

Internetrecht und Digitale Gesellschaft

Band 49

**Smart Legal Contracts
und Blockchain – Einordnung in
die Rechtsgeschäftslehre**

Von

Mauritz von Wedemeyer



Duncker & Humblot · Berlin

MAURITZ VON WEDEMEYER

Smart Legal Contracts und Blockchain –
Einordnung in die Rechtsgeschäftslehre

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 49

Smart Legal Contracts und Blockchain – Einordnung in die Rechtsgeschäftslehre

Von

Mauritz von Wedemeyer



Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät
der Albert-Ludwigs-Universität Freiburg im Breisgau hat diese Arbeit
im Jahr 2023 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten
© 2023 Duncker & Humblot GmbH, Berlin
Satz: TextFormA(r)t, Daniela Weiland, Göttingen
Druck: CPI Books GmbH, Leck
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-18893-2 (Print)
ISBN 978-3-428-58893-0 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

Vorwort

Die vorliegende Arbeit wurde von der Rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg im Breisgau im Wintersemester 2022/2023 als Dissertation angenommen. Gesetzgebung, Literatur und Rechtsprechung konnten noch bis März 2023 berücksichtigt werden.

Mein herzlicher Dank gilt meinem Doktorvater Professor Dr. Jan Lieder, LL. M. (Harvard) für die Betreuung der Arbeit sowie das Gewähren wissenschaftlicher Freiheit bei ihrer Erstellung. Er war jederzeit zur Stelle, wenn ich Fragen hatte oder Hilfe benötigte. Für die zeitnahe Erstellung des Zweitgutachtens danke ich Professor Dr. Hanno Merkt, LL. M. (Chicago).

Ebenso bedanke ich mich herzlich bei meinen Brüdern, Christopher und Felix von Wedemeyer, sowie bei Sven Köksal, die mich während der Dissertation unterstützten.

Zu besonderem Dank verpflichtet bin ich meinen Eltern, Margret und Dr. Hans-Georg von Wedemeyer, die mich stets in jeder erdenklichen Hinsicht bedingungslos gefördert haben. Ihnen ist diese Arbeit gewidmet.

Berlin, im März 2023

Mauritz von Wedemeyer

Inhaltsverzeichnis

Einleitung und Aufbau der Untersuchung	15
---	----

1. Teil

Technische Grundlagen		20
A. Blockchain		20
I. Die Distributed Ledger-Technologie (DLT)		22
II. Hash		22
III. Blöcke		23
IV. Chain		24
V. Erstellung eines Blocks		25
1. Proof of Work (PoW)		26
a) Technische Grundlage		26
b) Motivation eines Miners		28
c) Kritik am Proof of Work-System		29
2. Proof of Stake (PoS)		30
a) Technische Grundlage		30
b) Angriffe auf das Netzwerk		31
c) Auswahl des Validators		33
aa) Chain-based Proof of Stake		33
bb) Committee-based Proof of Stake		33
cc) BFT-based Proof of Stake		34
dd) Delegated Proof of Stake		34
d) Zusammenfassung		35
3. Andere		36
VI. Zugangsbeschränkungen und Öffentlichkeit		36
VII. Ablauf einer Transaktion		38
1. Art der Transaktion		38
2. Konto		38
3. Asymmetrische Kryptografie		40
4. Autorisierung der Transaktion		42
5. Senden an die Nodes		43

6. Pool verifizierter Transaktionen	44
7. Anhängen an die Blockchain	44
a) Erstellung des Blocks	45
b) Übermittlung an Nodes	45
c) Aktualisierung des Ledgers	46
d) Forks	46
aa) Entstehung eines Forks	47
bb) Auflösung des Forks	47
e) Bestätigte oder gescheiterte Transaktion	49
VIII. Zusammenfassung	50
B. Smart Contracts	51
I. Begriffserklärung	52
II. Smart Legal Contract	54
III. Anwendungsbereiche	55
IV. Funktionen	57
V. Smart Contracts und Blockchain	59
1. Schreiben eines Smart Contracts	59
2. Anfrage beim Netzwerk	61
3. Erstellung eines internen Kontos	62
4. Ethereum Virtual Machine (EVM)	63
5. Interaktion durch die Parteien	65
6. Ausführen des Programmcodes	66
7. „Gas“	66
8. Oracles	68
9. Scheitern eines Smart Contracts	70
10. Beispiel eines Smart Legal Contracts	71
11. Decentralized Applications (DApps)	73
12. Decentralized Autonomous Organisations (DAOs)	74
13. Token	74
C. Zusammenfassung	76

