittlung zu unterscheiden.

381 Liegt der Erklärungsinhalt körperlich vor, dann ist das Körperliche jeweils auch der Erklärungsträger; hier ist von einer Urkunde im klassischen Verständnis auszugehen (vgl. hiervor N 376). Wird diese Urkunde digitalisiert und auf ein elektronisches Speichermedium abgelegt, dann ist die digitalisierte Version lediglich als eine Kopie der Urkunde zu werten.

382 Ist der Erklärungsinhalt als Text unkörperlich abgespeichert, z.B. als PDF in einer Cloud, auf einem USB-Stick oder als Text auf einem Mailserver, dann muss sichergestellt werden, dass das entsprechende Speicherformat beständig und dauerhaft (vgl. N 376), sowie der Text veränderungsresistent abgespeichert (N 378) und körperlich reproduzierbar (N 378) ist. Das Bundesgericht hat entschieden, dass ein elektronisch hinterlegtes PDF-Dokument den Kriterien der Dauerhaftigkeit und Beständigkeit genügt.[607] Bei elektronischen Speichermedien ist das Erfordernis der körperlichen Reproduzierbarkeit dann erfüllt, wenn das elektronische Speichermedium eine Reproduktion des Verkörperten zulässt. Der Nachweis der Integrität des

---

605 Vgl. HUGUENIN, OR, N 349; XOUDIS, CR CO I, Art. 13 N 6.

606 Vgl. hierzu GISLER, der zwischen „elektronischen“ (= virtuelle, digitale) und „digitalen“ (= digitalisierte, ursprünglich in Papierform vorliegende) Dokumenten unterscheidend: GISLER, vertragliche Aspekte elektronischer Märkte, 128 ff.

607 BGer Urteil 9C_597/2014 vom 10.12.2014 E. 4.5 (elektronisch hinterlegtes PDF-Dokument genügt den Formerfordernissen gem. Art. 61a Abs. 1 KVG).

Dokumentes (d.h. dass es nachträglich nicht verändert wurde) wird durch die elektronische Signatur (vgl. nachfolgend N 390) sichergestellt.

383 Bei der Übermittlung des Erklärungsinhaltes ist darauf abzustellen, ob sie so erfolgen kann, dass die Integrität und Authentizität des Inhaltes sichergestellt werden kann. Auch dies wird durch die elektronische Signatur (vgl. nachfolgend N 390) sichergestellt werden müssen.

384 Daraus folgt, dass die Art des Erklärungsträgers grundsätzlich irrelevant ist, sofern ein visuell wahrnehmbarer Text dauerhaft, körperlich reproduzierbar sowie veränderungsresistent abgespeichert werden kann. Bei der elektronischen Übertragung ist insbesondere das Kriterium der Textintegrität, d.h. die Veränderungsresistenz, von zentraler Bedeutung.

385 Das Kriterium der körperlichen Reproduzierbarkeit ist aus heutiger Sicht grundsätzlich zu hinterfragen. Der Körperlichkeit kommt zwar eine gewisse Sicherheitsrelevanz zu, ihre Bedeutung ist aus heutiger Sicht jedoch überholt. Auch rein digitale Daten können zwischenzeitlich so geschützt werden, dass sie vor Manipulation sicher sind.

bb) Erklärungsträger bei Smart Contracts

386 Wie bereits ausgeführt, kann ein Vertrag entweder ausserhalb des Smart Contract geschlossen werden und als Hash-Wert auf der Blockchain hinterlegt werden oder aber direkt mittels Smart Contract aufgesetzt werden (vgl. hiervor N 250 ff.). Wird der Vertrag ausserhalb des Smart Contract geschlossen, dann beurteilt sich die Frage nach dem Erklärungsträger nach dem dort Vereinbarten. Wird das ausserhalb des Smart Contract geschlossene Grundgeschäft als Hash-Wert (vgl. Anhang N 5 ff.) auf der Blockchain abgespeichert, dann dient die Blockchain immerhin dazu, die Integrität des Dokumentes zu überprüfen.[608]

---

608 In Kombination mit einem auf der Blockchain abgelegten Hash-Wert (Anhang, N 5 f.) kann die Integrität eines Dokumentes festgestellt werden, ohne dass dem Erklärungsträger hierfür spezielle veränderungsresistente Eigenschaften zukommen müssten. Es ist jedoch zu beachten, dass aus einem Hash-Wert im Umkehrschluss kein Dokument produziert, sondern nur aus einem Dokument ein Hash-Wert hergeleitet werden kann. Es kann

387 Ist der Smart Contract selbst der Vertrag (N 294), dann stellt er auch den Erklärungsträger dar. In diesen Fällen ist aus einer technologischen Sicht zumindest das Kriterium der Dauerhaftigkeit und Beständigkeit erfüllt, wenn der Smart Contract selbst auf der Blockchain abgespeichert ist (N 251). Trotzdem ist in diesem Zusammenhang ein Fragezeichen hinter das Kriterium der Beständigkeit zu setzen, da der Fortbestand der Blockchain nur solange gewährt ist, wie die P2P-Teilnehmer gewillt sind, dieses Netzwerk aufrecht zu erhalten. Dies ist aus heutiger Sicht schwer einzuschätzen und muss aufgrund der Neuheit der Technologie mit einer gewissen Skepsis beurteilt werden. Ist der Smart Contract in einem virtuellen Container abgespeichert (N 252), dann kann die Dauerhaftigkeit und Beständigkeit nicht bejaht werden.

388 Die körperliche Reproduzierbarkeit müsste ebenfalls (technisch) sichergestellt werden, wenn ein Smart Contract als Erklärungsträger qualifiziert werden müsste.

389 Ein Smart Contract kommt als tauglicher Erklärungsträger also nur dann in Frage, wenn er erstens den Vertrag selbst darstellt, zweitens direkt auf einer Blockchain abgespeichert ist, diese drittens eine gewisse Beständigkeit aufweist und viertens die körperliche Reproduzierbarkeit des Erklärungsinhalts (*in casu* die Programmierung) gewährleistet werden kann. Zusammenfassend kann daher festgehalten werden, dass ein Smart Contract sich aus heutiger Sicht grundsätzlich nicht als Erklärungsträger eignet.

c) Unterschrift

390 Zentrales Element der einfachen Schriftlichkeit ist die Unterschrift der sich verpflichtenden Parteien (vgl. Art. 13 OR). Die Parteien anerkennen so den festgehaltenen Vertragsinhalt und dokumentieren ihren Abschlusswillen.[609] Die qualifizierte elektronische Signatur ist der eigenhändigen Unterschrift gleichgestellt (Art. 14 Abs. 2bis OR, zur elektronischen Signatur vgl. Anhang N 15 ff.). Die Unterschrift kann demnach entweder eigenhändig oder mit einer qualifizierten elektronischen Signatur unter den Erklärungsinhalt gesetzt

---

also festgestellt werden, ob das Dokument abgeändert wurde, aber nicht wie.

609 BGE 119 III 4 E. 3 S. 6.

werden. Zweck der Unterschrift ist der Ausdruck der Anerkennung des Inhaltes durch den Erklärenden sowie dessen Identifikation.[610]

aa) Unterschrift im elektronischen Geschäftsverkehr

391 Im elektronischen Geschäftsverkehr bietet sich die Verwendung der qualifizierten elektronischen Signatur an. Diese ist bereits seit 2005 der eigenhändigen Unterschrift gleichgestellt, doch hat sie sich im Geschäftsverkehr noch nicht durchgesetzt. Die Gründe mögen in der oft genannten benutzerfeindlichen Anwendung oder am fehlenden Interesse des breiten Publikums liegen.[611] Geregelt ist die elektronische Signatur im Bundesgesetz über die elektronische Signatur (ZertES).[612] Die qualifizierte elektronische Signatur kann die Identität des Unterzeichners der Nachricht, die Authentizität eines Dokumentes wie auch die Integrität (das Dokument wurde nicht abgeändert) nachweisen.[613]

bb) Unterschrift bei Smart Contracts

392 Auf allen Blockchain-Plattformen und Blockchain-Anwendungen werden grundsätzlich elektronische Signaturen eingesetzt, um Transaktionen zu tätigen (vgl. N 56 ff.). Auch die Vermögensverschiebungen der Parteien an den Smart Contract geschehen durch eine signierte Transaktion (vgl. N 256). Auf öffentlichen wie auch privaten Blockchains werden jedoch keine Signaturschlüssel eingesetzt, die von einer eidgenössisch anerkannten Zertifizierungsstelle zertifiziert worden sind (ungeachtet dessen, ob sie die Anforderungen erfüllen würden oder nicht). Das heisst, die (derzeit) weltweit verwendeten elektronischen Signaturen auf Blockchains genügen nicht, um die Voraussetzungen der einfachen Schriftlichkeit zu erfüllen. Um das Formerfordernis der einfachen Schriftlichkeit dennoch zu erfüllen, könnte ein

---

610 SCHWENZER, BSK OR I, Art. 13 N 6.

611 Vgl. WEBER, E-Commerce, 322.

612 Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) vom 18. März 2016, SR 943.03; vgl. Anhang, N 13 ff.

613 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 519b; WEBER, E-Commerce, 325; BOTSCHAFT ZERTES, BBl 2014 1001, 1016.

Anbieter einer Blockchain-Applikation ZertES-konforme qualifizierte elektronische Signaturen einsetzen.

393 Ein Smart Contract, also das auf einem Konto installierte Programm, hat keinen eigenen Private Key; ist der Smart Contract direkt auf der Blockchain abgespeichert, dann führen alle Knotenpunkte die Transaktion durch (vgl. N 251).

3. Qualifizierte Schriftlichkeit

394 Die qualifizierte Schriftlichkeit setzt neben der einfachen Schriftlichkeit noch ein zusätzliches Erfordernis voraus; dieses kann entweder inhaltlicher oder formeller Natur sein.[614] Das Zusatzerfordernis zur einfachen Schriftlichkeit ist der jeweiligen Gesetzesbestimmung zu entnehmen. So ist beispielsweise für die letztwillige Verfügung Eigenhändigkeit (Art. 505 ZGB) oder für die Kündigung von Miet- und Geschäftsräumen die Verwendung eines bestimmten Formulars (Art. 266l OR) vorgesehen.

395 Soweit das Zusatzerfordernis für die qualifizierte Schriftlichkeit inhaltlicher Natur ist, muss es auf dem Vertrag abgebildet werden. Handelt es sich um formelle Vorschriften, muss geprüft werden, ob diese auch digital abbildbar sind. So ist beispielsweise das Erfordernis der Eigenhändigkeit niemals mit einem rein digitalen Text erfüllt. Bei kantonal vorgeschriebenen Formularen im Mietrecht, bspw. bei Kündigung von Miet- und Geschäftsräumen, ist es davon abhängig, ob das kantonale Recht digitale Formulare zulässt.[615]

396 Sollte das Zusatzerfordernis digital abbildbar und gesetzlich zugelassen sein, dann könnte auch die qualifizierte Schriftlichkeit Eingang in den elektronischen Geschäftsverkehr finden. Denkbar ist dies am ehesten bei formellen Voraussetzungen wie bspw. einem Formularzwang, welcher auch in die digitale Welt transferierbar wäre.

---

614 BERGER, Allgemeines Schuldrecht, N 763; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 521; SCHWENZER, OR AT, N 31.16.

615 Dies ist – soweit ersichtlich – noch in keinem Kanton der Fall.

4. Öffentliche Beurkundung

397 Bei der öffentlichen Beurkundung wird eine rechtserhebliche Tatsache oder Erklärung von einer Notarin festgehalten.[616] Die Ausgestaltung der öffentlichen Beurkundung ist kantonal geregelt (Art. 55a SchlT ZGB). Seit der Totalrevision der Verordnung über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV)[617], die seit dem 1. Februar 2018 in Kraft ist, sind elektronische öffentliche Urkunden und elektronische Beglaubigungen den entsprechenden Dokumenten in Papierform gleichgestellt (Art. 3 EÖBV, Art. 55o SchlT ZGB).

398 Die gesetzlichen Grundlagen für die elektronische öffentliche Beurkundung sind damit geschaffen. Ob dabei in absehbarer Zukunft die Blockchain-Technologie eingesetzt wird, ist aufgrund der hohen Rechtssicherheit der bestehenden Systeme in der Schweiz fraglich.

5. Formungültigkeit

399 Die Verletzung einer der vorgenannten Formvorschriften führt zur Nichtigkeit des Vertrages. Unter Umständen kann der Vertrag jedoch in ein gültiges Geschäft konvertiert oder rückabgewickelt werden. Die Formvorschriften und die aus einer Verletzung derselben resultierenden Rechtsfolgen gelten für sämtliche Rechtsgeschäfte, unabhängig davon, ob sie physisch oder virtuell geschlossen werden.[618]

---

616 BERGER, Allgemeines Schuldrecht, N 764; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 524; SCHWENZER, OR AT, N 31.16.

617 Verordnung über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV) vom 8. Dezember 2017, SR 211.435.1.

618 Vgl. SCHWENZER, BSK OR I, Art. 11 N 12.

a) Nichtigkeit und Teilnichtigkeit

aa) Allgemeine Regeln

400 Eine Formvorschrift ist eine Gültigkeitsvorschrift (Art. 11 OR).[619] Gemäss Bundesgericht führt die Verletzung einer Formvorschrift zur Nichtigkeit des Vertrages; jeder könne sich darauf berufen und dieser Umstand sei von Amtes wegen zu beachten.[620] Die absolute Nichtigkeit relativiert das Bundesgericht durch die Anwendung des Rechtsmissbrauchsverbots (Art. 2 ZGB).[621] Ob ein Rechtsmissbrauch vorliegt, ist unter Würdigung der konkreten Umstände zu beurteilen. Das Bundesgericht hat rechtsmissbräuchliches Verhalten bspw. bejaht bei der beidseitigen Erfüllung des formungültigen Vertrages, bei arglistiger Herbeiführung des Formmangels oder bei bewusster Inkaufnahme des Formmangels und der daraufhin geltend gemachten Formungültigkeit.[622]

401 Die herrschende Lehre spricht sich für einen differenzierten Lösungsansatz aus und geht nicht von einer absoluten Nichtigkeit aus, sondern vielmehr von einer relativen oder einer Nichtigkeit *sui generis*, die geheilt und nur von den Parteien selbst geltend gemacht werden könne.[623]

402 Wird der Formmangel schuldhaft von einer Partei herbeigeführt und beruft sich die andere Partei erfolgreich auf diesen Formmangel, so kann sie zusätzlich für einen Schadenersatz gestützt auf c.i.c. haftbar sein.[624]

---

619 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 547.

620 BGE 112 II 330 E. 2b S. 334 f., 106 II 146 E. 3 S. 151; BERGER, Allgemeines Schuldrecht, N 771; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 549; SCHWENZER, OR AT, N 31.27.

621 BGE 138 III 40 E. 2.3.1 S. 404; BERGER, Allgemeines Schuldrecht, N 772.

622 Vgl. BGE 138 III 401 E. 2.3.2 f. S. 4.4; weitere Aufzählungen und Hinweise bei GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 554; SCHWENZER, OR AT, N 31.31 ff.

623 BUCHER, OR AT, 169; BERGER, Allgemeines Schuldrecht, N 773; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 561; ausführlich und m.w.H. SCHWENZER, BSK OR I, Art. 11 N 23 ff.

624 GAUCH/SCHLUEP/SCHMID/EMMENEGGEr, OR AT, N 583; SCHWENZER, OR AT, N 31.42.

bb) Nichtigkeit und Teilnichtigkeit bei Smart Contracts

403 Bezüglich der Nichtigkeit eines Vertrages und dessen Umsetzung auf einer Blockchain, resp. bei einem Smart Contract kann auf das hiervor bei N 361 ff. Gesagte verwiesen werden.

b) Rückabwicklung und Konversion

404 Wie einleitend ausgeführt, kann nach den allgemeinen Regeln des Obligationenrechts ein formungültiges Geschäft je nach Umständen in ein gültiges umgedeutet (Konversion) oder, falls dies nicht möglich ist und kein Rechtsmissbrauch vorliegt, rückabgewickelt werden.[625]

405 Ein Smart Contract kann technisch grundsätzlich nicht rückabgewickelt werden. Es kann jedoch eine neue Transaktion durchgeführt werden, welche das Ergebnis des Smart Contract durch eine neue Transaktion faktisch rückabwickelt. Eine Konversion scheint hingegen unproblematisch.

[625] Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 584b; SCHWENZER, BSK OR I, Art. 11 N 25 ff.; SCHWENZER, OR AT, N 31.39 ff.

6. Fazit

Mit Smart Contracts können die Formvorschriften der einfachen oder qualifizierten Schriftlichkeit und der öffentlichen Beurkundung nicht erfüllt werden. Eine Ausnahme für die Erfüllung der Anforderungen der einfachen Schriftlichkeit ist dort zu sehen, wo fachkundige Personen ZertES-konforme Signaturen einsetzen würden und das Vereinbarte keine Drittinteressen betrifft. 406

Bezüglich des Erfordernisses der Körperlichkeit und der körperlichen Reproduzierbarkeit von Erklärungsinhalten ist allerdings fraglich, ob daran weiterhin festgehalten werden sollte, da zwischenzeitlich technologisch sichergestellt werden kann, dass gewisse Sicherheitsaspekte (Veränderungsresistenz und Dauerhaftigkeit) auch auf anderem Wege erreicht werden können. 407

Die Verletzung von Formvorschriften führt je nach Lehrmeinung zu Nichtigkeit oder Teilnichtigkeit des Vertrages. Verletzt ein Smart Contract eine Formvorschrift, dann kann der Umstand der Nichtigkeit des Vertrages auf einer Blockchain-Plattform nicht umgesetzt werden, da nachträglich (nach der Validierung durch das Netzwerk) keine Transaktionen abgeändert oder als ungültig markiert werden können. Eine faktische Rückabwicklung in Form einer neuen Transaktion oder eine Konversion ist allerdings möglich. 408

VIII. Fazit

409 Grundsätzlich können Verträge direkt als Smart Contracts in Programmiersprache aufgesetzt werden, sofern dies dem Willen der Vertragsparteien entspricht. Es bestehen jedoch Einschränkungen; so sind Smart Contracts nicht als Verträge zu qualifizieren, wenn fachunkundige Parteien involviert oder Formvorschriften zu beachten sind. Der Nachweis der Rechts- und Geschäftsfähigkeit der involvierten Personen obliegt den Parteien. Die Blockchain eignet sich als pseudoanonymes System nicht dazu, Vertragspartner zu identifizieren (mit Ausnahme von geschlossenen Systemen).

410 Der Smart Contract kann ein Angebot oder eine invitatio ad offerendum enthalten und sich an bestimmte Personen oder einen unbestimmten Adressatenkreis richten. Eine Widerrufsmöglichkeit (eines Angebots) besteht bei Smart Contract grundsätzlich nicht, ausser in Anwendungen ausserhalb der Blockchain. Der Vertrag kommt mit der Signierung durch die akzeptierende Partei, die mit einer Transaktion bspw. einen Wert an die Adresse des Smart Contract sendet, zustande. Willenserklärung und Konsens werden mittels Vertrauensprinzip ausgelegt.

411 Bezüglich Inhalt bestehen auch für Smart Contracts die gesetzlichen Inhaltsschranken der Sittenwidrigkeit, Unmöglichkeit und Widerrechtlichkeit. Die Nichtigkeit eines Smart Contract kann auf einer Blockchain nicht abgebildet werden; dies betrifft insbesondere die direkt auf einer Blockchain gespeicherten Smart Contracts sowie die in einer Cloud gespeicherten Smart Contracts, die das Ergebnis (Transaktion) jedoch schon in die Blockchain überführt haben. Die fehlende Umsetzungsmöglichkeit, resp. die Nichtfeststellung einer nichtigen Transaktion auf einer Blockchain, führt zu Rechtsunsicherheit bezüglich blockchainbasierter Transaktionen. In geschlossenen Systemen könnte zwar theoretisch vorgesehen werden, dass eine Transaktion als ungültig markiert wird, dies würde jedoch ebenfalls zu Rechtsunsicherheit und das Blockhain-System ad absurdum führen. Die im OR vorgesehene Nichtigkeit widerspricht im Kern der Grundkonzeption der Blockchain-Technologie als vertrauensloses System.

C. Mangelhafte Willenserklärungen

412 Ein Mangel im Vertragsschluss im Sinne einer mangelhaften Willenserklärung kann nach dem Obligationenrecht bei Irrtum, Drohung oder Täuschung entstehen. Tritt einer dieser Tatbestände ein und wird er von der betroffenen Partei geltend gemacht, ist der Vertrag für diese Partei einseitig unverbindlich. Der Vertragsmangel kann jedoch durch Genehmigung durch die Parteien aufgehoben werden.

I. Irrtum

413 Der Irrtum im Vertragsschluss wird nur in engen Grenzen berücksichtigt, dies gilt auch für ähnliche Rechtsinstitute der europäischen Nachbarländer.[626] Für den elektronischen Geschäftsverkehr wurden von der Lehre spezifische Fallgruppen erarbeitet; diese betreffen insbesondere die fehlerhafte Übermittlung einer Willenserklärung. Ähnliche Kategorien können für Smart Contracts hergeleitet werden.

