

Michael Koenen

Auswertung von Blockchain-Inhalten zu Strafverfolgungszwecken



Nomos

DIKE 

Inhaltsverzeichnis

Abkürzungsverzeichnis	23
Kapitel 1 – Einleitung	29
Kapitel 2 – Die Blockchain-Technologie	33
A. Die Blockchain-Technologie anhand des Bitcoin-Systems	33
I. Historischer Hintergrund von Bitcoin und Blockchain-Technologie	33
II. Funktionsweise und Anwendung von Bitcoin für Nutzer – wie verwendet ein Nutzer Bitcoin?	35
1. Keine Zugangsbeschränkung	36
2. Private Key und Public Key	36
3. Bitcoin Adresse – als Ergebnis einer Hashfunktion	38
4. Hashfunktionen	38
5. Konten	39
6. Bitcoin	40
7. Transaktionen	41
a) „Transaktion 01“	41
b) „Transaktion 02“	42
c) Gültigkeit einer Transaktion	42
8. Blockchain	42
III. Funktionsweise der Blockchain-Technologie – wie wird die Blockchain fortgeschrieben?	43
1. Konsensmechanismus – Governance	44
a) Konnektivität durch Internet und Peer-to-Peer-Netzwerk	44
b) Nodes im Peer-to-Peer Netzwerk – wer schreibt die Blockchain fort?	45
c) Fortschreiben der Blockchain bzw. Bitcoin-Mining – wie wird die Blockchain fortgeschrieben?	46
(1) Überprüfung der Transaktionen – Verhinderung von „Double Spending“	47
(2) Proof-of-Work	48

d) Konsens über Gültigkeit der längsten Kette	49
e) Exkurs – Andere Konsensmechanismen	49
2. Unveränderlichkeit der Blockchain	50
IV. Öffentliche Verfügbarkeit der Blockchain-Daten als Folge dieser Funktionsweise der Blockchain-Technologie	52
V. Zwischenergebnis	52
B. Die Blockchain-Technologie außerhalb des Bitcoin- und Kryptowährungskontextes	53
I. Nicht die „eine“ Blockchain	53
II. Transaktions- und Dokumentationsfunktion	54
1. Transaktionsfunktion	54
2. Dokumentationsfunktion	55
III. Blockchain-Technologie ist dezentrale Datenverwaltungsstruktur	55
IV. Differenzierung von Blockchain-Technologien und thematische Beschränkung	56
1. Ausgangspunkt: Offene, genehmigungsfreie, pseudonymisierte Blockchain	56
2. Abweichung 1: geschlossene Blockchain	56
3. Abweichung 2: genehmigungsbedürftige Blockchain	57
4. Abweichung 3: Blockchain mit unmittelbarem Personenbezug	57
5. Beschränkung der Untersuchung auf offene Blockchains	57
C. Weitere blockchain-basierte Anwendungen	58
I. Virtuelle Kryptowährungen	58
1. Bitcoin-Cash	59
2. Litecoin	59
3. Libra / Diem – FacebookCoin	60
II. Smart Contracts	61
1. Was ist ein Smart Contract und wie funktioniert er?	61
a) Ziel und Funktion eines Smart Contracts	61
b) (Versuch einer) Definition eines Smart Contracts	62
c) Die Blockchain-Technologie bei Smart Contracts	62
2. Die „Ethereum“-Blockchain als Grundlage von Smart Contracts	63
3. Was sind ICOs – „Initial Coin Offerings“?	65