2. Teil

Vertragsschluss 78

A. Konkurrenz des technischen und rechtlichen Regimes	79
I. Digitale Rechtsordnung	79
II. Privatautonomie als Verdrängung von Recht?	81

III. Auflösung der Kollision	82
B. Smart Contract als rechtlicher Vertrag	84
C. Vertragsschluss	85
I. Smart Legal Contracts „on-chain“ vs. „off-chain“	86
II. Vorliegen einer Willenserklärung	88
1. Äußerer Tatbestand	89
a) Bloßes Vollzugsvehikel	89
b) Programmcode als „Black Box“	91
c) Interessenlage der Parteien	95
2. Innerer Tatbestand	97
III. Problem der Pseudonymität	99
IV. Zurechnung der Willenserklärung	100
1. Von automatisierten bis autonomen Systemen	101
2. Rückblick auf Funktionsweise von Smart Contracts	104
3. Unmittelbare Interaktion durch Rechtssubjekte	104
4. Mittelbare Interaktion durch Rechtssubjekte	105
5. Sonstige Konstellationen und Zwischenergebnis	107
6. Bestimmung des Vertragspartners hinter dem externen Konto	108
V. Angebot und Annahme	112
1. Angebot	113
a) Unter Anwesenden oder unter Abwesenden	113
b) Programmierung des Smart Legal Contracts	114
c) Einsetzen auf der Blockchain	115
d) Interaktion durch Transaktion	117
aa) Abgabe	119
(1) Grundlagen	120
(2) Autorisierung der Transaktion	120
(3) Senden an die Nodes	121
(4) Pool verifizierter Transaktionen	123
bb) Zugang	124
(1) Grundlagen	124
(2) Empfang der Transaktionsdaten durch die Nodes	125
(3) Pool verifizierter Transaktionen	126
(4) Anhängen des neuen Blocks	128
(a) Zugang durch Blockerstellung	129
(aa) Proof of Work-Blockchain	130
(bb) Proof of Stake-Blockchain	130

(cc) Blockerstellung im Allgemeinen	131
(b) Zugang durch Übermittlung des neuen Blocks	131
(aa) Erste Übermittlung des neuen Blocks	132
(bb) Der Empfänger-Node hat den neuen Block	133
(cc) Über 50 % der Nodes haben den neuen Block	133
(dd) Beweisprobleme	135
(ee) Folge für den Zugang	136
(5) Problem der „Forks“	137
(a) Problemstellung	138
(b) Bisherige Lösungsansätze	138
(c) Zugangsfrage, Wirksamkeitsbedingung oder Formfrage?	141
(d) Risiko- und Interessenlage	142
(aa) Art des Forks	143
(bb) Prozessbasierte Forks	144
(cc) Protokollbasierte Forks	148
(e) Umsetzung des eigenen Lösungsansatzes	151
(f) Bedeutung für die Rechtspraxis	152
2. Annahme	153
a) Korrespondierend	153
b) Übereinstimmend	155
c) Abgabe	156
aa) Willenserklärung verkörpert in der Transaktion	156
bb) Willenserklärung verkörpert in der Transaktionsquittung?	158
d) Zugang	159
aa) Entbehrlichkeit des Zugangs, § 151 S. 1 BGB	159
bb) Anwendung der Zugangsregeln	161
cc) Problem der Forks	161
dd) Annahmefrist, §§ 146 ff. BGB	162
VI. Token	164
VII. Zwischenergebnis	165

3. Teil

Schranken der Wirksamkeit	167
A. Überblick	167
B. Formerfordernisse	171
I. Anknüpfung für die Form der Erklärungen auf der Blockchain	171
II. Anwendbarkeit der Formvorschriften	172

III. Notarielle Beurkundung und öffentliche Beglaubigung, §§ 128, 129 BGB	173
IV. Schriftform, § 126 BGB	174
V. Elektronische Form, § 126a BGB	174
VI. Textform, § 126b BGB	178
1. Lesbarkeit	179
2. Nennung der Person des Erklärenden	180
3. Abgabe auf einem dauerhaften Datenträger	183
4. Abschlussfunktion	183
VII. Blockchain-Form, § 125 S. 2 BGB	184
VIII. Zwischenergebnis	184
C. Bedeutung einer (Teil-)Unwirksamkeit für den Smart Legal Contract	185