1. Allgemeine Regeln

414 Ein Irrtum ist die falsche Vorstellung über einen Sachverhalt: Vorstellung und Wirklichkeit klaffen auseinander.[627] Die fehlende Vorstellung wird rechtlich wie die falsche Vorstellung behandelt.[628] Grundsätzlich wird zwischen wesentlichem und unwesentlichem Irrtum unterschieden, wobei ein unwesentlicher Irrtum unbeachtlich ist (Art. 23 OR). Wesentlichkeit wird aus objektiver und subjektiver Sicht beurteilt und besteht dann, wenn der Irrende bei Kenntnis des wahren Sachverhaltes keine oder eine andere Erklärung

---

626 SCHMIDLIN, BK OR, Vorbem. zu Art. 23-27 N 45.

627 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 761; SCHMIDLIN, BK OR, Art. 23/24 N 4; SCHWENZER, OR AT, N 37.01.

628 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 761; SCHMIDLIN, BK OR, Art. 23/24 N 10; SCHWENZER, OR AT, N 37.01.

abgegeben hätte.[629] Zudem muss die Wesentlichkeit erkennbar sein.[630] Bei einem wesentlichen Irrtum ist der Vertrag für den Irrenden einseitig unverbindlich (Art. 23 OR).[631]

415 Zu unterscheiden ist zwischen Erklärungsirrtum, Motivirrtum und Grundlagenirrtum. Bei einem (einfachen) Motivirrtum besteht der Irrtum aus einem Beweggrund zum Vertragsschluss, welcher gem. Art. 24 Abs. 2 OR als unwesentlich gilt.

416 Beim Erklärungsirrtum will dagegen der Irrende nicht, was er tatsächlich geäussert hat;[632] der Irrende hat einen Rechtsbindungswillen gebildet, diesen jedoch fehlerhaft kundgetan.[633] Ein Irrtum kann auch in der Übermittlung der Willenserklärung durch einen Boten geschehen (Art. 27 OR). Diese unrichtige Übermittlung durch einen Boten wird dem Erklärungsirrtum gleichgestellt.[634] Der Bote ist eine unselbständig handelnde Mittelsperson, worunter bspw. Dolmetscher, Mäkler, Agenten oder auch Hilfsmittel wie Telegramm, Telefax oder E-Mail fallen.[635] Die unrichtige Übermittlung besteht darin, dass die ursprüngliche (richtige) Nachricht inhaltlich verändert wurde und nicht mehr dem entspricht, was der Erklärende wollte oder dass die Erklärung an die falsche Adresse übermittelt wurde.[636]

417 Bei einem Grundlagenirrtum (auch qualifizierter Motivirrtum) irrt der Erklärende über einen Sachverhalt, der für ihn nach Treu und Glauben im

---

629 BERGER, Allgemeines Schuldrecht; SCHWENZER, OR AT, N 37.01.

630 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 778 ff.; SCHWENZER, OR AT, N 37.25 ff.

631 BERGER, Allgemeines Schuldrecht, N 1006; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 766; SCHWENZER, OR AT, N 37.02.

632 BERGER, Allgemeines Schuldrecht, N 978, 983; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 767; SCHMIDLIN, BK OR, Art. 23/24 N 39; SCHWENZER, OR AT, N 37.02.

633 SCHWENZER, OR AT, N 37.03.

634 BERGER, Allgemeines Schuldrecht, N 986; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 817; SCHWENZER, OR AT, N 37.07.

635 SCHMIDLIN, BK OR, Art. 27 N 5 f; SCHWENZER, BSK OR I, Art. 27 N 2.

636 SCHMIDLIN, BK OR, Art. 27 N 11.

Geschäftsverkehr eine notwendige Grundlage des Vertrags darstellt (Art. 24 Abs. 1 Ziff. 4 OR).[637]

1. Irrtum im elektronischen Geschäfts-verkehr

418 Im elektronischen Geschäftsverkehr werden bezüglich des Irrtums verschiedene Fallgruppen unterschieden, welche insbesondere die Übermittlung der Willenserklärung betreffen. Eingeteilt werden diese in die Irrtumskategorien Eingabe- und Bedienungsfehler, Übermittlungsfehler sowie fehlerhafte Computererklärungen.

a) Eingabe- und Bedienungsfehler

419 Liegt ein Fehler in der Eingabe oder Bedienung vor (bspw. durch „Vertippen"), dann kann ein Erklärungsirrtum vorliegen. Die Schwierigkeit liegt hier jedoch im Nachweis eines solchen Fehlers – insbesondere im Zusammenhang mit Webformularen, die sofort versendet werden.[638] In diesem Zusammenhang ist jedoch zu beachten, ob der Absender der Willenserklärung die Möglichkeit hatte, die Willenserklärung vor Übermittlung an den Empfänger zu überprüfen.[639] Unterliegt der Absender einem wesentlichen Irrtum, hatte aber die Möglichkeit der Überprüfung vor der Absendung, dann kann der Tatbestand des fahrlässigen Irrtums gem. Art. 26 Abs. 1 OR erfüllt sein.[640]

420 Wird die elektronische Willenserklärung nicht direkt versendet, sondern befindet sie sich noch im Herrschaftsbereich des Erklärenden, dann ist dieser

---

637 BERGER, Allgemeines Schuldrecht, N 989; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 776; SCHWENZER, OR AT, N 37.24.

638 Vgl. WEBER, E-Commerce, 346.

639 Vgl. Art. 11 E-Commerce RL, wonach bei Verbraucherverträgen im Internet dem Konsumenten die Erkennung und Berichtigung von Eingabefehlern vor der Absendung ermöglicht werden muss; für das deutsche Recht vgl. HOEREN, Internetrecht, N 767.

640 Laut SCHWENZER kann bei einem Erklärungsirrtum die Fahrlässigkeit meistens bejaht werden: SCHWENZER, BSK OR I, Art. 26 N 2.

für allfällige falsche Erfassungen im System selbst verantwortlich (die fehlerhafte Willenserklärung wurde gegen aussen nicht kundgetan).[641]

b) Übermittlungsfehler

421 Grundsätzlich muss sich der Erklärende den Fehler bei der Übermittlung zuschreiben lassen, wenn die Nachricht bei der Übermittlung verändert wird.[642] Lässt sich der Übermittlungsfehler auf eine fehlerhafte Übermittlung durch einen Boten zurückführen, kann auf Art. 27 OR zurückgegriffen werden.[643] Botenfunktion haben gemäss Lehre nebst den bekannten Kategorien wie bspw. Agenten oder Dolmetscher (vgl. N 416) auch Provider-Anbieter (jedoch nicht die EDV-Anlage des Erklärenden)[644], d.h. technischen Hilfsmitteln zur elektronischen Übertragung wie bspw. E-Mail kommt auch eine Botenfunktion zu.[645] Die unrichtige Übermittlung wird gem. h.L als Sonderfall des Erklärungsirrtums behandelt (N 416), vereinzelt aber auch als unbeachtlicher Motivirrtum.[646]

422 Führt eine Software eine den Vertragsabschluss herbeiführende Willenserklärung selbständig aus, dann ist sie demjenigen zuzurechnen, der die computergenerierte Willenserklärung initiiert hat, auch wenn diese fehlerhaft ist (fehlerhafte Computererklärung).[647] Eine Ausnahme kann dann sachgerecht sein, wenn die Willenserklärung nach Treu und Glauben und unter den

---

641 SCHMIDLIN, BK OR, Art. 27 N 27.

642 WEBER, E-Commerce, 347; SCHMIDLIN, BK OR, Art. 27 N 27.

643 WEBER, E-Commerce, 347.

644 SCHMIDLIN, BK OR, Art. 27 N 22, 24; WEBER, E-Commerce, 347.

645 Vgl. BERGER, Allgemeines Schuldrecht, N 987; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 817; SCHWENZER, OR AT, N 37.08a.

646 Laut WEBER stellen Erklärungen, die aufgrund einer fehlerhaften Software, Daten- oder Rechenfehlern unrichtig werden, einen unbeachtlichen Motivirrtum dar, da der Wille aufgrund der mangelhaften Software gar nicht richtig gebildet werden könne: WEBER, E-Commerce, 346.

647 SCHMIDLIN, BK OR, Art. 27 N 22; WEBER, E-Commerce, 347.

gegebenen Umständen als nicht plausibel erscheint.[648] Fehlerhafte Computererklärungen gehören nach der hier vertretenen Meinung zur Kategorie der Übermittlungsfehler; teilweise werden sie als separate Kategorie behandelt.

2. Irrtum bei Smart Contracts

Wie beim elektronischen Geschäftsverkehr, steht bei Smart Contracts insbesondere die fehlerhafte Übermittlung von Willenserklärungen im Zentrum der Betrachtung; sie kann sich aber auch durch Eingabe- und Bedienungsfehler im Zusammenhang mit einem Smart Contract ergeben. 423

a) Fehlerhafte Willenserklärung beim Abschluss des Grundgeschäftes

Die fehlerhafte Willenserklärung kann sich bereits beim Abschluss des Grundgeschäfts ausserhalb des Smart Contract oder – falls das Vertragsverhältnis direkt als Smart Contract aufgesetzt ist – in diesem selbst manifestieren. Ob es sich dabei um einen Grundlagenirrtum, Erklärungsirrtum oder Motivirrtum handelt (vgl. N 414 ff.), ist im konkreten Einzelfall zu entscheiden. 424

b) Eingabe- und Bedienungsfehler

Ungeachtet dessen, ob das Grundgeschäft ausserhalb oder direkt mittels Smart Contract aufgesetzt wird, kann der ursprünglich fehlerlose Wille fehlerhaft in Programmiersprache abgebildet und entsprechend falsch durch den Smart Contract ausgeführt werden. Der Fehler liegt hier nicht in einem Fehler der Software selbst, sondern in der fehlerhaften Eingabe bei der Programmierung. Hierbei kann es sich um einen Fall des Erklärungsirrtumes handeln, analog der fehlerhaften Bedienung oder Eingabe beim elektronischen Geschäftsverkehr (vgl. N 419 f.). 425

648 WEBER, E-Commerce, 347 (Beispiel: Bestellung von 100 Kirschtorten durch Privatperson).

c) Übermittlungsfehler

426 Wird die ursprünglich fehlerlose Willenserklärung zwar im Smart Contract richtig hinterlegt, durch die Software jedoch verfälscht und fehlerhaft umgesetzt, dann kann ein Fall von Art. 27 OR vorliegen, wenn dem Smart Contract eine Botenfunktion zukommt.

427 Ein Smart Contract kann, wie andere elektronische Übermittlungsdienste auch (N 416, 421), grundsätzlich als Bote qualifiziert werden, da er keine eigenen Willenserklärungen abgibt, sondern die Willenserklärungen der Parteien umsetzt, resp. übermittelt.[649]

II. Täuschung und Furchterregung

428 Absichtliche Täuschung und Furchterregung können ebenfalls einen mangelhaften Willen einer Vertragspartei hervorrufen und bei erfolgreicher Geltendmachung den Vertrag für diese Partei einseitig unverbindlich werden lassen.

1. Täuschung

429 Täuschung liegt vor, wenn ein Vertragsschliessender durch absichtliche Täuschung des Vertragspartners zum Vertragsabschluss verleitet wurde (Art. 28 Abs. 1 OR). Beim Getäuschten liegt ein Motivirrtum vor, der durch

---

649 A.A. FURRER, der davon ausgeht, dass der Wille der Parteien beim Einsatz eines Smart Contract noch nicht gebildet ist und der Smart Contract daher auch keinen bestehenden Willen transportieren kann. Dem Smart Contract kommt nach dieser Meinung eine Art Stellvertreterfunktion zu und er wird als eine Art „Wissens- und Willenserklärungsgenerierungsmaschine“ bezeichnet: FURRER, Smart Contracts, 108. Wie bereits in FN 516 ausgeführt, wird hier die Meinung vertreten, dass ein Smart Contract – falls er direkt das Grundgeschäft abbildet – ein bedingtes Rechtsgeschäft darstellt und in diesen Fällen mit Abschluss des Rechtsgeschäftes der Wille sich auch auf die zukünftig ungewissen Tatsachen erstreckt.

den Täuschenden hervorgerufen wurde.[650] Diese Täuschungshandlung kann durch positives Verhalten oder auch durch Schweigen erfolgen.[651] Für die Erfüllung des Tatbestandes ist zudem eine Absicht des Täuschers, Widerrechtlichkeit sowie Kausalität erforderlich.[652]

2. Furchterregung

430 Wird ein Vertragsschliessender von einem Vertragspartner oder Dritten durch Furchterregung (Drohung) zum Vertragsschluss gedrängt, dann ist der Vertrag für den Bedrohten unverbindlich (Art. 29 Abs. 1 OR).[653] Hier liegt beim Bedrohten kein Irrtum vor, sondern der Mangel betrifft direkt den Willen, die innere Freiheit.[654] Die durch die Drohung ausgelöste Furcht muss gem. Art. 31 Abs. 1 OR eine gegründete sein, d.h. die Drohung muss eine gewisse Schwere aufweisen und widerrechtlich sein.[655]

---

650 BERGER, Allgemeines Schuldrecht, N 1035; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 856; SCHWENZER, OR AT, N 38.01.

651 BERGER, Allgemeines Schuldrecht, N 1039 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 856 ff; SCHWENZER, BSK OR I, Art. 28 N 6 ff.; SCHWENZER, OR AT, N 83.03 ff.

652 BERGER, Allgemeines Schuldrecht, N 1037 ff.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 864 ff.; SCHWENZER, OR AT, N 38.07 ff.

653 Vgl. BERGER, Allgemeines Schuldrecht, N 1051; vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 883; SCHWENZER, OR AT, N 38.13.

654 BERGER, Allgemeines Schuldrecht, N 1051; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 874; SCHWENZER, OR AT, N 38.13.

655 BERGER, Allgemeines Schuldrecht, N 1053 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 879 f.; SCHWENZER, OR AT, N 38.17, 38.20.

3. Täuschung und Furchterregung im elektronischen Geschäftsverkehr und bei Smart Contracts

431 Gemäss den allgemeinen Regeln müssen auch im elektronischen Geschäftsverkehr und bei Smart Contracts Willensmängel aufgrund von Täuschung oder Furchterregung (Drohung) geltend gemacht werden können. Es ist derzeit nicht ersichtlich, wie das vom Gesetz definierte menschliche Fehlverhalten der Parteien durch Computercodes verhindert werden könnte.

III. Rechtsfolgen

432 Sowohl bei einem wesentlichen Irrtum als auch bei einer Täuschung oder Furchterregung ist die Rechtsfolge die einseitige Unverbindlichkeit für diejenige Partei, die dem Irrtum unterlegen ist oder absichtlich getäuscht oder bedroht wurde (Art. 23, Art. 28 Abs. 1 und Art. 29 Abs. 1 OR).

1. Einseitige Unverbindlichkeit

433 Unterliegt eine Partei einem wesentlichen Irrtum, einer Täuschung oder Drohung, ist der Vertrag nach erfolgreicher Geltendmachung für diese Partei einseitig unverbindlich (Art. 23, Art. 28 Abs. 1 und Art. 29 Abs. 1 OR). In der Lehre herrschen unterschiedliche Auffassungen darüber, ob dabei gem. der Ungültigkeitstheorie[656] der Vertrag von Anfang an (ex tunc) ungültig ist und dementsprechend keine Wirkung entfaltet oder ob gem. der Anfechtungstheorie[657] der Vertrag zunächst gültig ist, aber unter Berufung auf

656 Zur Ungültigkeitstheorie vgl. GAUCH/SCHLUEP/SCHMID/ EMMENEGGER, OR AT, N 890 ff.; BERGER, Allgemeines Schuldrecht, N 1009.

657 Zur Anfechtungstheorie vgl. SCHMIDLIN, BK OR, Art. 23/24 N 379 ff.; SCHWENZER, BSK OR I, Art. 23 N 10; SCHWENZER, OR AT, N 39.07.

den Willensmangel aufgelöst wird.[658] Welcher Theorie gefolgt wird, ist von Bedeutung für den allfälligen Rückforderungsanspruch, wenn der Irrende, Getäuschte oder Bedrohte den Vertrag anficht. Bei der Ungültigkeitstheorie handelt es sich um eine Leistung wegen Nichtschuld (d.h. Rückforderung wegen Nichtschuld), nach der Anfechtungstheorie jedoch um eine Leistung wegen nachträglich weggefallenem Grund (d.h. Rückforderung aus nachträglich weggefallenem Grund).[659]

434 Nach der Ungültigkeitstheorie ist der Vertrag ex tunc unverbindlich, d.h. er entfaltet keine Wirkung, analog zu einem nichtigen Vertrag (vgl. N 355 ff.).[660] Die Unverbindlichkeit muss von der geschützten Partei geltend gemacht und kann nicht von Amtes wegen berücksichtigt werden.[661] Die geschützte Partei kann die Leistung verweigern und bereits geleistete Leistungen je nach den anzuwendenden Gesetzesbestimmungen aus Vindikation (Art. 641 Abs. 2 ZGB) oder ungerechtfertigter Bereicherung (Art. 62 ff. OR) zurückverlangen oder allenfalls eine Grundbuchberichtigungsklage (Art. 975 ZB) einleiten.[662] Der Gegenpartei ist es verwehrt, sich auf die Ungültigkeit des Vertrages zu berufen, da sie selbst keinem Willensmangel, keiner Drohung oder Täuschung unterlegen ist.[663] Macht die geschützte Partei die Ungültigkeit des Vertrages geltend, dann kann die Gegenpartei ebenfalls die Vertragserfüllung verweigern und bereits Geleistetes zurückverlangen (ebenfalls aus Vindikation, ungerechtfertigter Bereicherung oder Grundbuchberichtigungsklage).[664]

---

658 Ausführlich zum Theorienstreit vgl. SCHMIDLIN, BK OR, Art. 23/24 N 364 ff.

659 SCHWENZER, BSK OR I, Art. 23 N 9.

660 BERGER, Allgemeines Schuldrecht, N 1009; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 890; SCHWENZER, OR AT, N 39.23.

661 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 891 f.

662 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 892; SCHWENZER, OR AT, N 39.27.

663 BERGER, Allgemeines Schuldrecht, N 1006; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 893; SCHWENZER, OR AT, N 39.11.

664 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 893.

435 Wird der Anfechtungstheorie gefolgt, ist der Vertrag für beide Parteien gültig, wobei jedoch die geschützte Partei ein Anfechtungsrecht hat, bei dessen Ausübung der Vertag mit Wirkung ex tunc aufgehoben wird.[665]

436 Zu beachten ist die Einschränkung in Art. 25 Abs. 1 OR, wonach die Geltendmachung eines Irrtums unstatthaft ist, wenn sie Treu und Glauben widerspricht. Dies wird dann angenommen, wenn eine unnütze Rechtsausübung vorliegt oder ein krasses Missverhältnis zwischen den Interessen besteht.[666] Zudem muss ein Irrender bei einem wesentlichen Erklärungsirrtum diesen gegen sich gelten lassen, wenn die Vertragspartei dies dem Dahinfallen des Vertrages vorzieht (Art. 25 Abs. 2 OR).[667]

2. Schadenersatzpflicht

437 Bei fahrlässigem Irrtum wird der Irrende allenfalls schadenersatzpflichtig, ausser, die andere Vertragspartei hat den Irrtum erkannt oder hätte ihn erkennen sollen (Art. 26 OR); die Anspruchsgrundlage ist (eine gesetzliche) *culpa in contrahendo*.[668]

438 Bei dem Tatbestand der Täuschung oder der Drohung ist der Täuschende dem Getäuschten, resp. Bedrohten gegenüber ggf. schadenersatzpflichtig, sofern sich eine Schadenersatzpflicht aus Art. 41 ff. OR oder aus culpa in contrahendo herleiten lässt.[669]

---

665 BERGER, Allgemeines Schuldrecht, N 1008; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 896; SCHWENZER, OR AT, N 39.07.

666 BGE 132 III 737 E. 3.1. S. 743, 123 III 200 E. 2b S. 203; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 846.

667 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 848; SCHWENZER, BSK OR I, Art. 25 N 8.