4. Smart-Contract-Beispiele	65
a) The DAO	65
b) Lition	66
c) Fizzy – Flugverspätungsversicherung	67
d) „Bitsong“ und „KodakOne“ – Musik- und Fotoindustrie	68
e) Zwischenergebnis	68
III. Öffentliche Verwaltung	69
D. Zwischenergebnis	69
Kapitel 3 – Technische Auswertungs- und Ermittlungsmöglichkeiten bei Blockchain-Systemen	71
A. Auswertung der Blockchain-Daten	73
I. Entitäts-Clustering	74
1. Multi-Input-Clustering	74
2. Change- und Shadow-Clustering	76
3. Behavioural Clustering	78
4. Probleme der Entitäts-Clustering-Methoden	78
5. Zwischenergebnis	80
II. Aufdecken von bestimmtem Transaktionsverhalten	80
III. Vergleich mit bekanntem Transaktionsverhalten	81
1. Betrugs-Transaktionen	81
2. Transaktionen bei Schneeballsystemen	82
3. Kategorisierung von Entitäten – Labelling	83
IV. Zwischenergebnis	85
B. Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens	85
I. Grundsatz – Auswertung der Verbreitung von Transaktionsnachrichten	86
II. Das Tor-Netzwerk – IP-Adressen-Verschleierung und Auswertungsmöglichkeit	87
1. Technische Funktionsweise des Tor-Netzwerks	87
2. IP-Adressen-Ermittlung trotz des Tor-Netzwerks	88
3. Auswertung des Datenverkehrs	89
III. Bloom-Filter-Attacks	90
IV. Zwischenergebnis	92

C. Auswertung durch Verknüpfung mit anderweitig verfügbaren Daten	93
I. Durchsuchen des Internets nach Bitcoin-Adressen	93
II. Auswertung von Dritt-Anbieter-Cookies	94
III. Standortdaten-Ermittlung bei IoT-Blockchain-Anwendungen	95
IV. Zwischenergebnis	96
D. Zwischenergebnis	97
Kapitel 4 – Grundrechtsrelevanz der Auswertungen von Blockchain-Systemen	99
A. Blockchain-Ermittlungen in der Praxis	99
B. Betroffene Grundrechte	101
I. Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG	104
1. Schutzbereich	105
a) Schutzbereichsbegrenzung auf menschlich veranlasste Kommunikation	107
b) Zeitliche Schutzbereichsbegrenzung – nur fortlaufende Telekommunikation	109
c) Schutzbereichsbegrenzung auf Individualkommunikation	111
(1) Abgrenzungsschwierigkeiten bei Internetkommunikation als Massen- oder Individualkommunikation	111
(2) Rechtsprechung des BVerfGE	113
i. BVerfGE 120, 274 ff. – Online-Durchsuchungsvorschriften des Verfassungsschutzgesetzes NRW (VSG NRW)	113
ii. BVerfGE NJW 2016, 3508 ff. – Überwachung der Internetnutzung im Ermittlungsverfahren	115
iii. Zwischenergebnis – Rechtsprechung des BVerfGE zum Telekommunikationsgeheimnis	116
(3) Literatur-Ansichten	116
i. Zugangssicherungen als Indiz für Individualkommunikation	116
ii. Individuelle Adressierung der Nachricht	117

iii. Inhalte, die für jedermann zugänglich sind	117
(4) Auseinandersetzung mit den vorstehenden Ansichten	118
(5) Zwischenergebnis – Telekommunikationsgeheimnis nur bei einem unautorisierten Zugriff von außen auf Telekommunikation	122
d) Schutzbereich des Telekommunikationsgeheimnisses beim Be- oder Verhindern von (vertraulicher) Kommunikation	123
(1) Verhindern von Telekommunikation im Schutzbereich des Art. 10 Abs. 1 GG?	123
(2) Verschlüsseln von Telekommunikation im Schutzbereich des Art. 10 Abs. 1 GG	129
(3) Zwischenergebnis	131
e) Zwischenergebnis – Schutzbereich des Telekommunikationsgeheimnisses	131
2. Ist der Schutzbereich des Telekommunikationsgeheimnisses bei den dargestellten Auswertungsmöglichkeiten eröffnet?	132
a) Transaktionsdaten in Blockchains als geschützte Telekommunikation?	132
(1) Blockchain-Inhalte als menschlich veranlasste Telekommunikation	133
(2) Blockchain-Inhalte als fortlaufende oder außerhalb des Herrschaftsbereichs des Betroffenen gespeicherte Telekommunikation	136
(3) Blockchain-Inhalte als Individual- oder Massenkommunikation?	137
(4) Zwischenergebnis – Blockchain-Inhalte sind keine geschützte Telekommunikation	138
b) Netzwerkverbindungen und Netzwerkverhalten als geschützte Telekommunikation?	138
(1) Auswertung der Verbreitung von Transaktionsnachrichten	139
(2) Bloom-Filter-Attacks	140
(3) Verhindern der Verbindung über das Tor-Netzwerk	141