4. Teil

Bestimmung der Vertragsart 188

A. Atypischer Werkvertrag	188
B. Kaufvertrag	189
C. Tauschvertrag	193

5. Teil

Vertragsauslegung 196

A. Zweispurigkeit des Smart Legal Contracts	196
B. Auslegungsfähigkeit des Programmcodes	198
I. Übersetzung von Programmiersprache und natürlicher Sprache	199
II. Programmcodes ohne Wertungsspielraum	199
III. Programmcodes mit Wertungsspielraum	200
IV. Ricardian Contract	201
C. Auslegung des Smart Legal Contracts	202
I. Art des Vertragsschlusses	203
II. Absolute Auslegungsregeln	204
III. Bestimmung des objektiven Empfängerhorizonts	207
1. Sicht eines Programmierers	208
2. Sicht eines erfahrenen Netzwerkteilnehmers	210
3. Sicht eines unerfahrenen Netzwerkteilnehmers	211

4. Problem des pseudonymen Vertragspartners	211
5. Wahl des objektiven Empfängers bei Pseudonymität	212
6. Ausnahmsweise „Code is Contract“?	214
7. Ausdrückliche „Code is Contract“-Klausel	215
IV. Falsa demonstratio non nocet	217
V. Fehler im Code	218
VI. Lückenhafte Verträge und ergänzende Vertragsauslegung	219
VII. Folge für die Vertragsabwicklung	221
VIII. Blick in die Praxis	221
D. Zwischenergebnis	222

6. Teil

Verfügungen durch den Smart Legal Contract	223
A. Verfügung durch Übertragung von Kryptowährung	223
B. Dinglicher Vertrag	224
I. Zusammentreffen der schuldrechtlichen und dinglichen Ebene	226
II. Dingliche Einigung durch technischen Vollzug	228
III. Stellungnahme	230
C. Widerruf der dinglichen Einigung	231
I. Grundlagen	232
II. Kollision mit Smart Legal Contracts	233
III. Lösungsansatz	235
D. Folge bei Abweichung zwischen technischer und rechtlicher Vermögenszuweisung	236
E. Zwischenergebnis	236

7. Teil

De Lege Ferenda	237
A. Blick in die USA	239
B. Formvorschriften	241
I. Formfunktionen	241
II. Änderung der Formvorschriften	244
Zusammenfassung in Thesen	246

Anhang	250
A. Anhang 1	250
B. Anhang 2	251
I. Solidity	251
II. Opcodes	254
III. Bytecode und ABI	258
Literaturverzeichnis	261
Sachverzeichnis	282

Einleitung und Aufbau der Untersuchung

Die Digitalisierung erfasst immer mehr Lebensbereiche. Auch der Abschluss und die Abwicklung von Verträgen können digitalisiert werden. Das Mittel dazu sind sog. Smart Contracts, die sich mehr und mehr als unverzichtbar erweisen. Smart Contracts sollen es schaffen, Prozesse zu automatisieren, Kosten zu senken und die Sicherheit zu erhöhen. Traditionell müssen jeder Vertragsschluss und jeder Leistungsaustausch manuell durchgeführt werden. Schließt ein Fluggast beispielsweise einen Beförderungsvertrag mit einer Fluggesellschaft ab, hat er bei einer Verspätung des Fluges von drei Stunden nach der FluggastrechteVO¹ einen Anspruch auf Entschädigung, sofern keine Ausnahmen vorliegen. Herkömmlicherweise musste der Fluggast das Geld von der Fluggesellschaft einfordern und bei Weigerung der Zahlung gerichtliche Schritte einleiten. Da dies für den Einzelnen aufwendig und unwirtschaftlich sein kann und Flüge zudem häufig verspätet sind, sind im Zuge der Digitalisierung Inkassounternehmen wie Flightright entstanden, die Fluggästen helfen, ihre Ansprüche gegen Fluggesellschaften durchzusetzen. Die Prozesse der Geltendmachung der Ansprüche verlaufen jedoch bei diesen Unternehmen nicht automatisch. Hier kann der Smart Contract helfen und als eine Art Treuhänder fungieren: Der Ticketpreis wird an den Smart Contract gezahlt. Dieser prüft, ob ein Entschädigungsfall eingetreten ist. Ist der Flug pünktlich, fließt das Geld an die Fluggesellschaft. Bei einer Verspätung fließt nur ein Teil des Geldes an die Fluggesellschaft, den übrigen Teil erhält der Fluggast zurück.