668 BERGER, Allgemeines Schuldrecht, N 1026; SCHWENZER, BSK OR I, Art. 26 N 1.

669 BERGER, Allgemeines Schuldrecht, N 1062; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 870 f., 883 ff.

439 Für die Geltendmachung des Schadenersatzes ist die Anfechtungsfrist von Art. 31 OR (ein Jahr ab Entdeckung) sowie die Sonderbestimmung in Art. 31 Abs. 3 OR zu beachten, die auch eine Schadenersatzpflicht bei Genehmigung des Vertrages trotz Täuschung oder Drohung nicht ausschliesst.[670]

3. Genehmigung

440 Der mangelhafte Vertrag kann durch die betroffene Partei durch ausdrückliche Erklärung oder konkludentes Verhalten genehmigt werden.[671] Wenn der Mangel nicht innert Jahresfrist geltend gemacht wird, gilt der Vertrag als genehmigt (Art. 31 Abs. 1 OR).[672] Die Frist beginnt bei Irrtum und Täuschung mit deren Entdeckung, bei der Drohung mit deren Wegfall (Art. 31 Abs. 2 OR).[673]

4. Rechtsfolgen im elektronischen Geschäftsverkehr und bei Smart Contracts

441 Die Rechtsfolgen sind im elektronischen Geschäftsverkehr und bei Smart Contracts bei Irrtum, Täuschung und Drohung dieselben wie im traditionellen Vertragsrecht.

442 Bei automatisierten Vertragsabwicklungen und vordefinierten Parametern stellt die Beurteilung, ob ein Irrtum, eine Täuschung oder eine Drohung vorliegt, praktisch ein grosses Problem dar. Solche Verhaltensweisen können nicht mit vordefinierten Regeln abgebildet werden, da einerseits eine Einzelfallbetrachtung notwendig ist und andererseits fraglich ist, wie eine

---

670 BERGER, Allgemeines Schuldrecht, N 1016 ff.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 906; SCHWENZER, OR AT, N 39.15.

671 SCHWENZER, BSK OR I, Art. 31 N 17.

672 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 901.

673 Verwirkungs-, nicht Verjährungsfrist: BGE 114 II 131 E.2b S. 141; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 902; SCHWENZER, BSK OR I, Art. 31 N 11.

Software menschliches Verhalten angemessen beurteilen kann. Daher scheint es bei mangelhaften Willenserklärungen nach wie vor notwendig, dass auf eine menschliche Instanz (ordentliche Gerichte) zurückgegriffen werden muss. Das Gleiche gilt für die Berechnung von Schadenersatz oder die Beurteilung eines Anspruchs aus c.i.c. Sodann ist die Abbildung eines unverbindlichen Vertrages auf einer Blockchain nicht möglich, da aufgrund der nachträglichen Unabänderbarkeit insbesondere von Smart Contracts, die direkt auf einer Blockchain implementiert sind, nicht verändert werden können (vgl. N 361 ff.)

IV. Fazit

443 Für den elektronischen Geschäftsverkehr gibt es bereits an die besonderen Gegebenheiten angepasste Fallgruppen, auf die sich die allgemeinen Grundprinzipien des Irrtums anwenden lassen. Die gleichen Fallgruppen lassen sich bei der Verwendung von Smart Contracts anwenden. Es steht insbesondere die fehlerhafte Übermittlung im Zentrum, wobei dem Smart Contract (wie bei elektronischen Übermittlungsdiensten) grundsätzlich die Eigenschaft als Bote zukommt.

444 Auch Täuschung und Drohung können in der digitalen Welt nicht vermieden werden, da menschliches (Fehl-) Verhalten nicht durch Algorithmen verhindert werden kann. Da menschliche Verhaltensweisen nicht durch Prozesse abgebildet und eindeutig bewertet werden können, muss nach wie vor für die Beurteilung, ob ein Irrtum, eine Täuschung oder Drohung vorliegt, auf menschliche Instanzen der realen Welt zugegangen werden.

445 Die Rechtsfolgen einer mangelhaften Willenserklärung (die einseitige Unverbindlichkeit und allenfalls Anspruch auf Schadenersatz) gelten auch generell für den elektronischen Rechtsverkehr und für Verträge auf der Blockchain. Wird ein Vertrag, dem ein mangelhafter Wille zugrunde liegt, erfolgreich angefochten, dann ist die Folge davon (einseitige Unverbindlichkeit) nicht auf der Blockchain umsetzbar, da Transaktionen im Nachhinein nicht als ungültig markiert werden können.

D. Leistungsstörungen

Bei Vertragsverhältnissen kann es, sowohl im klassischen als auch im elektronischen Geschäftsverkehr, zu Leistungsstörungen kommen. Leistungsstörungen können unterteilt werden in Leistungsunmöglichkeit, positive Vertragsverletzung sowie Spätleistung. 446

Nachfolgend wird untersucht, ob Leistungsstörungen auch bei der Anwendung von Smart Contracts auftreten oder ob sie mit der Hilfe von Smart Contracts allenfalls vermieden werden können. 447

I. Leistungsunmöglichkeit

Die Leistungsunmöglichkeit beinhaltet die endgültige Nichterfüllung des Vertrages.[674] Sie wird auch Nichtleistung, Nichterfüllung oder schlicht Unmöglichkeit genannt.[675] Es gibt verschiedene Arten der Leistungsunmöglichkeit: Sie kann ursprünglich oder nachträglich, objektiv oder subjektiv und von der Schuldnerin, Gläubigerin oder von beiden Seiten zu verantworten oder nicht zu verantworten sein; in der Regel besteht sie aus einer Kombination dieser Möglichkeiten.[676] 448

674 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2523.

675 SCHWENZER, OR AT, N 63.01.

676 BERGER, Allgemeines Schuldrecht, N 1505 ff.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2523; SCHWENZER, OR AT, N 63.01 ff.

1. Ursprüngliche und nachträgliche Leistungsunmöglichkeit

449 Die ursprüngliche Unmöglichkeit bezeichnet einen Vertrag mit einem unmöglichen Inhalt (Art. Art. 20 Abs. 1 OR); die Unmöglichkeit liegt schon vor Vertragsschluss vor). Folge ist die Nichtigkeit (vgl. N 349 ff.).[677]

450 Bei der nachträglichen Unmöglichkeit tritt die Leistungsunmöglichkeit erst nach Vertragsschluss ein; dieser Tatbestand wird von Art. 97 Abs. 1 OR erfasst.[678]

2. Objektive und subjektive Leistungsunmöglichkeit

451 Liegt ein Fall der objektiven Unmöglichkeit vor, kann die Vertragspflicht der Schuldnerin weder von der Schuldnerin, noch von einer anderen Partei erfüllt werden.[679] Die nachträgliche, objektive Unmöglichkeit fällt unstrittig in den Anwendungsbereich von Art. 97 Abs. 1 OR.[680]

452 Bei der subjektiven Leistungsunmöglichkeit kann nur die eigentliche Schuldnerin nicht leisten.[681] Diese Leistungsunmöglichkeit unterliegt strengen Voraussetzungen; das Bundesgericht verlangt, dass die Leistung für die

---

677 GUILLOD/STEFFEN, CR CO I, Art. 19,20 N 76; SCHWENZER, OR AT, N 64.02.

678 Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2525; SCHWENZER, OR AT, N 63.10; WIEGAND, BSK OR I, Art. 97 N 7.

679 BERGER, Allgemeines Schuldrecht, N 1507; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2526; SCHWENZER, OR AT, N 63.08; WIEGAND, BSK OR I, Art. 97 N 10.

680 vgl. BERGER, Allgemeines Schuldrecht, N 1505; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2526; SCHWENZER, OR AT, N 64.09; WIEGAND, BSK OR I, Art. 97 N 10.

681 BERGER, Allgemeines Schuldrecht, N 1508; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2567; SCHWENZER, OR AT, N 63.03; WIEGAND, BSK OR I, Art. 97 N 11.

Schuldnerin geradezu unüberwindbar sei.[682] Auch hier kann zwischen anfänglicher und nachträglicher subjektiver Unmöglichkeit unterschieden werden. Sie kann zudem dauerhafter oder lediglich vorübergehender Natur sein.[683] Ist sie lediglich vorübergehend, dann handelt es sich um eine Leistungsverzögerung (sofern kein Fixgeschäft vorliegt).[684]

453 Das Bundesgericht und die h.L. subsumieren die anfängliche wie auch die nachträgliche subjektive Unmöglichkeit – gleich wie die objektive Unmöglichkeit – unter den Tatbestand von Art. 97 Abs. 1 OR, sofern die Schuldnerin die Unmöglichkeit zu verantworten hat.[685] Hat die Schuldnerin hingegen die Unmöglichkeit nicht zu vertreten, kommt Art. 119 OR zur Anwendung.[686]

454 Ein Teil der Lehre geht davon aus, dass die subjektive Leistungsunmöglichkeit generell nicht unter Art. 97 OR subsumierbar sei, da diesbezüglich ein Fall des Schuldnerverzugs vorliege und die Regeln von Art. 102 ff. OR zur Anwendung gelangten.[687]

---

682 BGE 115 III 212 E. 3.1 S. 218; BERGER, Allgemeines Schuldrecht, N 1510; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2567.

683 Vgl. BERGER, Allgemeines Schuldrecht, N 1519 ff.; SCHWENZER, OR AT, N 63.08 ff.

684 BERGER, Allgemeines Schuldrecht, N 1521; WIEGAND, BSK OR I, Art. 97 N 16.

685 BERGER, Allgemeines Schuldrecht, N 1508 (nachträglich subj.), N 1512 (anfänglich subj.); SCHWENZER, OR AT, N 63.08 (anfänglich subj.), 64.19 (nachträglich subj.); WIEGAND, BSK OR I, Art. 97 N 11 ff.

686 BERGER, Allgemeines Schuldrecht, N 1529; SCHWENZER, OR AT, N 64.08 (anfänglich subj.), 64.09, 64.11 (nachträglich subj.); WIEGAND, BSK OR I, Art. 97 N 13.

687 Ausführliche Begründung dieser Meinung bei GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2575 ff.; THÉVENOZ, CR CO I, Art. 97 N 11.

3. Unverschuldete Leistungsunmöglichkeit

455 Ist die Nichterfüllung, resp. die Leistungsunmöglichkeit durch keine Vertragspartei zu verantworten, bestimmt sich die Rechtsfolge gem. h.L. nach Art. 119 OR.[688] Folge von Art. 119 OR ist einerseits der Untergang der Forderung gegenüber der Schuldnerin und andererseits auch der Untergang der Gegenforderung bei synallagmatischen Verträgen.[689] Bereits empfangene Gegenleistungen sind zurückzuerstatten (Abs. 2). Ausgenommen von diesen Regelungen sind besondere Bestimmungen, nach denen die Gefahr[690] gem. Gesetzesvorschrift oder gem. Inhalt des Vertrages vor Erfüllung auf die Gläubigerin übergeht (Abs. 3).[691]

456 Bezieht die Schuldnerin einen Ersatz oder Ersatzanspruch infolge der nachträglichen Leistungsunmöglichkeit von einem Dritten, so muss dieser anstelle der unmöglich gewordenen Leistung der Gläubigerin auf dessen Verlangen herausgegeben werden (sog. *stellvertretendes Commodum*).[692]

---

688 BERGER, Allgemeines Schuldrecht, N 1591; vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2531 ff., 2591 ff., ; SCHWENZER, OR AT, N 64.09.

689 BERGER, Allgemeines Schuldrecht, N 1596; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2536, 2541; WIEGAND, BSK OR I, Art. 119 N 11 ff.

690 Im Sinne einer Preisgefahr, BERGER, Allgemeines Schuldrecht, N 1600; WIEGAND, BSK OR I, Art. 119 N 10.

691 BERGER, Allgemeines Schuldrecht, N 1601 ff.; WIEGAND, BSK OR I, Art. 119 N 9 f.

692 BERGER, Allgemeines Schuldrecht, N 1607 ff.; GAUCH/SCHLUEP/SCHMID/ EMMENEGGER, OR AT, N 2595; SCHWENZER, OR AT, N 61.14; WIEGAND, BSK OR I, Art. 119 N 15.

4. Verschuldete Leistungsunmöglichkeit

457 Ist die Leistungsunmöglichkeit durch die Schuldnerin zu vertreten, kommen generell die Rechtsfolgen von Art. 97 Abs. 1 OR zum Zuge.[693] Da die ursprüngliche Leistung aufgrund der Unmöglichkeit nicht mehr erbracht werden kann, entsteht ein Sekundäranspruch in Form eines Schadenersatzes.[694] Voraussetzungen für einen Schadenersatzanspruch aus Art. 97 Abs. 1 OR sind ein Schaden, eine Pflichtverletzung, ein Kausalzusammenhang sowie ein Verschulden.[695]

458 Die Leistungsunmöglichkeit der Schuldnerin, verursacht durch das Verschulden der Gläubigerin, wird im Allgemeinen Teil des Obligationenrechts nicht gesondert geregelt; vereinzelt finden sich Bestimmungen zu den einzelnen Vertragsverhältnissen im Besonderen Teil (z.B. Art. 176 Abs. 3, 324 und 378 OR).[696] Die herrschende Lehre und das Bundesgericht gehen davon aus, dass die Schuldnerin in Anwendung von Art. 119 Abs. 1 OR von ihrer Leitungspflicht befreit wird und grundsätzlich einen Anspruch gegen die Gläubigerin behält.[697]

459 Haben beide Parteien die Leistungsunmöglichkeit zu verantworten, dann wird gemäss Bundesgericht mangels gesetzlicher Regelung der Schadenersatzanspruch der Gläubigerin, der Anspruch der Schuldnerin auf Gegenleistung oder beide Ansprüche verrechnungsweise gekürzt.[698]

---

693 BERGER, Allgemeines Schuldrecht, N 1525; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2524; SCHWENZER, OR AT, N 64.19.

694 SCHWENZER, OR AT, N 64.20.

695 BERGER, Allgemeines Schuldrecht, N 1526; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2586a.

696 BERGER, Allgemeines Schuldrecht; SCHWENZER, OR AT, N 64.29.

697 BERGER, Allgemeines Schuldrecht, N 1614; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2591 ff.; SCHWENZER, OR AT, N 64.29; WIEGAND, BSK OR I, Art. 119 N 14; BGE 122 III 66 E. 3b S. 70.

698 BGE 122 III 66 E. 3b S. 70, 114 II 274 E. 4 S. 276; BERGER, Allgemeines Schuldrecht, N 1617 f.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2593.

5. Leistungsunmöglichkeit bei Smart Contracts

460 Zur Erinnerung: Ein Smart Contract führt die Vertragsbestandteile automatisiert aus und referenziert dabei auf prüfbare Ereignisse (vgl. N 251 ff.).[699]

a) Ursprüngliche Unmöglichkeit

461 Ob bei einem Smart Contract eine Leistungsstörung in Form eines unmöglichen Vertragsinhalts verhindert werden kann, bedarf einer differenzierten Betrachtung: Aus einer rein blockchaininternen Sicht und aufgrund der Grundannahme, dass jeder Eintrag auf einer Blockchain gemäss den systemimmanenten Regeln gültig ist (vgl. N 23 ff.), ist die Ausführung eines anfänglich unmöglichen Vertragsinhaltes mit einem Smart Contract grundsätzlich nicht möglich.[700] Der Smart Contract muss zur Abwicklung auf einen gültigen Wert oder eine gültige Eingabe referenzieren.[701] Gibt es diesen Wert nicht, dann kann der Smart Contract auch nichts automatisch abwickeln.

462 Diese Ansicht unterliegt jedoch einer Einschränkung: Wird bspw. ein Token eingesetzt, der einen Wert repräsentiert, den es tatsächlich nicht gibt, dieser Token aber gültig in der Blockchain transferierbar ist, dann ist die Ausführung eines Smart Contract mit einem unmöglichen Vertragsinhalt möglich.[702]

463 Die Folge eines unmöglichen Vertragsinhalts ist auch bei Smart Contracts die Nichtigkeit des Vertrages gem. Art. 20 OR. In diesem Zusammenhang ist die Nichtigkeit des Smart Contract aus einer praktischen Sicht in den Fällen nicht problematisch, wo keine Transaktion stattgefunden hat (vgl. N 355 ff.).

---

699 Vgl. WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 19.

700 Siehe auch MEYER/SCHUPPLI, Smart Contracts, 221.

701 WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 18.

702 Vgl. WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 19.

b) Nachträgliche Unmöglichkeit

464 Bei der nachträglichen Unmöglichkeit verhält es sich ähnlich wie bei der ursprünglichen Unmöglichkeit. Sie ist je nach Konstellation mit Hilfe von Smart Contracts vermeidbar. Der Smart Contract kann den Vertrag nicht automatisch abwickeln, wenn die referenzierten Daten oder Werte nicht mehr gültig sind oder nicht (mehr) existieren. Die Daten können nur dann nicht mehr gültig sein oder nicht mehr existieren, wenn sie sich nicht auf der Blockchain befinden oder aber auf der Blockchain gespeichert sind, tatsächlich jedoch nicht das repräsentieren, was sie vorzugeben scheinen. Dabei ist es unbeachtlich, ob es sich um eine nachträgliche objektive oder subjektive Unmöglichkeit handelt, da der Smart Contract diesbezüglich keinen Unterschied machen kann.

c) Objektive und subjektive Leistungsunmöglichkeit

465 Für die Vertragsabwicklung mit einen Smart Contract ergibt es keinen Unterschied, ob eine objektive oder subjektive Leistungsunmöglichkeit vorliegt. Entweder kann der Vertrag automatisch abgewickelt werden – oder eben nicht. Ist der Wert zum vorgegebenen Zeitpunkt vorhanden, dann wird die Transaktion durch den Smart Contract automatisch gemäss den vorgegebenen Regeln ausgeführt. Ist der Wert eine auf einer Blockchain abgespeicherte Referenz, kann diese (theoretisch) nicht ungültig werden, da einmal in die Blockchain aufgenommene Transaktionen nicht mehr abänderbar sind (vgl. N 27).

d) Unverschuldete und verschuldete Leistungsunmöglichkeit

466 Die Frage, wer über die Schuldhaftigkeit bei einer Unmöglichkeit zu befinden hat und die Berechnung der daraus resultierenden Schadenersatzfolgen vornimmt, kann mit einem Smart Contract nicht beantwortet werden. Eine Ausnahme stellt höchstens der Fall dar, dass im Rahmen der Vertragsautonomie sämtliche Haftungs- und Schadenersatzansprüche vertraglich wegbedungen oder Alternativleistungen vorgesehen wurden.[703] In

[703] Vgl. AEPPLI, ZK OR I, Art. 119 N 89; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2539; WIEGAND, BSK OR I, Art. 119 N 10.

der Lehre wird verschiedentlich vorgeschlagen, dass hierfür programmierte Schiedsstellen eingerichtet werden, die korrigierend eingreifen können.[704]

II. Positive Vertragsverletzung

467 Der Tatbestand von Art. 97 Abs. 1 OR erfasst nach dem Wortlaut nur die nachträgliche Leistungsunmöglichkeit (die Schuldnerin erfüllt ihre Leistungspflicht nicht oder nicht gehörig), der Anwendungsbereich wurde jedoch von Lehre und Rechtsprechung erweitert und unter dem Begriff der positiven Vertragsverletzung zusammengefasst.[705] Der Begriff der positiven Vertragsverletzung umfasst auch die Schlechtleistung, Verletzung von Nebenpflichten, den antizipierten Vertragsbruch sowie die Verletzung einer Unterlassungspflicht.[706]

1. Allgemeine Regeln

468 Eine Schlechtleistung liegt vor, wenn die Schuldnerin den Vertrag erfüllt, diese Erfüllung jedoch nicht vertragskonform ist.[707] Die Schlechtleistung ist eine Verletzung der vertraglichen Hauptpflicht.[708] Das Verhältnis von Art. 97 Abs. 1 OR zu den Regeln im Besonderen Teil wird vom Bundesgericht

---

704 KAULARTZ/HECKMANN, Smart Contract, N 624; ROON, Schlichtung und Blockchain, 363; WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 28.

705 BERGER, Allgemeines Schuldrecht, N 1741; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2616; SCHWENZER, OR AT, N 67.01.

706 Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2483; SCHWENZER, OR AT, N 67.01.

707 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2627; SCHWENZER, OR AT, N 67.03.

708 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2627; SCHWENZER, OR AT, N 67.04 f.

unterschiedlich beantwortet; je nachdem besteht zwischen den Regelungen eine Alternativität.[709]

469 Ebenfalls zur positiven Vertragsverletzung gehört die Verletzung einer Nebenpflicht. Nebenpflichten eines Vertrages sind nicht eigenständig einklagbar (ausser es handelt sich um eine Nebenleistungspflicht).[710] Eine Verletzung derselben kann jedoch unter Art. 97 Abs. 1 OR geltend gemacht werden;[711] ihre Verletzung ist nicht isoliert zu betrachten, sondern kann Einfluss auf die gehörige Erbringung der Hauptleistung haben.[712] Die Nebenpflichten können vertraglich vereinbart, direkt aus dem Gesetz abgeleitet oder aber durch die Lehre und Rechtsprechung entwickelt werden (bspw. Verhaltenspflichten: Obhuts- und Schutzpflichten, Informations- und Aufklärungspflichten, Verschaffungs- und Mitwirkungspflichten).[713]

470 Der antizipierte Vertragsbruch (Verletzung der Pflicht der Parteien, alle Handlungen zu unterlassen, welche geeignet sind, den Vertragszweck zu gefährden oder zu vereiteln) wird den positiven Vertragsverletzungen zugeordnet.[714] Dabei werden jedoch die Verzugsregeln von Art. 107 ff. OR analog oder direkt angewendet.[715]

---

709 Zu den einzelnen Vertragsverhältnissen vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2629 ff.

710 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2638 f.; SCHWENZER, OR AT, N 68.05 (Erfüllung von leistungsbezogenen Nebenpflichten u.U. selbständig erzwingbar); WIEGAND, BSK OR I, Art. 97 N 32 (erzwingbar, wenn es sich um eine Nebenleistungspflicht handelt).