(4) Auswertung des Datenverkehrs durch Ausnutzen der technischen Funktionsweise des Tor-Netzwerks	145
(5) Zwischenergebnis	145
c) Anderweitig verfügbare Daten als geschützte Telekommunikation	146
(1) Durchsuchen des Internets nach Bitcoin-Adressen	146
(2) Auswertung von Dritt-Anbieter-Cookies	146
(3) Standort-Daten-Ermittlung bei IoT-Blockchain-Anwendungen	147
d) Zwischenergebnis	148
3. Zwischenergebnis	148
II. Recht auf informationelle Selbstbestimmung – „RiS“	148
1. Schutzbereich	149
a) Herleitung des RiS – insbesondere Volkszählungsurteil des BVerfGE	149
b) Schutz von personenbezogenen Daten	150
(1) Rechtsprechung des BVerfG	151
(2) „Bestimmbarkeit“ im Datenschutzrecht	153
(3) Anwendbarkeit dieser Maßstäbe im Verfassungsrecht	156
(4) Zwischenergebnis	158
c) Ausgewertete Daten als personenbezogene Daten?	158
(1) Unmittelbare Blockchain-Daten	159
(2) Daten über Netzwerkverbindungen und Netzwerkverhalten	163
(3) Anderweitig verfügbare Daten	163
d) (Umstrittene) Erfassung öffentlich verfügbarer Daten	164
(1) Begriffsbestimmung öffentlich verfügbarer Daten	165
(2) Erfassung öffentlich verfügbarer Daten?	165
e) Zwischenergebnis	167
2. Eingriff	167
a) Grundsatz – Eingriffe in das RiS	167

b) Eingriff bei öffentlich verfügbaren/allgemein zugänglichen Daten	168
(1) Rechtsprechung des BVerfG	169
i. BVerfGE 120, 274 ff. – VSG NRW	169
ii. BVerfGE 120, 351 ff. – Datensammlung über steuerliche Auslandsbeziehungen	171
iii. BVerfGE 120, 378 ff. – Automatisierte Kfz- Kennzeichenerfassung	171
iv. BVerfGE 150, 244 ff. – Automatisierte Kfz- Kennzeichenerfassung II	172
v. Zwischenergebnis	177
(2) Eingriffseinschränkungen und -erweiterungen in der Literatur	178
i. Bagatellvorbehalt	178
ii. Grundrechtsverzicht	179
iii. Eingriffserweiterung bei Kenntnisnahme sozialer Netzwerke?	180
(3) Zwischenergebnis	182
c) Liegt durch die dargestellten Auswertungsmethoden ein Eingriff in das RiS in diesem Sinne vor?	184
(1) Auswertung der unmittelbaren Blockchain- Daten	185
(2) Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens	186
(3) Auswertung anderweitig verfügbarer Daten	187
d) Zwischenergebnis	187
3. Zwischenergebnis	187
III. Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme – „IT-Grundrecht“	188
1. Herleitung und Begründung des IT-Grundrechts	189
2. Schutzbereich des IT-Grundrechts	191
a) Schutzgegenstand – Informationstechnische Systeme	191
b) Schutz der Vertraulichkeit verarbeiteter Daten und der Integrität des informationstechnischen Systems	192
c) Literaturauffassungen zum Schutzbereich des IT- Grundrechts	193
d) Zwischenergebnis	193