Auch in den Bereichen fin und legal tech hört man von Smart Contracts.² Dabei haben die jüngsten Entwicklungen im Bereich Blockchain die Relevanz der Smart Contracts hervorgehoben.³ Bei Smart Contracts handelt es sich jedoch nicht um eine neue Idee. Genau genommen ist diese beim klassischen Warenautomaten bereits zweitausend Jahre alt.⁴ Der Einsatz solcher Technologien, die durch Code geprägt sind, stieß jedoch stets an die Grenzen der analogen Welt.⁵ Denn einerseits lassen sich komplexe Vorgänge nur mühevoll in Code abbilden, andererseits kann ein Smart Contract nicht ohne Weiteres die analoge Welt beeinflussen.

¹ Art. 5, 6, 7 Verordnung (EG) Nr. 261/2004, zur Rechtsfortbildung siehe EuGH Urt. v. 19. 11. 2009 – C-402/07, EU:C:2009:716 Rn. 1 ff.

² *Fries*, Anwaltsblatt 2018, S. 86 (86); *Korschinowski*, RdF 2017, S. 97 (97).

³ *Durovic/Janssen*, ERPL 2019, S. 753 (757).

⁴ Der erste Warenautomat war ein Weihwasserautomat, siehe *Fries*, *Rethinking Law* 2018, S. 46 (47).

⁵ *Jacobs/Lange-Hausstein*, ITRB 2017, S. 10 (12).

Die Idee eines intelligenten Vertrages erscheint vielversprechend, weil ein solcher Vertrag nicht mehr kostenträchtig und zeitintensiv ausgehandelt, überwacht und durchgeführt werden muss. Zudem sind traditionelle Verträge als solche „inaktiv“, das heißt, sie dienen zur Gestaltung der Rechtslage zwischen den Parteien, mehr nicht.⁶ Dies führt dazu, dass bestehende Ansprüche nicht immer durchgesetzt werden, da der erzielbare Mehrwert nicht die damit verbundenen Kosten und den Zeitaufwand rechtfertigt.

Hier setzen Smart Contracts an. Denn erfolgen der Abschluss und die Durchsetzung eines Vertrages automatisch, können die Parteien Zeit und Kosten sparen sowie Rechtsklarheit schaffen.⁷ Zudem erzeugen Smart Contracts eine größere Vertragssicherheit dadurch, dass die Vertragsdurchsetzung durch den Programmcode garantiert wird. Die Parteien müssen einander nicht vertrauen, denn eine Abweichung von dem, was im Code vereinbart wurde, ist nicht möglich. Smart Contracts wird daher ein großes Potenzial für die Wirtschaft zugeschrieben.

Als bedeutsam für die Anwendung von Smart Contracts gilt die sog. Blockchain-Technologie. Diese kann die Grundlage für den Abschluss von Smart Contracts bilden und es den Parteien ermöglichen, die Vorteile von Blockchain und Smart Contracts zusammen zu nutzen. Ein wichtiger Vorteil der Kombination dieser beiden Technologien liegt darin, dass ein Smart Contract im Nachhinein nicht oder nur schwer manipuliert werden kann. Zur Verdeutlichung mag ein einfacher Vergleich dienen: Der Kaufprozess bei einem Warenautomaten kann als Smart Contract bezeichnet werden. Jedoch weiß ein Käufer nicht, ob er nach dem Einwurf des Geldes die Ware tatsächlich erhält. Behält der Warenautomat das Geld, ohne die Ware freizugeben, müsste ein Käufer – abhängig von den Umständen des Falles – auf Rückzahlung des Geldes oder auf Leistung klagen. Die Blockchain soll solche Leistungsstörungen verhindern. Sie soll insbesondere transparenter und manipulationsfester sein.

Auch die EU erkennt die Potenziale dieser neuen Technologie. Das Europäische Parlament nahm 2016 eine Entschließung zu virtuellen Währungen an: Es

„erkennt an, dass sich das Potenzial der DLT noch entfaltet und weit über den Finanzsektor hinausreicht, etwa in Bereiche wie ‚Crypto-equity Crowdfunding‘ (Schwarmfinanzierung mit ‚Krypto-Kapital‘), Streitschlichtungsdienste, insbesondere im Finanzsektor und im Justizwesen, intelligente Verträge in Verbindung mit digitalen Unterschriften, Anwendungen, die einen erhöhten Datenschutz und Synergien mit der Entwicklung des Internets der Dinge ermöglichen“⁸.

Auf nationaler politischer Ebene lässt sich der folgende Passus im Koalitionsvertrag zwischen CDU, CSU und SPD von 2018 finden:

⁶ Eine Ausnahme bilden dingliche Verträge.