711 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2638; SCHWENZER, OR AT, N 68.05.

712 BERGER, Allgemeines Schuldrecht, N 1756.

713 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2643 ff.; vgl. BERGER, Allgemeines Schuldrecht, N 1756 f.

714 SCHWENZER, OR AT, N 97.09; WEBER, BK OR, Art. 97 N 59; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2651.

715 BERGER, Allgemeines Schuldrecht, N 1662, 1692; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2651.

471 Die Verletzung einer Unterlassungspflicht (Art. 98 Abs. 2 OR), welche auch zu den positiven Vertragsverletzungen zählt, kann aus einer ausdrücklichen Vereinbarung oder auch stillschweigend entstehen.[716] Sie kann sich mit der Schlechtleistung überschneiden und führt nicht immer zu einer Leistungsunmöglichkeit, weshalb sie zu den positiven Vertragsverletzungen hinzugerechnet wird.[717]

2. Positive Vertragsverletzung bei Smart Contracts

472 Ist die zu erbringende Leistung der Schuldnerin mit vordefinierbaren Parametern im Code hinterlegt, überprüft der Smart Contract die Einhaltung dieser Parameter vor der Vertragsabwicklung. Somit sollte eine Schlechtleistung rechtzeitig erkannt und der Vertrag nicht abgewickelt werden. Ist z.B. eine gewisse Menge oder eine gewisse Qualität vereinbart und meldet das Orakel nicht die Bestätigung der Menge oder Qualität, dann wird der Smart Contract nicht ausgeführt. Die Schuldnerin kann durch diese Nichtausführung des Vertrages aber in Verzug geraten (vgl. nachfolgend N 476 ff.).

473 Die Verletzung einer Nebenpflicht, ein antizipierter Vertragsbruch oder die Verletzung einer Unterlassungspflicht kann mit der Hilfe eines Smart Contract nicht grundsätzlich verhindert werden, da menschliches Verhalten nicht abschliessend voraussehbar und somit auch nicht mit Hilfe von Programmlogik abbildbar ist. Um die automatische Abwicklung eines Smart Contract zu behindern, muss das menschliche Verhalten jedoch dort einen Einfluss auf die Vertragsabwicklung haben, wo die Computerlogik eine Abweichung vom ursprünglich Vereinbarten nicht verifizieren, resp. nicht bemerken kann.

474

716 WIEGAND, BSK OR I, Art. 98 N 9.

717 BERGER, Allgemeines Schuldrecht, N 1644; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2652.

Eine positive Vertragsverletzung kann demnach auch bei Smart Contracts nicht gänzlich ausgeschlossen werden, doch sollte sie zumindest im Regelfall nicht eintreffen.[718]

III. Spätleistung

Eine Spätleistung kann aus einem Schuldnerverzug oder aus einem Gläubigerverzug resultieren. Beim Einsatz von Smart Contracts sind Leistungsverzögerungen aufgrund der Abhängigkeit der Rechenleistung vom gesamten Netzwerk zu bedenken, da die Transaktionsgeschwindigkeit je nach verwendetem Netzwerk sehr unterschiedlich ist.[719] 475

1. Allgemeine Regeln

Schuldnerverzug liegt im Gegensatz zur Unmöglichkeit dann vor, wenn trotz der Möglichkeit der Leistung nicht geleistet wird.[720] Voraussetzungen des Schuldnerverzugs sind gem. Art. 102 OR Fälligkeit und Mahnung (oder ein bestimmter Verfalltag).[721] Fälligkeit bedeutet, dass die Schuldnerin die 476

---

718 Vgl. WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 20.

719 Bei der Ethereum-Blockchain bspw. beträgt die Transaktionsgeschwindigkeit 10-20 Transaktionen pro Sekunde; bei der Bitcoin-Blockchain beträgt sie drei pro Sekunde. Zum Vergleich: *VISA* kann ca. 47'000 Transaktionen pro Sekunde abwickeln (PLOOM, Blockchains, 123 f.). Von der Transaktionsgeschwindigkeit ist die Blockbildung durch die Miner zu unterscheiden. Bei der Ethereum-Blockchain wird ca. alle 12 Sekunden ein neuer Block gebildet, bei der Bitcoin-Blockchain dauert dies zehn Minuten (PLOOM, Blockchains, 146).

720 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2658; SCHWENZER, OR AT, N 65.02.

721 BERGER, Allgemeines Schuldrecht, N 1650; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2659 f; WEBER, BK OR, Art. 102 N 50, 53; WIEGAND, BSK OR I, Art. 102 N 3.

Leistung erbringen muss; der Zeitpunkt ergibt sich aus dem Vertrag, den Umständen oder aus dem Gesetz.[722] Rechtsfolgen des Schuldnerverzugs sind in Art. 103-109 OR geregelt. Überdies besteht ab Eintritt der Fälligkeit grundsätzlich die Klagemöglichkeit der Gläubigerin auf Erfüllung des Vertrages.[723] Die Schuldnerin schuldet im Falle eines Schuldnerverzuges Ersatz des Verspätungsschadens (Art. 103 Abs. 1 OR, Art. 106 Abs. 1 OR), Haftung für Zufall (Art. 103 Abs. 1 OR) sowie Verzugszinsen bei Geldschulden (Art. 104 Abs. 1 OR).[724] Bei synallagmatischen Verträgen[725] steht nach Art. 107 Abs. 2 OR der Gläubigerin ein Wahlrecht zu; sie kann auf die Erfüllung beharren und zusätzlich Verzugsschaden geltend machen, Schadenersatz wegen Nichterfüllung fordern oder vom Vertrag zurücktreten.[726]

477 Ein Gläubigerverzug ist keine Vertragsverletzung, sondern eine Verletzung einer Obliegenheit, weshalb ein Verschulden der Gläubigerin auch nicht vorausgesetzt ist.[727] Liegt ein Gläubigerverzug vor, dann schliesst das einen Schuldnerverzug aus.[728] Eine Gläubigerin kommt gem. Art. 91 OR dann in

---

722 BERGER, Allgemeines Schuldrecht, N 1653 ff.; SCHWENZER, OR AT, N 65.02 f; vgl. WEBER, BK OR, Art. 102 N 54.

723 BERGER, Allgemeines Schuldrecht, N 1665; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2667.

724 Vgl. BERGER, Allgemeines Schuldrecht, N 1665; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2667 ff.; SCHWENZER, OR AT, N 66.02 ff.

725 Nach h.L. auch dann, wenn die Schuldnerin mit einer wesentlichen Vertragspflicht in Verzug kommt, vgl. BERGER, Allgemeines Schuldrecht, N 1683.

726 BERGER, Allgemeines Schuldrecht, N 1684; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2702; SCHWENZER, OR AT, N 66.23 ff.; THÉVENOZ, CR CO I, Art. 107 N 26 ff.; WIEGAND, BSK OR I, Art. 107 N 3, 13 ff.

727 BERGER, Allgemeines Schuldrecht, N 1283, 1288; BERNET, BSK OR I, Art. 91 N 13; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2430; SCHWENZER, OR AT, N 69.10.

728 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2664; SCHWENZER, OR AT, N 65.03.

Verzug, wenn sie die gehörig angebotene Leistung der Schuldnerin in ungerechtfertigter Weise verweigert.[729] Bei einem Gläubigerverzug haftet die Gläubigerin für den Zufall, schuldet der Schuldnerin Ersatz für allfällige Mehraufwendungen bei Hinterlegung (vgl. Art. 92 OR) und kann die Einrede des nicht erfüllten Vertrages gem. Art. 82 OR der Schuldnerin nicht entgegenhalten.[730] Der Schuldnerin steht es überdies zu, den Leistungsgegenstand zu verwerten (Art. 93 OR) oder vom Vertrag zurückzutreten (Art. 95).[731]

2. Spätleistung bei Smart Contracts

478 Spätleistungen sollten beim Einsatz von Smart Contracts grundsätzlich nicht auftreten, da insbesondere bei synallagmatischen Verträgen Leistung und Gegenleistung in Abhängigkeit voneinander ausgetauscht, resp. durch den Smart Contract zeitgleich ausgeführt werden.[732]

479 Wenn jedoch ein Fall der Schlechtleistung vorliegt (z.B. fehlende Qualität einer Ware, die mittels Sensoren überprüfbar ist und direkt dem Smart Contract gemeldet wird (vgl. hiervor N 472), und der Smart Contract aufgrund dessen die Vertragsabwicklung nicht durchführt (resp. nicht durchführen kann), dann könnte dennoch ein Fall der Spätleistung vorliegen.

---

729 Die Schuldnerin muss die Leistung in sachlicher, persönlicher, örtlicher und zeitlicher Hinsicht korrekt und frei von Bedingungen anbieten sowie die Gläubigerin zur Annahme auffordern, vgl. BERGER, Allgemeines Schuldrecht, N 1289 ff.; BERNET, BSK OR I, Art. 91 N 3 ff.

730 BERGER, Allgemeines Schuldrecht, N 1301 ff.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2434 ff.; SCHWENZER, OR AT, N 70.03 ff.

731 BERGER, Allgemeines Schuldrecht, N 1308 ff.; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 2451 ff.; SCHWENZER, OR AT, N 70.09 ff.

732 WEBER, Leistungsstörungen und Rechtsdurchsetzungen bei Smart Contracts, N 20.

IV. Fazit

480 Leistungsstörungen sind ein äusserst komplexes Thema. Mit dem Einsatz von Smart Contracts könnten Leistungsstörungen, insbesondere wo virtuelle Güter ausgetauscht werden, teilweise vermieden werden.

481 Prinzipiell ist zu unterscheiden, ob der Smart Contract auf Daten referenziert, die in der Blockchain gespeichert sind und so grundsätzlich vorhanden und nach der internen Logik der Blockchain gültig sind oder ob auf externe Daten zugegriffen wird. Sofern sich die vertraglichen Abmachungen allesamt auf Daten beziehen, die auf einer Blockchain abrufbar sind, können Leistungsstörungen grundsätzlich vermieden werden.

482 Sobald aber das Gefüge der Blockchain verlassen und auf Daten ausserhalb (virtuell oder reell) verwiesen wird, besteht die Gefahr, dass eine Leistungsstörung trotz automatisierter Vertragsabwicklung eintreten kann. Dies betrifft insbesondere die Unmöglichkeit einer Leistung, die durch einen an sich gültig transferierbaren Token ausgelöst wird, der einen nicht vorhandenen oder nicht gültigen Wert repräsentiert. Schlechtleistungen können vermieden werden, wenn die vertragliche Leistung mit messbaren Parametern durch den Smart Contract überprüfbar ist. Führt ein Smart Contract aufgrund der Nichterfüllung der erforderlichen Parameter einen Vertrag nicht aus, dann kann dies einen Schuldnerverzug auslösen. Möglich ist eine Leistungsstörung auch aufgrund der Verletzung einer Verhaltenspflicht, da menschliches Verhalten von Programmlogik nicht erfassbar ist.

E. Gewährleistung und Haftung

483 Es sind verschiedene Konstellationen denkbar, in denen Gewährleistung und Haftung im Zusammenhang mit Smart Contracts eine Rolle spielen können. Erstens können sich Gewährleistungs- und Haftungsfragen direkt aus dem Grundverhältnis der Vertragsparteien ergeben. Hierauf wird nachfolgend nicht näher eingegangen, da die Fragen jeweils anhand des konkreten Vertragsverhältnisses beurteilt werden müssen.

484 Zweitens stellen sich Gewährleistungs- und oder Haftungsfragen, wenn ein Smart Contract fehlerhaft programmiert ist (einen sog. *Bug*[733] enthält) und dadurch allenfalls ein Schaden entsteht. Es ist zu prüfen, ob der Softwareentwickler dafür einzustehen hat.

485 Drittens besteht die Möglichkeit, dass ein Schaden durch eine falsche Anwendung des Smart Contract durch eine der Parteien entsteht. Dies wäre beispielsweise dann der Fall, wenn die fehlerlose, vorprogrammierte Software durch die Parteien mit falschen Informationen bestückt wird und dadurch ein Schaden entsteht. Der Schaden kann dabei direkt bei einer Vertragspartei oder auch bei einem Dritten eintreten.

I. Fehler in der Software (Bug)

486 In der Praxis sehr häufig sind Fehler im Code eines Smart Contract, die in der Folge teilweise Schäden in mehrstelliger Millionenhöhe verursachen.

487 Wird durch einen Fehler im Quellcode eines Smart Contract ein Schaden verursacht, dann stellt sich die Frage, wer diesen zu verantworten hat. Smart Contracts stehen in aller Regel unter einer OSS-Lizenz (vgl. N 108 ff.). Es besteht auch die Möglichkeit, dass ein Smart Contract proprietär für eine Partei

---

733 Im Zusammenhang mit Software und Computern wird der Begriff *Bug* zur Bezeichnung von Fehlern verwendet. Diese Begrifflichkeit stammt angeblich aus den Zeiten, als noch Röhrenrechner im Einsatz waren und Wanzen (oder Motten) in den Schaltkreisen für Rechenausfälle sorgten (vgl. HEROLD/LURZ/WOHLRAB/HOPF, Grundlagen der Informatik, 142.

entwickelt worden ist (vgl. N 121). In der Folge wird untersucht, wem gegenüber im Fall von fehlerhaft programmierter Software Haftungsansprüche geltend gemacht werden können.

1. Vertragliche Gewährleistung und Haftung

488 Es ist zu unterscheiden, ob der Smart Contract unter einer OSS-Lizenz vertrieben oder aufgrund eines Softwarevertrages proprietär entwickelt wurde.

a) OSS-Lizenz

489 OSS-Lizenzen enthalten in der Regel umfassende Haftungs- und Gewährleistungsausschlüsse. Es sind jeweils die entsprechenden Lizenzbestimmungen zu prüfen. Der Smart Contract von Ethereum ist unter der GNU-GPL-3.0 veröffentlicht, der Chaincode von Hyperledger unter Apache-Lizenz 2.0. Es ist hierbei zu beachten, dass Smart Contracts laufend weiterentwickelt werden und bei jedem einzelnen initiierten Smart Contract zu prüfen ist, ob und falls ja, unter welcher OSS-Lizenz er vertrieben wurde.

490 Grundsätzlich enthalten die GNU-GPL-3.0 und die Apache-Lizenz 2.0 umfassende Haftungs- und Gewährleistungsausschlüsse.[734] Zudem enthält die GNU-GPL-3.0 eine Klausel, nach der das am weitest gehende Haftungs- und Gewährleistungsausschlussrecht zur Anwendung gelangt, sollten unter dem anwendbaren Recht die Gewährleistungs- und Haftungsausschlussklauseln nicht gültig sein. Ob Gewähr- und Haftungsfreizeichnungsklauseln nach Schweizer Recht erlaubt sind, ist je nach Vertragsverhältnis zu entscheiden. Wird den allgemeinen Regeln des Obligationenrechts gefolgt, dann sind Haftungsfreizeichnungsklauseln grundsätzlich zulässig, mit Ausnahme des Ausschlusses von Absicht und grober Fahrlässigkeit (Art. 100 Abs. 1 OR),[735] sowie dem Ausschluss bestimmter Vertragsverhältnisse (Art. 100 Abs. 2

[734] Vgl. Ziff. 15 und 15 GNU-GPL-3.0 sowie Ziff. 8 und 9 Apache-Lizenz 2.0; vgl. Kapitel C. II., N 108 ff.

[735] THÉVENOZ, CR CO I, Art. 100 N 15, 21; WIEGAND, BSK OR I, Art. 100 N 4.

und 3).[736] Ob eine umfassende Freizeichnungsklausel auf das erlaubte Mass reduziert wird oder gänzlich ungültig ist, ist in der Lehre umstritten, wobei mehrheitlich die Reduktion der Haftungsbeschränkung auf das erlaubte Mass befürwortet wird.[737]

491 Wie im ersten Teil der Arbeit ausgeführt, wird vorliegend davon ausgegangen, dass es sich bei einer OSS-Lizenz um einen unentgeltlichen Softwarelizenzvertrag handelt, bei dem die Grundsätze für den Softwarelizenzvertrag sowie die allgemeinen Grundsätze des Obligationenrechts anzuwenden sind (N 149).

492 Die Haftungsfreizeichnungsklauseln in den vorerwähnten OSS-Lizenzen würden demgemäss nach den Regeln des OR AT beurteilt. Die Freizeichnungsklauseln wären grundsätzlich gültig, aber nach h.L. bliebe die Haftung gem. Art. 100 Abs. 1 OR für Absicht oder grobe Fahrlässigkeit bestehen.[738] Das gleiche Ergebnis ergibt sich auch dann, wenn der Lehrmeinung gefolgt wird, die bei OSS-Lizenzverträgen für die Anwendung von Schenkungsrecht (Art. 248 Abs. 1 OR) plädiert (N 138).

493 Auch ein Gewährleistungsausschluss ist grundsätzlich möglich; es sind jedoch auch hier je nach Qualifikation des Vertrages die entsprechenden Sondervorschriften zu beachten. So ist bspw. ein Gewährleistungsausschluss bei Kaufverträgen möglich, jedoch nicht im Fall von arglistigem Verschweigen von Mängeln (vgl. Art. 199 OR).[739] Vorliegend kommt allerdings kein Kaufvertragsrecht zur Anwendung. Wird der Lehre zur Anwendung von

---

736 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3090 ff.; SCHWENZER, OR AT, N 24.10 ff.; THÉVENOZ, CR CO I, Art. 100 N 25 ff.; WIEGAND, BSK OR I, Art. 100 N 8 ff.

737 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3082 (geltungserhaltende Reduktion); SCHWENZER, OR AT, N 24.08 (Ungültigkeit der Klausel, umfassende Haftung, auch für leichte Fahrlässigkeit); THÉVENOZ, CR CO I, Art. 100 N 21 (geltungserhaltende Reduktion); WIEGAND, BSK OR I, Art. 100 N 4 (geltungserhaltende Reduktion).

738 Siehe FN 737.

739 Vgl. HONSELL, BSK OR I, Art. 199 N 7 f.; zum Verhältnis von Art. 100 zu 199 OR siehe GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3086; THÉVENOZ, CR CO I, Art. 100 N 32.

Schenkungsrecht bei OSS-Lizenzverträgen gefolgt, gilt die Gewähr nur dann, wenn sie versprochen wurde (vgl. Art. 248 OR).[740]

494 Kann keine OSS-Lizenz eruiert werden und besteht zwischen dem Entwickler und dem Nutzer der fehlerhaften Software kein vertragliches Verhältnis, bleibt zu klären, ob der Softwareentwickler aufgrund des Deliktsrechts haftbar sein könnte (vgl. nachfolgend N 496 ff.). Das Vorliegen eines OSS-Lizenzvertragsverhältnisses wird wohl in der Regel nicht anzunehmen sein, da dieses erst dann zustande kommen kann, wenn die Nutzung über den bestimmungsgemässen Gebrauch hinaus geht (N 129).

b) Übrige Softwareverträge

495 Wurde der Smart Contract für eine Partei entwickelt und ein Softwarevertrag abgeschlossen, dann richten sich die Gewähr- und Haftungsfragen nach diesem Vertrag. Grundsätzlich gilt auch hier, dass als Voraussetzung für die vertragliche Haftung seitens des Softwareentwicklers ein Schaden, ein Verschulden sowie ein Kausalzusammenhang vorliegen muss.[741]

---

740 VOGT/VOGT, BSK OR I, Art. 248 N 3; WEBER, Open Source Software, 89.

741 Ausführlich zur Haftung bei Softwareverträgen FISS, Haftung für fehlerhafte Software, 34 ff.; FRÖHLICH-BLEULER, Softwareverträge, N 1205 ff.

2. Deliktische Haftung

496 Die bereits mehrfach erwähnten OSS-Lizenzen enthalten meist Haftungsfreizeichnungsklauseln, welche sich explizit auch auf die ausservertragliche Haftung beziehen (bspw. Ziff. 16 GNU-GPL-3.0 sowie Ziff. 8 Apache-Lizenz 2.0).