3. Blockchain-Systeme als geschützte informations-technische Systeme?	194
a) Auswertung der Blockchain-Daten	195
b) Auswertung des Netzwerkverhaltens	197
c) Verhinderung der Verbindung über das Tor-Netzwerk	198
d) Auswertung des Datenverkehrs mittels Tor-Netzwerk	199
e) Bloom-Filter-Attacks	199
f) Auswertung anderweitig verfügbarer Daten	200
4. Zwischenergebnis	200
IV. Zwischenergebnis	201
C. Zusammenfassung	201
Kapitel 5 – Verfassungsrechtliche Rechtfertigung	203
A. Auswertungsmethoden in der Ermittlungspraxis	204
I. Einsatz zur Verdachtsbegründung	205
II. Einsatz zur Ermittlung nach bestehendem Verdacht	207
III. Einsatz von Ermittlungsmethoden, durch die unmittelbar ein Anfangsverdacht begründet werden kann	208
IV. Zwischenergebnis	209
B. Einschlägige Ermächtigungsgrundlage in der StPO	210
I. §§ 94, 110 StPO – Sicherstellung, Beschlagnahme, Durchsuchung und Durchsicht	211
1. § 94 StPO – Sicherstellung bzw. Beschlagnahme	212
a) Keine unmittelbare Einschlägigkeit von § 94 StPO	212
b) Keine Minus-Maßnahme der Beschlagnahme	214
c) Zwischenergebnis	216
2. § 110 StPO – Durchsicht von Papieren und elektronischen Speichermedien	216
II. § 98a StPO – Rasterfahndung	217
1. „Herkömmliche“ Rasterfahndung – Historie und Praxis	219
2. Maschineller Datenabgleich im Sinne des § 98a Abs. 1 StPO	223

3. Rasterfahndung nur beim Abgleich der Daten mehrerer Speicherstellen im Verantwortungsbereich der Strafverfolgungsbehörden	225
a) BVerfG NJW 2009, 1405ff. – Abfrage von Kreditkartendaten	226
b) OLG Stuttgart NStZ 2001, 158 f.; OLG Köln NStZ -RR 2001, 31f – Entschädigung für Auskunft durch Telekommunikationsanbieter	228
c) Herrschende Literaturauffassung	229
d) Begründung des Bundestages	230
e) Abweichende Literaturauffassungen	230
f) Kritische Würdigung	232
(1) Erstellen von Persönlichkeitsbildern	233
(2) Streubreite	236
(3) Gesetzesbegründung des Bundestages	238
(4) Abweichende Literaturauffassungen	239
(5) Zwischenergebnis	240
g) Lösungsvorschlag – Rasterfahndung nur dann, wenn personenbezogene Daten eines unbestimmten Personenkreises abgefragt werden	241
h) Zwischenergebnis	243
i) Anwendung dieser Abgrenzung für die hier gegenständlichen Auswertungsmethoden	243
(1) Clustering-Verfahren aus Kap. 3, A.I., II.	243
(2) Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens	244
(3) Auswertung anderweitig verfügbarer Daten	246
(4) Zwischenergebnis	246
4. Datengrundlage der Rasterfahndung	246
a) Personenbezogene Daten im Sinne des § 98a Abs. 1 StPO	246
b) Andere Daten im Sinne des § 98a Abs. 1 StPO	247
(1) Herrschende Literaturauffassung	247
(2) Kritische Würdigung	249
i. Binnensystematik des § 98a StPO	249
ii. Systematisches Verhältnis zu § 98c StPO	251
iii. EDV-gestützte Auswertung von Informationen	251