⁷ Vgl. *Braegelmann/Kaulartz*, in: *Braegelmann/Kaulartz* (Hrsg.), *Rechtshandbuch Smart Contracts*, S. 1 (3 (Rn. 7)).

⁸ Europäisches Parlament, Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2016, S. 6.

„Wir erleichtern Verbraucherinnen und Verbrauchern die Rechtsdurchsetzung durch Digitalisierung, insbesondere bei smart contracts. Deshalb werden wir die Entwicklung der automatischen Vertragsentschädigung fördern und rechtssicher gestalten.“⁹

Entwicklungen auf der Legislativebene lassen sich vereinzelt beobachten. So wurde im Juni 2021 ein Gesetz zur Einführung von elektronischen Wertpapieren verabschiedet.¹⁰ Inhaltlich zielt der Regierungsentwurf darauf ab, dass das deutsche Wertpapierrecht die Ausgabe digitaler Wertpapiere ggf. mittels einer Blockchain ermöglicht.¹¹ Von Interesse sind in dieser Hinsicht auch die Entwicklungen auf EU-Ebene. Denn aufgrund der häufigen Transnationalität der Sachverhalte bietet sich hier eine einheitliche Lösung an. Im Mai 2022 wurde eine Verordnung durch das Europäische Parlament und den Europäischen Rat zur Regelung des Finanzsektors bei Nutzung von Blockchains verabschiedet.¹² Es soll ein Rechtsrahmen für Kryptowerte in Bezug auf Finanzdienstleistungen geschaffen werden. Weitere Entwicklungen auf der Legislativebene sind nicht ausgeschlossen.

Die Möglichkeit der Nutzung der Blockchain-Technologie wird auch von staatlichen Institutionen untersucht. So hat etwa die Deutsche Bundesbank einen Test für eine Abwicklungsschnittstelle für elektronische Wertpapiere, basierend auf der Distributed Ledger-Technologie, unternommen.¹³ In der Wirtschaft gibt es eine Vielzahl von Unternehmen, z. B. Amazon, Microsoft oder SAP, die Blockchain-Plattformen als Dienstleistung zur Verfügung stellen.¹⁴

Neue Technologien stellen in der Regel eine Herausforderung für die Rechtsordnung dar. Legislative Entwicklungen im Hinblick auf allgemeine zivilrechtliche Regeln sind jedoch in naher Zukunft nicht zu erwarten.¹⁵ Dies ist insofern überraschend, als eine Ausarbeitung des Bundestages die rechtliche Bedeutung von Smart Contracts als „bislang ungeklärt“ beschreibt.¹⁶ Dieser Mangel an rechtlicher Klarheit soll mit dieser Untersuchung reduziert werden. Mit ihr wird das Ziel ver-

⁹ Koalitionsvertrag zwischen CDU, CSU und SPD, 2018, S. 124 (Rn. 5825–5827). Der Koalitionsvertrag 2021 zwischen SPD, Bündnis 90/Die Grünen und FDP enthält einen solchen Passus nicht.

¹⁰ Gesetz zur Einführung von elektronischen Wertpapieren (eWpG) v. 2021.

¹¹ Bundestag, Drucksache 19/26925, S. 1.

¹² Verordnung (EU) 2022/858 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über eine Pilotregelung für auf Distributed-Ledger-Technologie basierende Marktinfrastrukturen und zur Änderung der Verordnungen (EU) Nr. 600/2014 und (EU) Nr. 909/2014 sowie der Richtlinie 2014/65/EU, ABl. L 151/1.

¹³ Deutsche Börse, Abwicklung von DLT-basierten Wertpapieren in Zentralbankgeld erfolgreich getestet, <https://www.bundesbank.de/de/presse/pressemitteilungen/abwicklung-von-dlt-basierten-wertpapieren-in-zentralbankgeld-erfolgreich-getestet-861438> (Stand: 16. 01. 2023).

¹⁴ Siehe *Matthes*, in: Braegelmann/Kaulartz (Hrsg.), *Rechtshandbuch Smart Contracts*, S. 37 (39 (Rn. 9)) m. w. N.

¹⁵ Siehe Bundesregierung, *Blockchain-Strategie*, <https://www.bundesregierung.de/breg-de/themen/digitalisierung/blockchain-strategie-1671902> (Stand: 16. 01. 2023).

¹⁶ Bundestag, *Ausarbeitung, Fragen zu Blockchain und Kryptowährungen*, WD 4 – 3000 – 051/18, 2018, S. 11.