497 Eine deliktische Haftung kann sich aus einem Verschulden (Art. 41 Abs. 1 OR) oder aus einer Kausalhaftung (z.B. Geschäftsherrenhaftung oder Produktehaftpflichtgesetz[742]) ergeben.[743]

a) Verschuldenshaftung nach Art. 41 ff. OR

498 Die ausservertragliche Haftung nach Art. 41 OR ist eine Verschuldenshaftung; sie greift also nur, wenn der Schädiger vorsätzlich oder fahrlässig handelt.[744] Gegenüber spezialgesetzlichen Regelungen tritt die Haftung nach Art. 41 OR zurück.[745] Voraussetzung für die Haftung nach Art. 41 OR ist ein Schaden, Widerrechtlichkeit, ein Verschulden sowie ein Kausalzusammenhang.[746] Reine Vermögensschäden werden durch die Haftung aus Art. 41 Abs. 1 OR nicht geschützt, ausser es wird gegen eine entsprechende Schutznorm verstossen.[747]

499 Die h.L. wie auch das Bundesgericht gehen davon aus, dass sich eine vertragliche Freizeichnungsklausel auch auf die deliktische Haftung auswirkt.[748] Steht ein Smart Contract mit einer fehlerhaften Programmierung also unter einer OSS-Lizenz, die eine Haftungsfreizeichnungsklausel enthält, dann kann sich diese Freizeichnung auch für die deliktische Haftung

---

742 Bundesgesetz über die Produktehaftpflicht (Produktehaftpflichtgesetz, PrHG) vom 18. Juni 1993, SR 221.112.944.

743 BERGER, Allgemeines Schuldrecht, N1840, 1887.

744 KESSLER, BSK OR I, Art. 41 N 1; SCHWENZER, OR AT, N 49.07.

745 KESSLER, BSK OR I, Art. 41 N 1a.

746 KESSLER, BSK OR I, Art. 41 N 2c; SCHWENZER, OR AT, N 50.01; BERGER, Allgemeines Schuldrecht, N 1840.

747 Vgl. BERGER, Allgemeines Schutzrecht, N 1843, KESSLER, BSK OR I, Art. 41 N 13.

748 BGE 120 II 58 E. 3 S. 61; KESSLER, BSK OR I, Art. 41 N 2; SCHWENZER, OR AT, N 5.05; WERRO, CR CO I, Intro. Art.41-61, N 10.

auswirken. Die praktischen Auswirkungen der vertraglichen Freizeichnungsklauseln auf eine allfällige deliktische Haftung sind jedoch fraglich. Es ist anhand des Einzelfalls zu entscheiden, ob der Fehler in der Software absichtlich oder fahrlässig passiert ist und so allenfalls eine deliktische Haftung begründet werden kann. Daneben muss aber auch der Schaden, die Widerrechtlichkeit, sowie die Kausalität nachgewiesen werden (N 498). Bei allfälligen Schäden aus einem fehlerhaft programmierten Smart Contract dürften reine Vermögensschäden die Regel sein; hierzu müsste durch den Softwareentwickler eine entsprechende Schutznorm verletzt worden sein (vgl. N 498).

500 Wird der Lehrmeinung gefolgt, die bei einer OSS-Lizenz Schenkungsrecht analog anwendet (vgl. N 138), ist fraglich, ob die Freizeichnungsklausel, resp. die Haftungsmilderung in Art. 248 Abs. 1 OR auch auf das Deliktsrecht anwendbar ist. WEBER schlägt diesbezüglich eine differenzierte Vorgehensweise vor: Eine gänzliche Freizeichnung des Schenkers von der deliktischen Haftung könne nicht angenommen werden, jedoch sei eine Haftungsreduktion gem. Art. 99 Abs. 2 bzw. Art. 43/33 OR aufgrund der Freigiebigkeit des Schenkers angezeigt.[749]

b) Geschäftsherrenhaftung

501 Im Gegensatz zu Hilfspersonenhaftung (vgl. N 188) bezieht sich die Geschäftsherrenhaftung auf Handlungen der Hilfsperson, die sich im ausservertraglichen Bereich abspielen; es handelt sich um eine Haftung für unerlaubte Handlungen der Hilfsperson.[750] Verlangt wird für die Haftung nach Art. 55 OR nebst Schaden und Kausalität auch der Nachweis der Widerrechtlichkeit.[751] Beim Exzeptionsbeweis muss der Geschäftsherr

---

749 WEBER, Open Source Software, 90.

750 GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 3072; KESSLER, BSK OR I, Art. 55 N 1; SCHWENZER, OR AT, N 23.12.

751 SCHWENZER, OR AT, N 23.14, vgl. BERGER, Allgemeines Schuldrecht, N 1892.

nachweisen, dass er die nach den Umständen gebotene Sorgfalt angewendet hat, um den tatsächlichen Schaden zu verhüten.[752]

502 Die Hilfsperson ist eine dem Geschäftsherrn hierarchisch untergeordnete Person.[753] Dabei wird von natürlichen Personen ausgegangen. Ein durch einen Smart Contract ausservertraglich verursachter Schaden kann folglich nicht als Hilfsperson des Geschäftsherrn subsumiert werden, da dem Smart Contract als Software keine eigene Rechtspersönlichkeit zukommt (vgl. N 239).

c) Produktehaftung

503 Das Produktehaftpflichtgesetz (PrHG) regelt die Ansprüche für Schäden durch ein fehlerhaftes Produkt. Darunter fallen Personenschäden oder Sachschäden an Gegenständen zum privaten Gebrauch (Art. 1 PrHG). Reine Vermögensschäden werden durch das PrHG jedoch nicht gedeckt.[754] Zwischen Ansprüchen aus dem Produktehaftpflichtgesetz und Art. 55 OR besteht Anspruchskonkurrenz; Art. 55 OR kommt grundsätzlich dann zur Anwendung, wenn das PrHG Schutzlücken aufweist (bspw. bei Schäden am Produkt selbst).[755]

504 Ein Produkt nach Art. 3 PrHG ist grundsätzlich eine bewegliche, körperliche Sache. Vorab ist dabei an bewegliche Sachen (Konsumgüter jeder Art) zu denken, die von Menschen hergestellt und in Verkehr gesetzt wurden.[756] Keine Produkte im Sinne des PrHG sind Dienstleistungen.[757] Es herrscht keine abschliessende Einigkeit darüber, ob geistige Leistungen eine gewisse Körperlichkeit erlangen müssen, um als Produkte qualifiziert zu werden. Und auch bei der Erlangung einer gewissen Körperlichkeit besteht überdies keine Einigung darüber, ob ein allfälliger Schaden sich aus der Verkörperung der geistigen Leistung ergeben muss oder ob die Verkörperung und dessen Inhalt

---

752 KESSLER, BSK OR I, Art. 55 N 16; SCHWENZER, OR AT, N 23.22; BERGER, Allgemeines Schuldrecht, N 1894.

753 KESSLER, BSK OR I, Art. 55 N 7; BERGER, Allgemeines Schuldrecht, N 1891.

754 FELLMANN, BSK OR I, Art. 1 PrHG N 2; SCHWENZER, OR AT, N 53.40.

755 KESSLER, BSK OR I, Art. 55 N 3a.

756 FELLMANN, BSK OR I, Art. 3 PrHG N 3; HESS, SHK PrHG, Art. 3 N

757 HESS, SHK PrHG, Art. 3 N 24.

sich nicht trennen lassen.[758] Diese Diskussion lässt sich auch auf die Qualifizierung von Software als Produkt übertragen. Hier herrscht ebenfalls keine Einigkeit darüber, ob Software ohne die Einbettung in ein Gerät für sich selbst ein Produkt gem. PrHG darstellt.[759] FELLMANN differenziert danach, ob es sich um eine Standard-Software oder um eine Individual-Software handelt. Bei letzterer überwiege der Dienstleistungscharakter und daher sei zumindest Individual-Software nicht als Produkt zu qualifizieren.[760] Eine Standard-Software, die auf einer „Diskette" erworben werde, stelle ein Produkt im Sinne von Art. 3 Abs. 1 lit. a PrHG dar.[761]

505 Um unter das PrHG zu fallen, müssten Smart Contracts in einem ersten Schritt als Produkt qualifiziert werden. Da Smart Contracts, wie vorhergehend ausgeführt, nicht als körperliche Sache, sondern als Software zu klassifizieren sind (N 239) und nicht auf Datenträgern verkörpert oder fest in Geräte (Hardware) eingebettet sind, fallen sie nicht in den Anwendungsbereich des Produktehaftpflichtgesetzes.[762]

---

758 FELLMANN, BSK OR I, Art. 3 PRHG N 9.

759 FELLMANN, BSK OR I, Art. 3 PrHG N 10; HESS, SHK PrHG, Art. 3 N 31.

760 FELLMANN, BSK OR I, Art. 3 PrHG N 10.

761 FELLMANN, BSK OR I, Art. 3 PrHG N 10; a.A. HESS, SHK PrHG, Art. 3 N 34.

762 Sollte sich in der aktuellen Diskussion um die rechtliche Einordnung von Daten, insbesondere auch im Zusammenhang mit Daten auf der Blockchain (bspw. Token) die Meinung durchsetzen, dass Daten wie Sachen zu behandeln seien, dann wäre zu prüfen, ob Software, die nicht fest mit Geräten verbunden ist, ebenfalls als Sache zu behandeln wäre und eine analoge Anwendung des PrHG angebracht sein könnte (ablehnend zu Open Source Software unter PrHG LAUX/WIDMER, Produkthaftung, 499 ff.; zu Daten als Sache siehe ECKERT, Besitz und Eigentum an digitalen Daten, 246 ff.; ECKERT, digitale Daten als Sache, 265 ff.; GRAHAM-SIEGENTHALER/FURRER, Blockchain Technology and Bitcoin, N 45 ff.).

II. Fehlerhafte Anwendung des Smart Contract

506 Kommt ein Schaden nicht durch einen Fehler in der Software selbst, sondern durch eine fehlerhafte Anwendung derselben zustanden, ist zu prüfen, ob die fehlhafte Anwendung einer Partei direkt zugerechnet werden kann. Eine fehlerhafte Anwendung eines Smart Contract kann sich – soweit ersichtlich – nur in einem Fall manifestieren: Eine der Vertragsparteien passt einen standardisierten Smart Contract den vertragsgemässen Vereinbarungen an (d.h. individualisiert den Smart Contract) und dabei passiert ein (Eingabe- oder Bedienungs-) Fehler. Resultiert aus diesem Fehler ein Schaden bei einer der Vertragsparteien, dann ist zu prüfen, ob es sich bei der Individualisierung des Smart Contract um eine vertragliche Pflicht gehandelt hat und welche Ansprüche aus dem Vertrag abgeleitet werden können. Resultiert ein Schaden bei einem Dritten, dann steht dem Dritten allenfalls ein Anspruch aus Deliktshaftung zu.

1. Vertragliche Haftung

507 Das Aufsetzen oder Anpassen eines Smart Contract kann sich aus einer vertraglichen Verpflichtung ergeben; die Folge der fehlerhaften Anwendung könnte sich in einer Leistungsstörung, resp. einem Schaden für eine der Vertragsparteien manifestieren. Auf eine Prüfung, ob einem Smart Contract eine Hilfspersonenstellung zukommt, kann aufgrund der fehlenden Rechtspersönlichkeit eines Smart Contract verzichtet werden. Dies entspricht auch der h.L, nach der auch Maschinen, Apparaten und Tieren (sowie intelligenten Robotern[763]) eine Hilfspersonenstellung abgesprochen wird.[764]

---

763 Intelligente Roboter sind nichts anderes als Software, die je nach gewünschter Funktionalität in einem Gehäuse verbaut oder mit einem solchen verbunden ist: vgl. LOHMANN, Roboter, 154 f., 159 ff.

764 WIEGAND, BSK OR I, Art. 101 N 9.

508 Wird vertraglich vereinbart, dass eine der beteiligten Parteien den Smart Contract für die Vertragsabwicklung aufsetzt, dann ist im Einzelfall zu prüfen, ob dies ein wesentlicher Vertragsbestandteil oder eine Nebenpflicht des Vertrages war. Wird das Grundgeschäft direkt als Smart Contract aufgesetzt, dann kann die Annahme getroffen werden, dass die Programmierung oder die Individualisierung eines (Standard-) Smart Contract einen wesentlichen Vertragspunkt darstellt. Die Folge der Verletzung eines wesentlichen Vertragsbestandteils richtet sich nach der daraus resultierenden Leistungsstörung (vgl. vorhergehend N 446 ff.).

509 Aber auch wenn das fehlerhafte Aufsetzen des Smart Contract durch eine der Vertragsparteien lediglich die Verletzung einer Nebenpflicht darstellt, stellt dies eine positive Vertragsverletzung dar und kann Schadenersatzansprüche auslösen (vgl. N 467 ff.).

510 Hat der Fehler einen Einfluss auf die geschuldete Leistung i.S. einer Schlechtleistung, dann entscheiden sich die allfälligen Gewährleistungsrechte nach dem Grundgeschäft zwischen den Parteien. Hier ist jedoch zu prüfen, ob der Fehler einen Einfluss auf die Schlechtleistung derjenigen Partei hat, die den Smart Contract fehlerhaft angewendet hat oder auf die Leistung der anderen Partei, da im letzten Fall ein Verschulden der Partei entfällt. Gleiches gilt für einen allfälligen Schaden, der aus der fehlerhaften Anwendung bei der anderen Partei eintritt.

2. Deliktische Haftung

511 Ob ein Dritter, für den ein Schaden aufgrund einer fehlerhaften Anwendung eines Smart Contract resultiert, einen Anspruch aus Art. 41 Abs. 1 OR geltend machen kann, ist im Einzelfall unter Prüfung der einzelnen Tatbestandsmerkmale (Schaden, Widerrechtlichkeit, Verschulden, Kausalität, vgl. N 498) abzuklären. Im Gegensatz zu einem Schaden, der aus einer fehlerhaften Software (vgl. N 486 ff.) resultiert und bei dem aufgrund der Freizeichnungsklauseln in den OSS-Lizenzen nur bei Absicht oder grober Fahrlässigkeit auf die Softwareentwickler Rückgriff genommen werden kann (N 499 f.), besteht bei einem Schaden aufgrund einer Fehlanwendung keine Haftungseinschränkung durch eine OSS-Lizenz. Im Ergebnis ist jedoch bei

beiden Konstellationen gem. Art. 41 Abs. 1 OR ein Vorsatz oder eine Fahrlässigkeit nachzuweisen. Handelt es sich bei dem Schaden um einen reinen Vermögensschaden, was im Zusammenhang mit Smart Contracts wohl die Regel darstellen wird, dann ist zu prüfen, ob die Parteien durch die fehlerhafte Anwendung des Smart Contract gegen eine das Vermögen schützende Norm verstossen haben (vgl. N 498).

512 Zur Geschäftsherrenhaftung gem. Art. 55 OR kann auf die Ausführungen im vorangehenden Kapitel I. Fehler in der Software (Bug), 2. Deliktische Haftung (N 496 ff.) verwiesen werden.

III. Fazit

513 Verursacht ein Smart Contract aufgrund einer fehlerhaften Programmierung einen Schaden und wurde dieser Smart Contract unter einer Open-Source Software-Lizenz erworben, dann könnten die oftmals umfassenden Freizeichnungsklauseln bezüglich Haftung und Gewähr nicht nur auf die vertraglichen, sondern auch auf die deliktischen Ansprüche durchgreifen. Die Freizeichnung würde jedoch auf das erlaubte Mass reduziert, d.h. es bliebe eine Haftung für Absicht und grobe Fahrlässigkeit in den vertraglichen wie auch ausservertraglichen Verhältnissen bestehen.

514 Eine Hilfspersonen- als auch Geschäftsherrenhaftung kann ausgeschlossen werden, da einem Smart Contract aufgrund der fehlenden Rechtspersönlichkeit keine Eigenschaft als Hilfsperson zukommt.

515 Wird ein Smart Contract fehlerhaft angewendet und resultiert daraus ein Schaden, kann dies als Leistungsstörung zwischen den Vertragsparteien eingeordnet werden. Gegenüber Dritten besteht allenfalls eine deliktische Haftung gem. Art. 41 ff. OR, wenn die Voraussetzungen des Schadens, der Widerrechtlichkeit, des Kausalzusammenhanges sowie des Verschuldens erfüllt werden. Da im Zusammenhang mit Smart Contracts reine Vermögensschäden im Vordergrund stehen, ist die Verletzung einer entsprechenden Schutznorm zu eruieren.

516 Eine Haftung gemäss Produktehaftpflichtgesetz ist für Smart Contracts aufgrund der fehlenden Produkteigenschaft ausgeschlossen.

F. Smart Contracts als Halter von Vermögenswerten

517 Ein Smart Contract eignet sich grundsätzlich dazu, für eine selbständige Vertragsabwicklung Vermögenswerte entgegen zu nehmen sowie diese nach Eintritt der vordefinierten Bedingungen an die vorbestimmte Partei (resp. deren Adresse) weiterzuleiten (vgl. N 250 ff.). So kann bspw. bei zweiseitigen Verträgen die vertraglich geschuldete Summe (in Kryptowährung) beim Smart Contract hinterlegt werden. Der Smart Contract überträgt sodann die vereinbarte Summe der Gegenpartei, wenn diese ihrerseits ihre vertraglich vereinbarte Leistung erbracht hat. So müssen sich einerseits die Parteien gegenseitig nicht vertrauen und andererseits kann grundsätzlich auf einen vertrauenswürdigen Intermediär wie bspw. eine Treuhänderin oder eine Bank, verzichtet werden. Nachfolgend wird nun untersucht, welche Vermögenswerte an einen Smart Contract übertragen werden können und ob das Halten dieser Vermögenswerte einem bekannten vertraglichen Konzept wie dem Treuhandverhältnis, dem Hinterlegungsvertrag, dem Escrow-Agreement oder der Sicherungszession zugeordnet werden kann.

I. Übertragung von Vermögenswerten

518 Smart Contracts eigenen sich insbesondere für das temporäre Halten und zur Übertragung von digitalen Vermögenswerten, die sich innerhalb der Blockchain befinden. Es besteht jedoch die Möglichkeit, auch andere digitale Vermögenswerte sowie Vermögenswerte ausserhalb der digitalen Welt oder gar körperliche Sachen zu übertragen. Diese Werte werden durch einen Token (vgl. Anhang, N 30 ff.) repräsentiert.

1. Arten von Vermögenswerten

519 Grundsätzlich ist es den Parteien unbenommen, jegliche Vermögenswerte auf einen Smart Contract zu übertragen (an dessen Adresse zu senden). Mit Hilfe von Token, die einen Wert, ein Recht oder eine Sache (auch ausserhalb der

Blockchain) repräsentieren können (vgl. Anhang, N 30 ff.), scheinen die Möglichkeiten nahezu unbegrenzt. Hierbei müssen jedoch zwei wesentliche Punkte beachtet werden: Erstens stellt sich die Frage, wie ein digitales oder reales Gut, eine Forderung oder ein Vermögenswert durch einen Token repräsentiert und die tatsächliche Verfügungsmacht darüber hergestellt werden kann. Zweitens ist abzuklären, welche Art von Recht, Vermögenswert oder Sache der Token repräsentiert. Handelt es sich dabei um eine dem Schweizer Recht bekannte Form einer Sache (Fahrnis oder Grundstück) oder um ein obligatorisches Recht (Forderung), ein Wertpapier, eine Bucheffekte oder einen sonstigen Vermögenswert, dann müssen die einschlägigen Regeln zur gültigen Übertragung beachtet werden, ansonsten der Übertragung auf der Blockchain-Plattform keine Rechtsgültigkeit zukommt.[765]

520 Der einfacheren Lesbarkeit halber werden nachfolgend Sachen, Forderungen, Wertpapiere, Bucheffekten und sonstige Vermögenswerte zusammenfassend unter dem Begriff *Vermögenswerte* genannt.

2. Übertragung an Smart Contract

521 Wird ein Vermögenswert an einen Smart Contract übertragen, ist dies aus rechtlicher Sicht nicht unproblematisch: Die Parteien überweisen den Vermögenswert an die Adresse des Smart Contract und nicht jeweils an die andere Vertragspartei.[766] Obwohl also faktisch der Vermögenswert an den Smart Contract überwiesen wird und so ggf. die Verfügungsmacht über den Vermögenswert (für eine bestimmte Zeit) den Parteien entzogen wird, hat diese Übertragung keine rechtlichen Konsequenzen, da der Smart Contract aufgrund

765 So bedarf es bspw. für die gültige Übertragung von Fahrniseigentum nebst einem gültigen Verpflichtungsgeschäft auch eines Besitzübergangs (Art. 714 ZGB), entweder durch Tradition oder Traditionssurrogate (z.B. Besitzesanweisung).

766 An die andere Partei wird der geschuldete Vermögenswert erst dann überwiesen, wenn die vordefinierten Bedingungen eintreten. Es besteht auch die Möglichkeit, dass der Wert an die Partei, die den Wert beim Smart Contract hinterlegt hat, zurückfällt.

seiner fehlenden Rechtspersönlichkeit keine Vertragspartei sein kann, wie bspw. ein Treuhänder oder Aufbewahrer. Erfüllen wird eine Vertragspartei ihre vertragliche Pflicht in der Regel also erst dann, wenn der Vermögenswert an die andere Partei übertragen wird und nicht dann, wenn der Vermögenswert bei einem Smart Contract hinterlegt wird. Vorbehalten sind natürlich anderslautende Parteiabreden.