iv. Auswertung öffentlich verfügbarer Daten	252
v. Zwischenergebnis	253
(3) Zwischenergebnis	253
(4) Daten der Blockchain-Auswertungsmethoden als andere Daten im Sinne des § 98a Abs. 1 StPO	254
i. Öffentlich verfügbare Daten als freiwillig herausgegebene Daten?	254
ii. Daten, die nach § 98a Abs. 2 StPO erhoben wurden?	255
iii. Entsprechende Anwendung des § 98a Abs. 2 StPO?	256
c) Zwischenergebnis	257
5. Zwischenergebnis	257
III. § 98c StPO – Maschinelles Datenabgleich	258
IV. § 100a StPO – Telekommunikationsüberwachung	259
V. § 100b StPO – Online-Durchsuchung	261
VI. § 100g StPO – Erhebung von Verkehrsdaten	263
VII. § 100j StPO – Bestandsdatenauskunft	265
VIII. §§ 161, 163 StPO – Ermittlungsgeneralklauseln	266
IX. Zwischenergebnis	269
C. Verfassungsmäßigkeit der Ermittlungsgeneralklauseln §§ 161, 163 StPO	270
I. Zitiergebot des Art. 19 Abs. 1 S. 2 GG	270
1. Anforderungen des Zitiergebotes	270
2. Das Zitiergebot bei der Ermittlungsgeneralklausel des § 161 StPO	273
II. Verbot des Einzelfallgesetzes, Art. 19 Abs. 1 S. 1 GG	274
III. Wesensgehaltsgarantie, Art. 19 Abs. 2 GG	275
IV. Parlamentsvorbehalt und Wesentlichkeitslehre	277
V. Bestimmtheitsgebot	278
VI. Verhältnismäßigkeitsgrundsatz	281
1. Legitimer Zweck, Geeignetheit und Erforderlichkeit	282
2. Verhältnismäßigkeit im engeren Sinne bzw. Angemessenheit	283
VII. Zwischenergebnis	284

D. Können die gegenständlichen Auswertungsmethoden zulässigerweise auf §§ 161, 163 StPO gestützt werden?	284
I. Anfangsverdacht	285
1. Voraussetzungen eines Anfangsverdachts	286
a) Kein Anfangsverdacht beim proaktiven Aufklären von Dunkelfeldern	286
b) Objektive Anhaltspunkte	286
c) Hindeuten auf eine konkrete Straftat	287
d) Exkurs – Vorermittlungen	288
e) Exkurs – Strafverfolgungsvorsorge	291
f) Legales Verhalten zur Begründung eines Anfangsverdachts?	293
g) BVerfG NJW 2009, 1405ff. – Abfrage von Kreditkartendaten	294
h) Zwischenergebnis	294
2. Anfangsverdacht bei der Anwendung der Auswertungsmethoden	295
a) Einsatz zur Verdachtsbegründung	295
b) Einsatz zur Ermittlung nach bestehendem Verdacht	296
c) Einsatz von Ermittlungsmethoden, durch die unmittelbar ein Anfangsverdacht begründet werden kann	296
(1) Verwertung von Daten aus einzelnen, vorangegangenen Strafverfahren	298
(2) Anfangsverdacht bei abstrakten Transaktionsmustern	300
d) Zwischenergebnis	301
e) Exkurs – verdachtsbegründender Einsatz als zulässige Vorermittlungen?	302
II. Lediglich geringfügiger Grundrechtseingriff	302
1. Herkömmliche Ermittlungsmaßnahmen, die wohl nach § 161 Abs. 1 StPO zulässig sind	303
a) Einfache Fahndungsmaßnahmen und kurzfristige Observationen	304
(1) Vergleich mit der Rasterfahndung, § 98a StPO	305
(2) Vergleich mit der Einrichtung von Kontrollstellen und Kontrollfahndung, §§ 111, 163d StPO	307