522 Aus praktischer Sicht kann zudem problematisch sein, wenn die Vertragsparteien es unterlassen haben, entweder eine zeitliche Beschränkung des Smart Contract zu definieren oder nicht die Möglichkeit vorsehen, im gegenseitigen Einverständnis die Vermögenswerte wieder aus dem Smart Contract herauszulösen (z.B. mittels *Multisignaturen*[767]). In diesen Fällen können unter Umständen die Vermögenswerte aufgrund des Grundsatzes der Unabänderbarkeit des Smart Contract für immer blockiert sein – zumindest in Smart Contract, die direkt auf einer öffentlichen Blockchain implementiert sind.[768]

---

767 Multisignatur (auch *Multisig*) bedeutet, dass für die Ausführung einer Handlung (z.B. Auslösen einer Transaktion) M von N Signaturen (d.h. eine bestimmte Anzahl von hinterlegten Signaturen) notwendig sind. Dies kann einer höheren Sicherheit der Vermögensübertragung und Verhinderung von Missbrauch dienen, aber auch zur allfälligen Anpassung oder Beendigung eines Smart Contract führen. Ausführlich zu Multisig ANTONOPOULOS, Mastering Bitcoin, 149 f.; BERENTSEN/SCHÄR, Kryptoassets, 184 f.

768 Ist ein Vermögenswert tatsächlich blockiert, sodass weder die eine noch die andere Partei darüber verfügen kann, dann ist zu prüfen, ob die richtige (im Sinne von sorgfältige) Programmierung des Smart Contract eine vertragliche Pflicht einer der Parteien darstellt und gestützt darauf allenfalls eine Vertragsverletzung geltend gemacht werden kann. Ist der Wert wegen eines Fehlers in der Software blockiert, bleibt ggf. ein Rückgriff auf den Entwickler (vgl. dazu N 489 ff.).

3. Involvierte Parteien

523 Grundsätzlich kann ein Smart Contract, je nach Zweck und Einsatzmöglichkeit des verwendeten Smart Contract, von einer oder mehreren Parteien eingesetzt werden. Praktisch kommen die Vorteile eines Smart Contract insbesondere dort zur Geltung, wo er von mehreren Parteien zur automatisierten Vertragsabwicklung eingesetzt wird.[769]

II. Funktion des Smart Contract

524 Wie bereits ausgeführt, kann ein Smart Contract dazu eingesetzt werden, Vermögenswerte (kurzzeitig) zu halten und nach den vordefinierten Regeln zu transferieren. Normalerweise wird diese Funktion von Intermediären wahrgenommen, wie bspw. Escrow-Agenten oder Treuhändern. Es ist nun fraglich, ob die geltenden Regelungen auch auf Smart Contracts angewendet werden können. Nachfolgend wird als Auswahl das Treuhandverhältnis, die Hinterlegung, das Escrow-Agreement sowie die Sicherungszession einer näheren Betrachtung unterzogen.

1. Smart Contract als Fiduziar

525 Das Schweizer Recht kennt das Treuhandverhältnis als vertragliches Verhältnis, obwohl es nicht kodifiziert ist.[770]

a) Treuhandvertrag

526 Das Treuhandverhältnis ist ein zweiseitiger Vertrag zwischen dem Fiduziant (Treugeber) und Fiduziar (Treuhänder).[771] Der dem Treuhandverhältnis zugrundeliegende Vertrag wird auch das Grundgeschäft zwischen Fiduziant

769 Zur Definition, Funktionsweise und Anwendungsbeispiele vgl. Kapitel D. Einführung Smart Contracts, N 214 ff.

770 EICHNER, Rechtsstellung von Treugebern, N 175.

771 Vgl. EICHNER, Rechtsstellung von Treugebern, N 176.

und Fiduziar genannt, in dem eine Übertragung eines Rechts sowie eine fiduziarische Abrede vereinbart wird.[772] Der Treugeber beauftragt den Treuhänder, im eigenen Namen, aber im Interesse und auf Rechnung des Treugebers tätig zu sein; dies wird gem. h.L. als Auftrag im Sinne von Art. 394 OR qualifiziert.[773] Gestützt auf dieses obligatorische Grundgeschäft wird zusätzlich eine dinglich wirkende Übertragung eines Rechts auf den Fiduziar vorgenommen.[774]

527 Das Treugut kann aus Wertschriften, Beteiligungen, Forderungen, Liegenschaften, Handelsgeschäften, Geld oder immateriellen Gütern bestehen.[775]

b) Smart Contract als Fiduziar

528 Ein Vertrag kann grundsätzlich nur zwischen rechts- und geschäftsfähigen Personen geschlossen werden (vgl. N 277 ff.).[776] Wie bereits mehrfach ausgeführt, ist ein Smart Contract eine Software verfügt nicht über eine eigene Rechtspersönlichkeit (vgl. N 239). Mit einem Smart Contract kann daher kein Treuhandvertrag geschlossen werden. Es ist jedoch denkbar, dass im Rahmen eines Treuhandverhältnisses ein Smart Contract eingesetzt wird, wobei in dieser Konstellation die Vorteile eines Smart Contract (u.a. automatisierte Durchsetzung, Wegfall von Intermediär), nicht genutzt werden können.

529 Es ist auch möglich, dass anstelle eines Treuhandverhältnisses ein Smart Contract aufgesetzt wird und dort die Regeln hinterlegt werden, wie die Software die Vermögenswerte verwalten und ggf. im Namen des „Treugebers“ tätig werden soll. In diesem Fall ist jedoch nicht mehr von einem vertraglichen

---

772 Vgl. EICHNER, Rechtsstellung von Treugebern, N 202; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1024 ff.; KRAMER/SCHMIDLIN, BK OR, Art. 18 N 123 f.; WEBER, BSK OR I, Art. 394 N 11 ff.

773 EICHNER, Rechtsstellung von Treugebern, N 201; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1025; KRAMER/SCHMIDLIN, BK OR, Art. 18 N 125 f.; WEBER, BSK OR I, Art. 394 N 11.

774 KRAMER/SCHMIDLIN, BK OR, Art. 18 N 124.

775 Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT, N 1026.

776 Vgl. HUGUENIN/REITZE, BSK ZGB I, Art. 54 N 2; FANKHAUSER, BSK ZGB I, Art. 12 N 4.

Verhältnis auszugehen, sondern vom Einsatz einer Software zur automatisierten Durchsetzung eigener Interessen.

c) Sicherungszession

530 Die Sicherungszession ist im Gesetz nicht definiert;[777] sie stellt aber eine Unterart des fiduziarischen Rechtsgeschäfts dar und zeichnet sich dadurch aus, dass die Schuldnerin zur Sicherung der Hauptschuld der Gläubigerin zu Sicherungszwecken eine Forderung abtritt.[778] Im Regelfall handelt es sich beim Sicherungszedenten und dem Schuldner der Hauptforderung um die gleiche Person, der Sicherungszedent kann jedoch auch ein Dritter sein.[779] Die Sicherungszession enthält eine Zession im Sinne von Art. 165 OR, ist jedoch durch ein fiduziarisches Grundgeschäft ergänzt (vgl. N 526); die Sicherungsforderung wird bei einem Dritten, dem Fiduziar, hinterlegt.[780]

aa) Sicherungszession mit Smart Contracts

531 Wie bereits mehrfach dargelegt, kann ein Smart Contract aufgrund fehlender Rechtspersönlichkeit nicht Vertragspartei sein. Dennoch stellt die Sicherungszession einen Hauptanwendungsfall für den Einsatz von Smart Contracts dar: Der Smart Contract kann als sichere Verwahrstelle für eine Zession dienen und macht so den Einsatz eines Intermediärs überflüssig. Dank dem Smart Contract benötigen die beiden Parteien keine vertrauenswürdige Instanz, bei der sie die Sicherungszession hinterlegen. Sie können, wie bereits mehrfach dargelegt, den Smart Contract so ausgestalten, dass bei Eintreten des Ereignis X (Erfüllung oder Nichterfüllung der Hauptverpflichtung der Schuldnerin) die Forderung entweder automatisch an die Schuldnerin zurückfällt oder vereinbarungsgemäss an die Gläubigerin übergeht.

---

777 REETZ, aktuelle Rechtsfragen Sicherungszession, 178.

778 Vgl. REETZ, Sicherungszession, N 41 f.; REETZ, aktuelle Rechtsfragen Sicherungszession, 178.

779 REETZ, Sicherungszession, N 28.

780 REETZ, Sicherungszession, N 48; REETZ, aktuelle Rechtsfragen Sicherungszession, 181.

bb) Forderungsübertragung mit Smart Contracts

532 Um eine Sicherungsforderung rechtsgültig bei einem Smart Contract zu hinterlegen, müsste diese Forderung einerseits durch einen Token repräsentiert werden – was grundsätzlich möglich ist (vgl. Anhang, N 30 ff.) – und andererseits müsste die Übertragung dieses Token dem Schrifterfordernis gem. Art. 165 Abs. 1 OR genügen.[781] Zum Einsatz kann dabei die qualifizierte elektronische Unterschrift gem. Art. 14 Abs. 2bis OR kommen.

533 Um die für die Forderungsübertragung notwendige Unterschrift sicherzustellen, müsste der entsprechende Smart Contract (oder die Blockchain-Plattform) eine ZertES-konforme qualifizierte elektronische Unterschrift einsetzen.[782] Die derzeit genutzten Signaturen in den öffentlichen (und soweit ersichtlich auch in den privaten) Blockchains sind jedoch nicht ZertES-konform. Dementsprechend kann das Schrifterfordernis von Art. 165 Abs. 1 OR für die gültige Übertragung einer Forderung nicht erfüllt werden. Sollten ZertES-konforme Unterschriften (z.B. durch eine spezialisierte Applikation) zum Einsatz gelangen, dann müsste überdies sichergestellt werden, dass die automatisierte Übertragung von einem Smart Contract auf einen Vertragspartner die ZertES-konforme Unterschrift des ursprünglichen Forderungsinhabers trägt, da ein Smart Contract in der Regel über keine eigene Signatur verfügt. Diese würde für eine gültige Übertragung der Forderung ohnehin nicht ausreichen, da der Smart Contract aufgrund seiner fehlenden Rechtspersönlichkeit rechtsgültig keine Forderungen übertragen kann.

534 Einer gültigen Forderungsübertragung mittels Smart Contract steht nebst einer gültigen Unterschrift auch der Aspekt im Wege, dass der (unterzeichnete) Erklärungsinhalt in Schrift und Sprache den sich erklärenden Parteien zugänglich sein muss; wenn Drittinteressen betroffen sind, muss die Sprache der Allgemeinheit zugänglich sein (N 375). Der Erklärungsinhalt ist bei Smart Contracts in Programmiersprache verfasst. Ein Erklärungsinhalt in Programmiersprache ist nur in den (seltenen) Fällen unproblematisch, in denen die Parteien den Inhalt erfassen können und keine Drittparteien betroffen sind

781 GIRSBERGER/HERRMANN, BSK OR I, Art. 165 N 2.

782 Vgl. Ausführungen zur einfachen Schriftlichkeit bei Kapitel E.VII.2., N 367 ff.; zur ZertES-konformen Unterschrift vgl. Anhang, N 15 ff.

(N 375). Bei einer Sicherungszession könnte diese Voraussetzung nur dann erfüllt werden, wenn der Sicherungszedent und der Schuldner ein und dieselbe Person ist und beide Vertragsparteien fachkundige Personen sind (Beherrschung der Programmiersprache).

2. Smart Contract als Aufbewahrer

535 In der Praxis spielen Hinterlegungsverträge insbesondere im Bankengeschäft eine grosse Rolle (Depotverträge).[783]

a) Hinterlegungsvertrag

536 Der Hinterlegungsvertrag regelt die Aufbewahrung einer beweglichen Sache bei einem Hinterleger, der diese Sache übernimmt und an einem sicheren Ort aufbewahrt (Art. 472 Abs. 2 OR). Wesensmarkmal dieses Vertrages ist das Anvertrauen einer beweglichen Sache durch den Hinterleger an den Aufbewahrer, das Recht des Hinterlegers, die Rückgabe der Sache zu verlangen sowie die Aufbewahrung im Interesse des Hinterlegers.[784]

b) Smart Contract als Aufbewahrer

537 Auch hier gilt, dass der Smart Contract nicht als Vertragspartner (Aufbewahrer) auftreten kann, sondern vielmehr von einer Partei dazu verwendet werden kann, eine Sache aufzubewahren. Der Hinterlegungsvertrag regelt die Aufbewahrung von beweglichen Sachen.[785] Ein Smart Contract ist in erster Linie nicht dazu geeignet, bewegliche Sachen zu verwahren. Nichtsdestotrotz ist es möglich, einen Gegenstand so zu sichern, dass die tatsächliche Verfügungsgewalt nur beim Smart Contract oder subsidiär bei beiden Vertragsparteien gleichermassen liegt. So kann zum Beispiel eine Sache, z.B. ein Auto, in einer Garage zwischengelagert sein. Das Autoschloss (und allenfalls auch das Garagenschloss) ist mit einem Sensor (IoT) verbunden. Sobald der Smart Contract die Information erhält, dass das Auto freigegeben

783 KOLLER, BSK OR I, Vorbem. zu Art.472-491 N 3.
784 KOLLER, BSK OR I, Art. 472 N 1 ff.
785 KOLLER, BSK OR I, Art. 472 N 4.

werden darf (z.B. durch Eingang einer Zahlung oder durch das Einverständnis beider Vertragsparteien), sendet er dem (neuerdings) Verfügungsberechtigten einen Token, mit Hilfe dessen er das Autoschloss (und falls nötig auch das Garagenschloss) öffnen kann.

3. Smart Contract als Escrow-Agent

538 Das ursprünglich aus dem anglo-amerikanischen Recht stammende Escrow-Agreement ist im Schweizer Recht nicht geregelt, kann jedoch zwischenzeitlich als konstituiert angesehen werden.[786]

a) Escrow-Agreement

539 Umschrieben wird das Escrow-Verhältnis als ein Dreiparteienverhältnis, bei dem eine beliebige Sache im Interesse zweier Parteien bei einem neutralen Dritten (dem Escrow-Agenten) zu Sicherungszwecken hinterlegt wird.[787] Das Escrow-Agreement besteht demgemäss aus einem Hauptgeschäft zwischen zwei Parteien, das es zu sichern gilt, einem Sicherungsobjekt sowie einem Vertrag zwischen den Parteien und dem Escrow-Agenten.[788] Das Sicherungsobjekt ist eine bewegliche Sache.[789]

b) Smart Contract als Escrow-Agent

540 Da bei einem Escrow-Agreement mit einem Escrow-Agenten ein vertragliches Verhältnis eingegangen wird, kann ein Smart Contract aufgrund seiner fehlenden Rechtspersönlichkeit nie die Rolle eines Escrow-Agenten einnehmen.[790]

---

786 Vgl. EISENHUT, Escrow-Verhältnisse, 7 f.; GLARNER/MEYER, Smart Contracts in Escrow-Verhältnissen, N 7.

787 Vgl. EISENHUT, Escrow-Verhältnisse, 13; GLARNER/MEYER, Smart Contracts in Escrow-Verhältnissen, N 7.

788 EISENHUT, Escrow-Verhältnisse, 13 ff.

789 EISENHUT, Escrow-Verhältnisse, 87; GLARNER/MEYER, Smart Contracts in Escrow-Verhältnissen, N 9.

790 GLARNER/MEYER, Smart Contracts in Escrow-Verhältnissen, N 28.

Das Sicherungsobjekt bei einem Escrow-Agreement ist eine bewegliche Sache. Ein Smart Contract eignet sich in erster Linie dazu, digitale Werte und weniger, bewegliche Sachen in der realen Welt zu verwahren. Trotzdem ist es möglich, eine bewegliche Sache durch einen Smart Contract zu sichern (vgl. vorhergehend N 537). Wird diese Möglichkeit genutzt, dann ist der Einsatz eines Escrow-Agenten hinfällig. 541

III. Fazit

Ein Smart Contract kann dazu verwendet werden, Vermögenswerte temporär aufzubewahren, resp. zu halten und diese im Anschluss gemäss den hinterlegten Regeln einer Partei zu übertragen. 542

Der Einsatz eines Smart Contract kann gegebenenfalls die Funktion eines Treuhänders, eines Aufbewahrers oder eines Escrow-Agenten übernehmen. Hierbei ist jedoch zu beachten, dass sich ein Smart Contract in erster Linie zur Aufbewahrung und Halten von digitalen Werten eignet und reelle Gegenstände den Einsatz von zusätzlichen Mechanismen (IoT u.a.) erforderlich machen. 543

Bezüglich der Übertragung von Sicherungszessionen auf einen Smart Contract ist zu bedenken, dass Forderungen nur mit einer gültigen Unterschrift übertragen werden können. Dieses Erfordernis stellt beim Einsatz von Smart Contracts ein dreifaches Problem dar: Erstens werden (derzeit) keine ZertES-konformen Signaturen in Blockchain-Plattformen verwendet, die das Unterschrifterfordernis für die gültige Übertragung erfüllen können. Zweitens müsste die Übertragung, die von dem Smart Contract vorgenommen wird, die (ZertES-konforme) Signatur der ursprünglich verfügungsberechtigten Partei enthalten, damit der Übertrag gültig ist. Ein Smart Contract hat keine eigene Signatur und diese würde aufgrund der fehlenden Rechtspersönlichkeit des Smart Contract keine gesetzeskonforme Wirkung entfalten. Drittens muss der unterzeichnete Erklärungsinhalt den Parteien in Schrift und Sprache und, falls Dritte betroffen sind, der Allgemeinheit zugänglich sein. Dies ist bei einer Forderungsübertragung in Form eines Token grundsätzlich zu verneinen und kann nur in Ausnahmefällen bejaht werden. 544

3. Teil: Zusammenfassung

545 In diesem dritten und letzten Teil der Arbeit werden die wichtigsten Erkenntnisse des ersten und zweiten Teils zusammengefasst. Zum Abschluss folgt eine Würdigung der wichtigsten Erkenntnisse.

I. Erkenntnisse

Begriff und Funktionalitäten der Blockchain

546 Der Begriff *Blockchain* wird als Sammelbegriff verwendet und kann stark vereinfacht als gigantisches Transaktionsregister bezeichnet werden, das basierend auf einem dezentralen und verteilten P2P-Netzwerk Daten so abspeichert, dass sie transparent nachvollziehbar und unabänderlich sind (N 22 f.).

547 Die Blockchain kann nach den Funktionalitäten eingeteilt werden, die ein solches Netzwerk einnehmen kann. Dabei kann grundsätzlich zwischen der Blockchain generell-abstrakt als technisches Konzept, der zugrundeliegenden Software und der durch die Software geschaffenen Infrastruktur – der Plattform – unterschieden werden (N 21).

Vertragsrechtliche Erfassung der Blockchain

548 Wird die der Blockchain-Infrastruktur zugrundeliegende Software betrachtet, kann festgestellt werden, dass es sich dabei um eine Open-Source-Software handelt. Open-Source-Software wird unter OSS-Lizenzen vertrieben, die nach der hier vertretenen Meinung als unentgeltliche Softwarelizenzverträge einzuordnen sind und zu deren Auslegung die Regeln zum Softwarelizenzvertrag sowie zum allgemeinen Teil des Obligationenrechts heranzuziehen sind (N 148 f.). Zwischen einem Knotenbetreiber und dem Urheber der Software kann dann ein Lizenzverhältnis begründet werden, wenn die Blockchain-Software über das normale Gebrauchsrecht hinaus benutzt wird (N 207).

549 Die mit Hilfe der Blockchain-Software geschaffene Infrastruktur, die Plattform, wird durch ein P2P-Netzwerk betrieben. Dieses Netzwerk ist eine Gemeinschaft mit gewissen Elementen einer einfachen Gesellschaft, kann aber

keiner gesellschaftsrechtlichen Form des Schweizer Rechts zugeordnet werden. Es ist vielmehr von einem losen Zusammenschluss von Personen, der zwar ein gemeinsames Ziel mit gemeinsamen Mitteln verfolgt, jedoch keinerlei Rechte und Pflichten begründet, auszugehen (N 208). Innerhalb des Netzwerkes können keine Vertragsverhältnisse ausgemacht werden; einzig bei der Beziehung zwischen einem Nutzer (i.S. eines Knotenbetreibers) und einem Miner kann von einem einseitigen Rechtsgeschäft, einer Auslobung i.S.v. Art. 8 OR, ausgegangen werden (N 209).

550 Der Zugang zum P2P-Blockchain-Netzwerk wird in der Regel durch Wallet-Anbieter gewährt. Wallet-Anbieter können funktionell einem Access Provider gleichgestellt werden, weshalb eine für Access Provider ausgestaltete Providerhaftung auch auf Wallet-Anbieter angewendet werden könnte (N 210).

Begriff und Funktionsweise von Smart Contracts

551 In der vorliegenden Arbeit wird ein Smart Contract als ein auf der Blockchain-Technologie basierendes, individualisierbares Computerprogramm definiert (N 239). Eigenschaften von Smart Contracts sind eine gewisse Autonomie, die Unveränderbarkeit und die fehlende Interpretationsmöglichkeit (N 240).

Smart Contract als Vertrag

552 Aufgrund der Formfreiheit des Schweizer Vertragsrechts ist es grundsätzlich möglich, einen Vertrag in Programmiersprache aufzusetzen (N 276).

553 Wird ein Smart Contract von fachkundigen Personen benutzt, die seinen Inhalt nachvollziehen können, kann er selbst den Vertrag – in Form eines bedingten Vertrages – darstellen. Wird er hingegen von fachunkundigen Personen eingesetzt, so ist von der Annahme auszugehen, dass die Personen sich nicht über die Konsequenzen des Vereinbarten bewusst sind, d.h. sich ihr Rechtsbindungswille nicht auf die möglichen Folgen des Einsatzes eines Smart Contract richtet. In diesen Fällen ist jedoch bei bewusster Unkenntnis des Vereinbarten eine Berufung auf den fehlenden Rechtsbindungswillen allenfalls rechtsmissbräuchlich. Wird ein Smart Contract zwischen einer fachkundigen und einer fachunkundigen Person eingesetzt, dann ist eine Einzelfallbetrachtung notwendig. Grundsätzlich kann jedoch festgehalten werden, dass in den Fällen, wo der Inhalt des Smart Contract mit zumutbarem Aufwand erschlossen werden kann und die fachunkundige Person kein

Konsument ist, der Smart Contract ebenfalls direkt das Grundgeschäft darstellen kann (N 330).

554 Ein in einem Smart Contract hinterlegtes Angebot muss terminiert werden, ansonsten der Offerent aufgrund der Unabänderbarkeit des Smart Contract auf unbestimmte Zeit gebunden ist. Dies gilt zumindest für Smart Contracts, die direkt auf einer (öffentlichen) Blockchain installiert sind (N 331). Der Vertrag kommt mit der Signierung der akzeptierenden Partei mit dem Private Key (Vornahme einer Transaktion) zustande (N 332).

555 Wie bei einer Computererklärung können die ausgeführten „Handlungen" eines Smart Contract immer mindestens einer Partei zugeordnet werden, da einerseits ein Vermögenswert (oder sonst ein Token) an den Smart Contract transferiert und von diesem wiederum an eine weitere (oder zurück an dieselbe) Partei überwiesen wird. Durch diese Transaktion(en) sind die beteiligten Personen an einem Smart Contract eruierbar und somit sämtliche Handlungen des Smart Contract diesen Parteien zuzuordnen (N 332).

556 Smart Contracts bedürfen aufgrund ihrer deterministischen Ausgestaltung keiner Auslegung (N 332).

557 Ist ein Smart Contract auf einer öffentlichen Blockchain implementiert, kann dieser grundsätzlich nicht widerrufen werden. Ein Smart Contract sollte daher immer eine zeitliche Terminierung vorsehen, insbesondere dann, wenn mit Hilfe eines Smart Contract ein Angebot gesetzt wird (N 345 f.).

558 Beinhaltet ein Smart Contract einen gesetzeswidrigen Vertragsinhalt und ist der Vertrag dementsprechend nichtig, kann diese Nichtigkeit auf der Blockchain nicht umgesetzt werden. Ein Smart Contract kann, wenn er direkt auf einer öffentlichen Blockchain platziert ist, nicht gelöscht, widerrufen oder abgeändert werden. Eine Transaktion, die aufgrund eines nichtigen Grundgeschäftes auf der Blockchain getätigt wurde, kann nicht entsprechend markiert werden. Dies führt zu einer gewissen Rechtsunsicherheit bezüglich der Gültigkeit von blockchainbasierten Transaktionen und widerspricht dem Grundsatz der Blockchain-Logik, nach der die in der Blockchain gespeicherten Transaktionen gemäss dem vereinbarten Konsens als gültig zu betrachten sind. Selbes gilt für Smart Contracts, die ausserhalb einer Blockchain gespeichert sind und deren Ergebnis (die Transaktion) bereits in die Blockchain

aufgenommen wurde, bevor das Grundgeschäft als nichtig deklariert wurde (N 411 ff.).

559 Die Formvorschriften der einfachen sowie qualifizierten Schriftlichkeit und der öffentlichen Beurkundung können mit Smart Contracts nicht erfüllt werden. Zu erfüllen wären die Voraussetzungen der einfachen Schriftlichkeit unter den folgenden Gesichtspunkten: Die Unterschrift wird mit ZertES-konformen Signaturen gesetzt. Solche werden jedoch, soweit ersichtlich, in keiner Blockchain eingesetzt. Selbst wenn solche Signaturen bei Smart Contracts eingesetzt würden, wäre zu beachten, dass die entsprechende Transaktion jeweils die Signatur der zur Unterschrift verpflichteten Person tragen würde – Smart Contracts haben keine eigene Signatur und eine solche würde aufgrund der fehlenden Rechtspersönlichkeit dem Schrifterfordernis auch nicht gerecht. Zusätzlich müsste der unterzeichnete Erklärungsinhalt den Parteien in Schrift und Sprache, und ist ein Dritter (z.B. bei einer Forderungsübertragung) betroffen, der Allgemeinheit zugänglich sein. Programmiersprache ist nur fachkundigen Personen und nicht der Allgemeinheit zugänglich; die Vereinbarung dürfte also nur zwischen fachkundigen Personen wirken (N 375, 392 f).

Mangelhafte Willenserklärungen bei Smart Contracts

560 Mangelhafte Willenserklärungen, insbesondere Fälle des Irrtums, können auch bei Verwendung von Smart Contracts vorkommen. Dabei steht insbesondere der Erklärungsirrtum als Folge eines Übermittlungsfehlers im Vordergrund. Die Beurteilung, ob eine mangelhafte Willenserklärung vorliegt, kann nicht durch vordefinierte Parameter eines Smart Contract eruiert werden. Die Rechtsfolge, die einseitige Unverbindlichkeit, lässt sich mit einem Smart Contract grundsätzlich nicht abbilden, da er nachträglich nicht geändert (oder als ungültig markiert) werden kann (N 443 ff.).

Leistungsstörungen bei Smart Contracts

561 Mit Hilfe von Smart Contracts können Leistungsstörungen zu einem grossen Teil vermieden werden. Eine Leistungsunmöglichkeit ist nur noch in den Fällen denkbar, in denen ein Token auf der Blockchain transferiert wird, der tatsächlich jedoch nicht das repräsentiert, was er vorzugeben scheint. Schlechtleistungen sollten dank Smart Contracts nicht vorkommen, jedenfalls

dann nicht, wenn die geschuldete Leistung mit klaren Parametern überprüfbar ist. Der Smart Contract führt bei Nichterfüllung dieser Parameter den Vertrag nicht aus. Aus dieser Nichtausführung kann jedoch eine Spätleistung resultieren (N 480 ff.).

Gewährleistung und Haftung bei Smart Contracts

562 Smart Contracts werden unter OSS-Lizenzen veröffentlicht. Diese Lizenzen enthalten Freizeichnungsklauseln für Gewähr und Haftung. Nach der hier vertretenen Ansicht werden bei OSS-Lizenzen die Regeln des Softwarelizenzvertrages sowie die allgemeinen Regeln des Obligationenrechts herangezogen. Nach Art. 100 OR ist eine Freizeichnung erlaubt, jedoch unter Ausschluss von Absicht und grober Fahrlässigkeit. Ein aus einem fehlerhaft programmierten Smart Contract resultierender Schaden kann bei Nachweis von Absicht oder grober Fahrlässigkeit gegenüber dem Softwareentwickler geltend gemacht werden. Eine deliktische Haftung gegenüber Dritten kann bei Vorliegen der entsprechenden Voraussetzungen begründet werden (N 513 f.).

563 Wird ein Smart Contract fehlerhaft angewendet, d.h. der Fehler liegt nicht im Softwarecode selbst, dann kann ein Anspruch direkt aus dem Vertrag zwischen den Parteien abgeleitet werden, wenn die Individualisierung eine vertragliche Haupt- oder Nebenpflicht darstellt. Resultiert aus der fehlerhaften Anwendung ein Schaden bei einem Dritten, dann kann bei Vorliegen der Tatbestandsvoraussetzungen allenfalls ein Anspruch aus Delikt geltend gemacht werden (N 515 f.).

Smart Contract als Halter von Vermögenswerten

564 Ein Smart Contract kann eine Art Treuhänderfunktion einnehmen, wobei hier kein vertragliches Verhältnis eingegangen wird, sondern Eigeninteressen mit Hilfe von Technologie verfolgt und die Vermögenswerte keiner (spezialisierten) Partei mehr übergeben werden (N 528 f.). Der Smart Contract kann faktisch auch dazu dienen, Sicherungszessionen zu hinterlegen. Rechtlich ist ein solches Rechtsgeschäft nicht verbindlich, da das Schriftlichkeitserfordernis für die gültige Übertragung der Sicherungszession nicht erfüllt werden kann. Die Übertragung kann einerseits nicht rechtsgültig vorgenommen werden, wenn keine ZertES-konformen elektronischen Signaturen eingesetzt werden. Selbst wenn eine solche zum Einsatz käme, wäre

sicherzustellen, dass die Übertragung der Sicherungszession, wenn sie vom Smart Contract an die vertraglich vereinbarte Partei transferiert wird, die (ZertES-konforme) Signatur der verfügungsberechtigten Partei trägt (ein Smart Contract hat selbst keine Signatur). Andererseits ist der unterzeichnete Erklärungsinhalt in Programmiersprache verfasst und so der Allgemeinheit nicht zugänglich, was ebenfalls der Erfüllung der Voraussetzungen der einfachen Schriftlichkeit widerspricht (N 531 ff.).

565 Ein Smart Contract eignet sich in erster Linie nicht als Aufbewahrer oder als Escrow-Agent, da in diesen Fällen bewegliche Sachen aufbewahrt werden. Es ist jedoch unter Einbezug von IoT und Hilfsmitteln möglich, einem Smart Contract die Aufbewahrung (resp. die tatsächliche Verfügungsmacht) einer beweglichen Sache zu übertragen (N 537, 541).

II. Würdigung

566 Wie in der vorliegenden Arbeit aufgezeigt, birgt die Blockchain-Technologie, und insbesondere der Smart Contract, ein grosses Potential zur Digitalisierung und Automatisierung von Vertragsbestandteilen. Eine rechtliche Einordnung dieser Technologie bedarf zwar eines hohen Abstraktionsvermögens, ist aber *de lege lata* und unter Einbezug der Dogmatik durchaus möglich; auch wenn dafür bisweilen eine flexible Auslegung nötig ist.

567 Smart Contracts eignen sich grundsätzlich nicht dazu, Verträge direkt abzubilden. Sie dienen aber unbestrittenermassen einer vereinfachten und automatisierten Ausführung und Durchsetzung von gewissen Vertragsbestandteilen.

568 Auffällig ist eine Diskrepanz zwischen der in einer Blockchain-Plattform herrschenden apodiktischen Konsensregelung zur Gültigkeit von Transaktionen und der differenzierten Beurteilung eines gültigen Rechtsgeschäftes in der realen Welt: In der Blockchain gilt die unwiderlegbare Vermutung der Gültigkeit einer Transaktion, ist sie erst einmal in der Blockchain abgespeichert. Diese Regel lässt keinen Raum für menschliche Verhaltensweisen, wie bspw. jene des sich Irrens. Werden in der realen Welt Verträge, die auf einer blockchainbasierten Transaktion beruhen, als ungültig beurteilt, dann kann diese Ungültigkeit in der Blockchain nicht abgebildet werden. Dies führt *de facto* zu einer Rechtsunsicherheit im Zusammenhang mit blockchainbasierten Transaktionen.

569 Abschliessend kann festgehalten werden, dass eine Blockchain und insbesondere ein Smart Contract aufgrund der inhärenten Computerlogik im Gegensatz zum bestehenden Vertragsrecht nicht in der Lage ist, die komplexe Realität aufzufangen.

Anhang: Begriffe und Erläuterungen

1. Software, Computerprogramm, Algorithmus

In der IT werden die Termini *Algorithmus, Software und Computerprogramm* auseinandergehalten und nicht synonym verwendet. Software umfasst als Oberbegriff und umfasst (Computer-)Programme, Dokumentationen (Anwender- und Entwicklungsdokumentation) und dazugehörige Daten.[791] Teilweise wird Software als Gegenbegriff zu Hardware (die technische, physikalische Form des Computers) beschrieben.[792] 1

Computerprogramme sind in Programmiersprache verfasst und befähigen einen Computer, Steuerungs- und Berechnungsfunktionen auszuführen.[793] *Programmiersprachen* können durch Computer nicht direkt gelesen werden, sondern müssen erst in Maschinensprache übersetzt werden.[794] 2

Ein Computerprogramm umfasst *Algorithmen*[795] und die dazugehörigen Datenstrukturen. Der Algorithmus ist durch für den Computer durch das Computerprogramm ausführbar.[796] 3

---

791 SCHWARZ/KRUSPIG, Computerimplementierte Erfindungen, N 73; WIDMER, Softwarepflegevertrag, 5; vgl. ADLER, Rechtsfragen der Softwareüberlassung, 7.

792 BAUSEN, Softwarepatente, 4; WEBER, E-Commerce, XCI.

793 SCHWARZ/KRUSPIG, Computerimplementierte Erfindungen, N 55 und Glossar S. 418.

794 HEROLD/LURZ/WOHLRAB/HOPF, Grundlagen der Informatik, 137 f.

795 Der Begriff *Algorithmus* wird in der Informatik und in der Mathematik uneinheitlich verwendet (vgl. SCHWARZ/KRUSPIG, Computerimplementierte Erfindungen, N 63). In der Informatik ist ein Algorithmus „eine detaillierte und explizite Vorschrift zur schrittweisen Lösung eines Problems, d.h. eine Vorschrift zur Lösung einer Aufgabe, die präzise formuliert, in endlicher Form dargestellt und effektiv ausführbar ist“: HEROLD/LURZ/WOHLRAB/HOPF, Grundlagen der Informatik, 152.

796 SCHWARZ/KRUSPIG, Computerimplementierte Erfindungen, N 54 f.

4 In der vorliegenden Arbeit werden die Begriffe *Software* und *Computerprogramm* synonym verwendet.

2. Hash

5 *Hash*, auch *Hash-Wert* genannt, ist eine sogenannte Streuwertfunktion. Dieser Begriff stammt aus der Mathematik und bezeichnet eine kurze Zeichenfolge mit fester Länge und stellt die Abkürzung einer beliebig langen Zeichenfolge (Prüfsumme) dar. Aus einem Datensatz wird eine Prüfsumme gebildet: der sog. Hash-Wert. Ein kryptografischer Hash-Wert wird in der Blockchain-Technologie als Sicherungsmechanismus benutzt.[797] Ändert sich ein Zeichen am Ursprungswert (d.h. am ursprünglichen Inhalt des Datensatzes), so ändert sich auch der entsprechende Hash-Wert. Der Hash-Wert dient also dazu, zwei Zeichenfolgen (Prüfsummen) miteinander zu vergleichen und so festzustellen, ob sie identisch sind.[798] Auf der Blockchain wird derjenige Datensatz, der gespeichert werden soll, in einen Hash-Wert umgewandelt und dieser im Block gespeichert.[799] Grundsätzlich ist alles in einen Hash-Wert umwandelbar, es kommt dabei nicht auf die Art des Datensatzes an.

6 Beispiel:[800]

Der Hash-Wert von der Wortkombination *Blockchain und Smart Contracts* lautet:

---

797 Eine kryptografische Hash-Funktion stellt sicher, dass ein potentieller Angreifer bspw. nicht einen identischen Hash-Wert aufgrund eines anderen Datensatzes herstellen kann. Es gibt auch nicht kryptografische Hashfunktionen. Ausführlich zum Thema Hash und kryptografische Hash-Funktionen siehe PAAR/PELZL, Kryptografie verständlich, 335 ff.; SCHMEH, Kryptografie, 241 ff.

798 KAULARTZ, Blockchain Technologie, 475; BERENTSEN/SCHÄR, Krypto-assets, 141.

799 SWAN, Blockchain, 39.

800 Es ist ein Beispiel für einen Hash-Verfahren nach SHA 256 (zu SHA 256 siehe SCHMEH, Kryptografie, 256).

b6d51e0c1d1b56745e43f877d54b8152f2d955ba7c5023366c46c57992dc9b52

Wird das *s* bei Smart Contracts weggelassen, ergibt *Blockchain und Smart Contract* folgenden Hash-Wert:

49337a83ed782b61f0ecf33beff1f6d481f6e93c37afce9f4e2d57fcf9158643

3. Hash-Bäume

Werden grosse Datenmengen, resp. grosse Datenbanken in Hash-Werte umgewandelt und signiert, kann dies eine enorm aufwändige Verifizierungsarbeit nach sich ziehen. Um dies zu umgehen, erlaubt eine mathematische Lösung, um eine vereinfachte Datenstruktur zu schaffen. Durch diese vereinfachte Datenstruktur, auch *Hash-Baum* (oder *Merkle-Tree* genannt), wird die Authentifizierung stark vereinfacht.[801] 7

4. Kryptografische Verschlüsselungsverfahren

Es existieren unzählige kryptografische Verschlüsselungsverfahren. Grundsätzlich kann zwischen symmetrischen und asymmetrischen Verfahren unterschieden werden. Bei beiden Verfahren ist das gemeinsame Ziel, die Nachricht, die versendet wird, so zu sichern, dass keine unbefugte Drittperson die Nachricht lesen, resp. verfälschen kann.[802] Prinzipiell gilt: je wichtiger die Information für den „Datenbesitzer“ ist, desto komplizierter sollte seine Verschlüsselung sein.[803] Quantencomputer[804] könnten in dieser Hinsicht eine 8

---

801 PAAR/PELZL, Kryptografie verständlich, 346 ff.; SCHMEH, Kryptografie, 285 ff.

802 PAAR/PELZL, Kryptografie verständlich, 4 f.; SCHMEH, Kryptografie, 12 ff.

803 Laut GERHARDS gibt es eine absolute, physikalische Obergrenze bis zu welcher Schlüssellänge entschlüsselt werden können, GERHARDS, Verschlüsselung, 36.

804 Ein Quantencomputer könnte bestimmte Problemstellungen, wie z.B. die asymmetrischen Verschlüsselungsverfahren, deutlich effektiver lösen als

Gefahr für die Verschlüsselungstechnik darstellen, wobei diese (vorerst) nur in der Theorie existieren. Andererseits ist zu erwarten, dass die Weiterentwicklung der Verschlüsselungstechniken mit der Entwicklung der Quantencomputer Schritt zu halten vermag.[805]

a) Symmetrische Verschlüsselung

9 Die symmetrische Verschlüsselung ist das klassische Verfahren und hat zum Ziel, die Versendung einer Nachricht über einen unsicheren Kommunikationskanal (heute z.B. das Internet) so zu schützen, dass keine unbefugte Partei diese mitlesen (oder mithören) kann.[806] Beim symmetrischen Verfahren wird sowohl zum Ver- als auch Entschlüsseln derselbe Schlüssel benutzt.[807] Der Schlüssel kann aus einer geheimen Nummer, einem Passwort oder einer Folge von Bits bestehen.[808] Symmetrische Verschlüsselungsverfahren gelten für heutige Standards meist nicht mehr als genügend sicher.[809]

b) Asymmetrische Verschlüsselung

10 Beim asymmetrischen Verfahren wird im Gegensatz zur symmetrischen Verschlüsselung ein Schlüsselpaar benötigt. Es wird zwischen zwei Schlüsseln unterschieden: dem öffentlichen (*Public Key*) und dem privaten (*Private* oder *Secure Key*). Der öffentliche Schlüssel wird veröffentlicht und ist prinzipiell für jedermann zugänglich. Der zweite Schlüssel ist der geheime, private Schlüssel. Das Prinzip funktioniert so: Absender A will Empfänger B eine verschlüsselte Nachricht senden. A verschlüsselt die Nachricht an B mit dessen

---

ein herkömmlicher Rechner; die Bauteile des Quantencomputers arbeiten nach den Gesetzen der Quantenmechanik. Siehe ausführlich dazu SCHMEH, Kryptografie, 311 ff.