(3) Vergleich mit längerfristiger Observation, § 163f StPO	311
(4) Vergleich mit Ausschreibung zur polizeilichen Beobachtung, § 163e StPO	313
(5) Zwischenergebnis	314
b) Erkundigungen im Umfeld einer Person und Vernehmungen von Zeugen, Sachverständigen und dem Beschuldigten	315
c) Einsatz von V-Leuten, Scheinkäufern und nicht offen ermittelnden Polizeibeamten	315
d) Insbesondere: Online-Ermittlungen	318
(1) Gegenstand der Online-Ermittlung	318
(2) Ähnliche, spezielle Ermittlungsbefugnisse	320
(3) Exkurs – Grenze der nach § 161 Abs. 1 StPO zulässigen Online-Ermittlungen	321
(4) Zwischenergebnis	323
e) Abfragen von Kontoinformationen im Rahmen Europäischer Rechtshilfe	323
f) Zwischenergebnis	326
2. Rechtsprechung des BVerfG zu Kriterien und Bewertung der Grundrechtsintensität	328
a) Art der erfassten Informationen	328
b) Anlass und Umstände der Erhebung	329
(1) Intensitätsverringering bei öffentlich verfügbaren Daten?	331
(2) Zwischenergebnis	334
c) Art der Verwertung der erhobenen Daten	335
d) Zwischenergebnis	336
3. Bewertung der Grundrechtsintensität der hier gegenständlichen Maßnahmen	337
a) Entitätsclustering	337
(1) Grundrechtsintensität, die bei beiden Einsatzmöglichkeiten vorliegt	338
(2) Unterschiedliche Grundrechtsintensität	342
(3) Abschließende Bewertung der Grundrechtsintensität	345
b) Aufdecken von auffälligem Transaktionsverhalten	346

c) Vergleich mit bekanntem Transaktionsverhalten	349
(1) Exkurs – Grundrechtsintensität beim Einsatz zum Aufdecken von Transaktionsmustern, die auf bestimmte Straftaten hindeuten	353
(2) Zwischenergebnis	356
d) Auswertung des Netzwerkverhaltens und der Netzwerkverbindungen	356
(1) Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten	357
(2) Auswertung der Verbreitung von Transaktionsnachrichten, wenn zusätzlich eine Verbindung über das Tor-Netzwerk verhindert wird	361
(3) Auswertung des Datenverkehrs des Tor-Netzwerks	361
(4) Bloom-Filter-Attacks	362
(5) Zwischenergebnis	364
e) Auswertung durch Verknüpfung mit anderweitig verfügbaren Daten	365
(1) Durchsuchen des Internets nach Bitcoin-Adressen	365
(2) Auswertung von Dritt-Anbieter-Cookies	366
(3) Standortdaten-Ermittlung bei IoT-Blockchain-Anwendung	366
f) Kombination von Auswertungsmethoden	367
g) Zwischenergebnis	367
4. Zwischenergebnis	369
III. Zwischenergebnis	369
E. Zusammenfassung	370
F. Lösungsvorschlag – § 98a Abs. 2 S. 2 StPO-E	371
Kapitel 6 – Exkurs – Datenschutzrechtliche Einordnung (privater) Auswertungen von Blockchain-Systemen	375
A. Anwendungsbereich der DSGVO	375
I. Verarbeitung personenbezogener Daten	376
1. Personenbezogene Daten nach Art. 4 Nr. 1 DSGVO	376
2. Verarbeitung	379
II. Kein Ausnahmetatbestand des Art. 2 Abs. 2 DSGVO	381

III. Exkurs – Private Ermittlungen im Zusammenhang mit Straftaten und Kooperationen zwischen Strafverfolgungsbehörden und Privaten	383
IV. Zwischenergebnis	385
B. Rechtmäßigkeit der Datenverarbeitung	385
I. Art. 6 Abs. 1 lit. a) – Einwilligung des Betroffenen	386
II. Art. 6 Abs. 1 lit. f) DSGVO – Wahrnehmung berechtigter Interessen	388
III. Zwischenergebnis	393
C. Zusammenfassung	394
Kapitel 7 – Schlussbetrachtung	397
A. Die Blockchain-Technologie und ihre Auswertbarkeit	397
B. Die Auswertungsmethoden als Eingriff in das Recht auf informationelle Selbstbestimmung	399
C. Verfassungsrechtliche Rechtfertigung dieses Eingriffs	402
I. § 161 Abs. 1 StPO als einschlägige Ermittlungsbefugnis	402
II. Einsatz der Auswertungsmethoden nur bei bestehendem Anfangsverdacht	403
III. Nur geringfügige Grundrechtseingriffe nach § 161 Abs. 1 StPO	403
D. Empfehlung und Ausblick	406
Stichwortverzeichnis zu technischen Begriffen	409
Literaturverzeichnis	413