805 Ausführlich dazu SCHMEH, Kryptografie, 313 ff.; GERHARDS, Verschlüsselung, 36.

806 PAAR/PELZL, Kryptografie verständlich, 4 f; vgl.SCHMEH, Kryptografie, 39 ff.

807 GERHARDS, Verschlüsselung, 33; SCHMEH, Kryptografie, 41.

808 SCHMEH, Kryptografie, 39.

809 SCHMEH, Kryptografie, 39.

öffentlichem Schlüssel. Zur Entschlüsselung dieser Nachricht benützt B seinen privaten Schlüssel. Diese Verschlüsselungsmethode nennt man auch *Public-Key-Verfahren*.[810]

11 Ein bekanntes Public-Key-Verfahren ist das RSA-Verfahren.[811] Dem RSA-Verfahren (wie auch anderen Public-Key-Verfahren) liegen Modulo-Rechnungen zugrunde. Vereinfacht gesagt bedeutet dies, dass einfache Rechenaufgaben benützt werden, um die Verschlüsselung durchzuführen.[812] Diese Rechnungen sind zwar einfach zu berechnen, jedoch nur sehr schwer (resp. mit sehr grossem Rechenaufwand) umzukehren.[813] Dies ist als die sogenannte *Einwegfunktion* bekannt. Falls eine Zusatzinformation hinzugefügt wird, mit der die komplizierte Umkehrrechnung vereinfacht werden kann, nennt man dies *Falltürfunktion* genannt.[814]

12 Geknackt werden kann die Formel auch mittels *Brute-Force-Methode*, d.h. dem Suchen der Lösung mittels wiederholtem Ausprobieren, bis sie gefunden ist. Dies kann durch die Benutzung einer Formel verhindert werden, bei der eine zufällige Lösungsfindung durch „Ausprobieren“ eher unwahrscheinlich ist.[815] Hinzu kommt ein zeitlicher Aspekt: Sind die Einwegfunktionen nicht innert nützlicher Zeit umkehrbar, ist der Nutzen für den Angreifer fraglich. Je wichtiger die zu entschlüsselnde Information für den Angreifer ist, desto mehr Zeit wird er für die Entschlüsselung in Kauf nehmen.

---

810 GERHARDS, Verschlüsselung, 33.

811 RSA steht für die Abkürzung der Nachnamen der Erfinder dieser Methode: RON RIVEST, ADI SHAMIR und LEONARD ADLEMAN.

812 Ausführlich dazu SCHMEH, Kryptografie, 192 ff.

813 Deren Problemstellung ist bekannt, aber deren effiziente Lösung (i.S.v. zeitsparender Rechenformel) für den Umkehrschluss jedoch nicht. Theoretisch ist es also möglich, dass jemand einen effizienten Weg für die Berechnung des Umkehrschlusses findet. Werden allerdings bekannte mathematische Probleme benutzt, die schon seit geraumer Zeit bekannt sind und für die noch keine effiziente Lösung gefunden wurde, ist die Wahrscheinlichkeit klein.

814 SCHMEH, Kryptografie, 198.

815 GERHARDS, Verschlüsselung, 35 f.

5. Digitale Signatur

a) Allgemeines

13 Die digitale Signatur ist eine Anwendung der asymmetrischen Kryptografie. Die digitale (elektronische) Signatur dient hauptsächlich der Authentifizierung und Identifizierung des Absenders aber auch der Sicherstellung der Integrität der Daten.[816] Es soll sichergestellt werden, dass eine bestimmte Nachricht oder ein Schriftstück von einer bestimmten Person stammt – vergleichbar mit der handschriftlichen Unterschrift in der analogen Welt.[817] Für die digitale Signatur wird ebenfalls kryptografische Verschlüsselungstechnik benutzt, gleich wie bei der Verschlüsselung der Daten selbst.[818] Die Funktionsweise der digitalen Signatur mittels einem Public-Key-Verfahren (N 10) wie bspw. beim RSA-Verfahren (N 11) funktioniert genau umgekehrt zu der Verschlüsselung der Daten: Absender A sendet Empfänger B eine Nachricht. Die Signatur setzt A mit seinem privaten Schlüssel. B überprüft die Authentizität der Signatur von A mit dem öffentlichen Schüssel von A.[819] Auch bei der digitalen Signatur können Hash-Werte (N 5 ff.) eingesetzt werden. So können bspw. sämtliche zu signierende Daten zu einem Hash umgewandelt werden und nur dieser Wert wird mit der digitalen Signatur versehen.[820] Dieses Vorgehen eignet sich bei einer grossen Datenmenge, damit nicht einzelne Datensätze signiert werden müssen. Bezüglich der Sicherheit von digitalen Signaturen kann auf die Feststellungen zur Verschlüsselungstechnik allgemein (N 12) verwiesen werden.[821]

14 Um sicherzustellen, dass nicht gefälschte öffentliche Schlüssel von Personen kursieren, werden Zertifikate verwendet, die eine Identität (bspw. E-Mail-

---

816 GERHARDS, Verschlüsselung, 39 f.; PAAR/PELZL, Kryptografie verständlich, 299 f.

817 PAAR/PELZL, Kryptografie verständlich, 299 f.

818 Vgl. SCHMEH, Kryptografie, 216.

819 GERHARDS, Verschlüsselung, 40 f; SCHMEH, Kryptografie, 217.

820 GERHARDS, Verschlüsselung, 41.

821 Zur Sicherheit von RSA-Signaturen vgl. PAAR/PELZL, Kryptografie verständlich, 306 f.; SCHMEH, Kryptografie, 217 f.

Adresse) an einen öffentlichen Schlüssel binden.[822] Damit eine digitale Signatur als Ersatz für die handschriftliche Unterschrift rechtsgültig verwendet werden kann (vgl. Art. 14 Abs. 2 OR), müssen in der Schweiz die Anforderungen des ZertES und in der EU die der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung)[823] erfüllt sein. Die Anforderungen und Ausgestaltungen der elektronischen Signaturen gem. ZertES entsprechen den europäischen Pendants gem. eIDAS-Verordnung.[824]

b) Elektronische Signatur gemäss ZertES

15 Laut Obligationenrecht ist die qualifizierte elektronische Unterschrift der eigenhändigen Unterschrift gleichgestellt (Art. 14 Abs. 2bis OR). ZertES regelt nebst der qualifizierten elektronischen Unterschrift, die für den Rechtsverkehr benötigt wird, auch weitere Signaturen, Siegel und Zertifikate, abgestuft nach deren Verwendungszweck und den Anforderungen (Art. 2 ZertES):

16 *Elektronische Signatur (lit. a)*: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen.

17 *Fortgeschrittene elektronische Signatur (lit. b)*: Eine elektronische Signatur, die folgende Anforderungen erfüllt: 1. sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet, 2. sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers, 3. sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer/seiner alleinigen Kontrolle halten kann, 4. sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

---

822 PAAR/PELZL, Kryptografie verständlich, 327.

823 Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (in Kraft seit 1. Juli 2016).

824 Botschaft ZertES, 1019 f.

18 *Geregelte elektronische Signatur (lit. c):* Eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Signaturerstellungseinheit generiert wurde und auf einem geregelten, auf eine natürliche Person ausgestellten und zum Zeitpunkt der Erzeugung der elektronischen Signatur gültigen Zertifikat beruht.

19 *Geregeltes elektronisches Siegel (lit. d)*: Eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Siegelherstellungseinheit auf einem geregelten, auf eine UID-Einheit[825] gem. UIDG ausgestellten und zum Zeitpunkt der Erzeugung des elektronischen Siegels gültigen Zertifikat beruht.

20 *Qualifizierte elektronische Signatur (lit. e)*: Eine geregelte elektronische Signatur, die auf einem qualifizierten Zertifikat beruht.

21 *Digitales Zertifikat (lit. f)*: Eine digitale Bescheinigung, die den öffentlichen Schlüssel eines asymmetrischen kryptografischen Schlüsselpaars seinem Inhaber oder seiner Inhaberin zuordnet.

22 *Geregeltes Zertifikat (lit. g)*: Ein digitales Zertifikat, das die Anforderungen nach Art. 7[826] erfüllt und von einer nach ZertES anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt wurde.

---

825 Unternehmensidentifikationsnummer gem. Art. 3 Abs. 1 lit. c Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010 (UIDG), SR. 431.03.

826 Ein geregeltes Zertifikat kann gem. Art. 7 ZertES auf natürliche oder UID-Einheiten ausgestellt werden; folgende Angaben sind zwingend (Abs. 2): a) Seriennummer; b) Hinweis, dass es sich um ein geregeltes Zertifikat handelt; c) Namen oder Bezeichnung der Inhaberin oder des Inhabers des zugehörigen privaten kryptografischen Schlüssels; besteht eine Verwechslungsmöglichkeit, so ist der Name oder die Bezeichnung mit einem unterscheidenden Zusatz zu versehen; d) bei natürlichen Personen gegebenenfalls das als solches gekennzeichnetes Pseudonym anstelle des Namens; e) bei UID-Einheiten die Unternehmens-Identifikationsnummer nach UIDG; f) der öffentliche kryptografische Schlüssel; g) die Gültigkeitsdauer; de Name, der Niederlassungsstaat und das geregelte

Qualifiziertes Zertifikat (lit. h): Ein geregeltes Zertifikat, das die Anforderungen nach Art. 8[827] erfüllt. 23

Elektronischer Zeitstempel (lit. i): Bestätigung, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen. 24

Qualifizierter elektronischer Zeitstempel (lit. j): Elektronischer Zeitstempel, der von einer nach ZertES anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt und mit einem geregelten elektronischen Siegel versehen wurde. 25

Anbieter von Zertifizierungsdiensten (lit. k): Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt. 26

Anerkennungsstelle (lit. l): Stelle, die nach dem THG[828] für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist. 27

6. Virtuelle Währung / Kryptowährung

Virtuelle Währungen sind digitale Codes, die einen Wert digital darstellen und diesen in der virtuellen Welt handelbar machen.[829] Emittiert werden virtuelle Währungen grundsätzlich von dezentralen P2P-Netzwerken (z.B. Bitcoin), kann aber auch von Instituten ausgegeben werden.[830] Virtuelle Währungen sind 28

elektronische Siegel der Anbieterin von Zertifizierungsdiensten, die das Zertifikat ausstellt. Dem Zertifikat können noch mehr Elemente hinzugefügt werden (Abs. 3).

827 Ein qualifiziertes Zertifikat kann nur auf eine natürliche Person ausgestellt werden (Abs. 1); es enthält einen Eintrag, wonach es nur für die elektronische Signatur bestimmt ist (Abs. 2) und einen Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt (Abs. 3).

828 Bundesgesetz vom 6. Oktober 1995 über die technischen Handelshemmnisse (THG), SR 946.51.

829 Vgl. BUNDESRAT, virtuelle Währungen, 7 f.

830 SANSONNETTI, Bitcoin, 46; KÜTÜK-MARKENDORF, Internetwährungen, 48.

nicht durch ein gesetzliches Zahlungsmittel unterlegt und unterscheiden sich dadurch von E-Geld[831].[832] Virtuelle Währungen qualifizieren in der Schweiz als Vermögenswerte aber nicht als Währung oder gesetzliches Zahlungsmittel.[833]

29 Eine Unterart der virtuellen Währungen stellen Kryptowährungen dar. Die bekannteste Kryptowährung ist Bitcoin. Daneben gibt es unzählige weitere Kryptowährungen, wie bspw. Ether, EtherClassic, Ripple, Litecoin oder Dash.[834] Seit geraumer Zeit ist eine gewisse Begeisterung für Kryptowährungen in der (Risiko-) Investorenwelt auszumachen, die zwischenzeitlich auch die breitere Masse erreicht hat.[835] Bei Kryptowährungen gilt es, sich zu vergegenwärtigen, dass es sich dabei um eine Historie von Transaktionen eines Wertes handelt, der aus dem Nichts geschaffen wurde und lediglich aus einer Abfolge von Transaktionsdaten besteht.[836] Ein Kryptowährungstoken repräsentiert nie einen individualisierbaren

---

831 Anders als in der EU ist E-Geld ist in der Schweiz nicht reguliert und stellt kein gesetzliches Zahlungsmittel dar (vgl. für die EU-Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG); vgl. HESS/WEISS VOIGT, E-Geld, 8 f.

832 BUNDESRAT, virtuelle Währungen, 7 f.

833 BUNDESRAT, virtuelle Währungen, 7 f.; ausführlich zum monetärrechtlichen Hintergrund BERENTSEN/SCHÄR, Kryptoassets, 7 ff.; ZELLWEGER-GUTKNECHT, Digitale Landeswährung, 4 ff.

834 Eine Übersicht über die sich in Umlauf befindlichen Kryptowährungen und deren Marktkapitalisierung findet sich unter https://coinmarketcap.com/currencies/.

835 Vgl. die auch in Massenmedien regelmässig erscheinenden Berichte über Kryptowährungen und die zunehmende Marktkapitalisierung der einzelnen Kryptowährungen, zu verfolgen z.B. auf Coinmarketcap (FN 89).

836 Vgl. SWANSON, Great Chain, 17; allgemein zu Kryptowährungen MEISSER, Kryptowährungen, 23 ff.

Vermögenswert, einzig die zugrundeliegende Transaktion kann in der Blockchain identifiziert werden.[837]

7. Token

Es besteht keine einheitliche Definition des Begriffs *Token*.[838] Damit ein Datensatz (z.B. Wert oder Gegenstand in der realen Welt) Gegenstand von Transaktionen in einer Blockchain sein kann, muss er einen eindeutigen Vertreter (*Platzhalter*) in der Blockchain haben. Dies geschieht mit einem Token. Die Schaffung eines Token nennt man Tokenizing.[839] Verkörpert ein Token einen Anspruch auf einer Blockchain, ist es ein sog. *Native Token*. Native Token verkörpern weder relative noch absolute Rechte.[840] Im Gegensatz dazu werden Token, die für ausserhalb der Blockchain durchsetzbaren Rechte stehen, sog. *Non-Native Token* genannt.[841] Ein Non-Native Token kann relative wie auch absolute Rechte repräsentieren.[842] 30

Die FINMA qualifiziert Token aus einer finanzmarktrechtlichen Perspektive in die Kategorien Zahlungs-Token, Nutzungs-Token und Anlage-Token. [843] Dabei sind jedoch Mischformen (*hybride Token*) nicht auszuschliessen.[844] 31

Ein Zahlungs-Token (*Currency Token*) ist laut FINMA mit Kryptowährungen gleichzusetzen.[845] Es sind diejenigen Token, die tatsächlich oder mit Absicht des Organisators als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen akzeptiert werden oder zur Währungs- und Wertübertragung dienen. Kryptowährungen – und damit auch Zahlungs-Token – begründen 32

---

837 EGGEN, Was ist ein Token?, 228 f.

838 Vgl. EGGEN, Was ist ein Token?, 558, 560; SCHMEH, Kryptografie, 461 f.

839 Vgl. SWAN, Blockchain, 72 f.

840 Ausführliche Begründung bei EGGEN, Was ist ein Token?, 561 ff.

841 EGGEN, Was ist ein Token?, 559.

842 EGGEN, Was ist ein Token?, 563.

843 FINMA, Wegleitung ICOs, 3.

844 FINMA, Wegleitung ICOs, 3; EGGEN, Was ist ein Token?, 561.

845 FINMA, Wegleitung ICOs, 3; EGGEN, Was ist ein Token?, 560.

keine Ansprüche gegenüber dem Emittenten.[846] Die FINMA klassifiziert die Zahlungs-Token nicht als Effekten, da sie in erster Linie als Zahlungsmittel konzipiert sind und nicht unter den Effektenbegriff von Art. 2 lit. b Finanzmarktinfrastrukturgesetz (FinfraG)[847] subsumiert werden können.[848]

33 Unter Nutzungs-Token (*Utility Token*) versteht die FINMA die Token, die eine digitale Nutzung ermöglichen oder Dienstleistung vermitteln, wobei die Nutzung oder die Dienstleistung auf oder unter Nutzung einer Blockchain-Infrastruktur erbracht wird.[849] Sie werden dann nicht als Effekten qualifiziert, wenn der Bezug zum Kapitalmarkt fehlt und die Realerfüllung des Anspruchs im Vordergrund steht.[850] Nutzungs-Token können wiederum in *Usage Token* und *Work Token* unterteilt werden, wobei erstere Zugang zu digitalen Dienstleistungen oder Produkten gewähren, während letztere ein Recht zur Erbringung einer Leistung sicherstellen.[851]

34 Unter Anlage-Token (*Real Asset Token*) subsumiert die FINMA sämtliche Token, die Vermögenswerte repräsentieren. Diese Token können schuldrechtliche Forderungen gegenüber dem Emittenten oder aber ein Mitgliedschaftsrecht im gesellschaftlichen Sinne darstellen.[852] Versprochen werden beispielsweise Anteile an künftigen Unternehmenserträgen oder Kapitalflüssen. Je nach wirtschaftlicher Funktion repräsentiert ein solcher Token eine Aktie, Obligation oder ein Derivat. Ebenfalls in diese Kategorie fallen diejenigen Token, die physische Wertgegenstände auf der Blockchain handelbar machen.[853] Diese Art von Token werden als Effekten gem. Art. 2 lit. b FinfraG qualifiziert, wenn sie ein Wertrecht repräsentieren und die Token

---

846 FINMA, Wegleitung ICOs, 3.

847 Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarkt-infrastrukturgesetz, FinfraG) vom 19. Juni 2015, SR 958.1.

848 FINMA, Wegleitung ICOs, 4.

849 FINMA, Wegleitung ICOs, 3.

850 FINMA, Wegleitung ICOs, 4.

851 EGGEN, Was ist ein Token?, 559 f.

852 FINMA, Wegleitung ICOs, 3; EGGEN, Was ist ein Token?, 560.

853 FINMA, Wegleitung ICOs, 3.

vereinheitlicht und zum massenweisen Handel geeignet sind. Das Gleiche gilt, wenn der Token ein Derivat repräsentiert.[854]

8. ICO / TGE

Ein *Initial Coin Offering (ICO)* (auch *Token Generating Event* (*TGE*) oder *Initial Token Sale*) ist eine Form der Kapitalbeschaffung.[855] Gemäss FINMA überweisen Anleger den ICO-Organisatoren finanzielle Mittel in Form von Kryptowährung und erhalten im Gegenzug blockchainbasierte Coins bzw. Token. Diese Token werden auf einer neu entwickelten Blockchain oder mittels Smart Contract auf einer bereits bestehenden Blockchain geschaffen und dezentral gespeichert.[856] 35

9. Hard Fork / Soft Fork

Hard Fork und *Soft Fork* stellen einen Eingriff in die Blockchain dar. Bildlich gesprochen handelt es sich dabei um eine „Gabelung" der Blockchain, faktisch handelt es sich dabei um eine Spaltung. Eine Gabelung, resp. eine Verästelung widerspricht eigentlich dem Grundwesen der Blockchain; Prinzip ist die einheitliche, komplett synchronisierte Datensammlung aller Transaktionen gleichzeitig auf allen angeschlossenen Knotenpunkten. Zu einer Gabelung kann es in den Fällen kommen, in denen es bspw. neue Konsens-Regeln gibt und noch nicht aktualisierte Kotenpunkte die neuen Blöcke deswegen nicht bilden können.[857] Bei einem Hard Fork entstehen aus der Gabelung zwei Blockchains, die separat und autonom voneinander weiterlaufen oder eine Kette läuft ins Leere und nur eine Gabelung stellt die valide Blockchain dar. Eine Soft Fork stellt nur eine temporäre Gabelung dar; die Blockchain wird 36

854 FINMA, Wegleitung ICOs, 4 f.

855 Vgl. ESSEBIER/BOURGEOIS, Regulierung von ICOs, 568; BAFIN, Hinweisschreiben ICO, Ziff. 5; zur Regluglierung von ICOs in der Schweiz siehe ESSEBIER/BOURGEOIS, Regulierung von ICOs, 580 ff.

856 FINMA, Wegleitung ICOs, 1.

857 Vgl. BERENTSEN/SCHÄR, Kryptoassets, 73.

danach nicht dauerhaft gespalten, sondern wieder vereint weitergeführt.[858] Eine Hard oder Soft Fork kann –falls vorhanden – auch durch die Kontrollinstanz oder den Systembetreiber im Betrugsfall angewendet werden.

10. DAOs / DAPs / DACs etc.

37 *DAO* steht für *Dezentrale Autonome Organisation* (*decentralized autonomous organization*).[859] Die DAO ist eine blockchainbasierte Applikation,[860] die individuell programmiert werden kann. Ihre bekannteste Anwendung dürfte wohl „The DAO“ sein, die aufgrund eines Hackerangriffs einen Verlust von damals ca. USD Mio. 50 erlitt und zu einer Spaltung der Ethereum-Blockchain geführte.[861]

38 *DAP* steht für *Dezentrale Autonome Applikation*, während *DAC* für *Dezentrale Autonome Company* steht.[862] Gemeinsam haben alle diese Systeme, dass sie für dezentrale und autonome Anwendungen auf einer Blockchain-Plattform stehen. Sie können unterschiedlich ausgestaltet sein und es entstehen auch fortwährend neue Formen. Meist bestehen sie aus einer dezentralen Applikation, die verschiedene Smart Contracts enthält.

858 Vgl. ANTONOPOULOS, Mastering Bitcoin, 213 ff.

859 Vgl. www.ethereum.org/dao.

860 BURGWINKEL, Blockchain Technology, 47; MOUGAYAR, Business Blockchain, 70 ff.; SWAN, Blockchain, 24.

861 Ausführlich GYR, DAO, N 7 ff.; TOSOVIC, DAO-Hack, 159 ff.

862 Vgl. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.