

Daniel Drescher

Blockchain Grundlagen

Eine Einführung in die elementaren
Konzepte in 25 Schritten

Übersetzung aus dem Englischen
von Guido Lenz



mitp

Inhaltsverzeichnis

	Einleitung	13
	Über den Autor	19
	Über den Fachlektor	19
Teil I	Fachbegriffe und technische Grundlagen	21
1	Denken in Schichten und relevanten Aspekten	23
	Die Metapher	23
	Schichten eines Softwaresystems	24
	Gleichzeitiges Betrachten von zwei Schichten	25
	Integrität	26
	Ausblick	26
	Zusammenfassung	27
2	Das große Ganze	29
	Die Metapher	29
	Ein Zahlungssystem	29
	Zwei Arten von Softwarearchitektur	30
	Vorteile verteilter Systeme	31
	Nachteile verteilter Systeme	32
	Verteilte Peer-to-Peer-Systeme	34
	Vermischen von zentralisierten und verteilten Systemen	34
	Identifizieren verteilter Systeme	35
	Der Zweck der Blockchain	36
	Ausblick	36
	Zusammenfassung	37
3	Erkennen des Potenzials	39
	Die Metapher	39
	Wie ein Peer-to-Peer-System eine ganze Branche revolutionierte ...	40
	Das Potenzial von Peer-to-Peer-Systemen	40

	Fachbegriffe und die Verbindung zur Blockchain	42
	Das Potenzial der Blockchain	43
	Ausblick	44
	Zusammenfassung	44
Teil II	Warum die Blockchain benötigt wird	47
4	Erkennen des Kernproblems	49
	Die Metapher	49
	Vertrauen und Integrität in Peer-to-Peer-Systemen	49
	Bedrohungen der Integrität in Peer-to-Peer-Systemen	50
	Das Kernproblem, das die Blockchain lösen soll	51
	Ausblick	51
	Zusammenfassung	52
5	Begriffserklärung	53
	Der Begriff	53
	Die Verwendung des Begriffs in diesem Buch	54
	Vorläufige Definition	55
	Die Rolle der Eigentumsverwaltung	55
	Das Einsatzgebiet der Blockchain in diesem Buch	56
	Ausblick	56
	Zusammenfassung	56
6	Grundlagen zur Beschaffenheit des Eigentums	59
	Die Metapher	59
	Eigentum und Zeugen	59
	Grundlagen des Eigentums	60
	Ein kleiner Abstecher in die Sicherheit	62
	Zwecke und Eigenschaften eines Hauptbuchs	64
	Eigentum und die Blockchain	65
	Ausblick	66
	Zusammenfassung	66
7	Geld zweimal ausgeben	69
	Die Metapher	69
	Das Double-Spending-Problem	69
	Double-Spending: Begriffsdefinition	70
	Wie sich das Double-Spending-Problem lösen lässt	71

	Die Verwendung von Double-Spending in diesem Buch.	73
	Ausblick	73
	Zusammenfassung	73
Teil III Wie die Blockchain funktioniert		75
8	Planen der Blockchain.	77
	Das Ziel	77
	Ausgangspunkt	77
	Der Weg zum Ziel.	78
	Ausblick	81
	Zusammenfassung	81
9	Dokumentieren von Eigentum.	83
	Die Metapher	83
	Das Ziel	83
	Die Herausforderung	84
	Die Idee	84
	Ein kleiner Abstecher in Bestands- und Transaktionsdaten	84
	Funktionsweise	84
	Warum das funktioniert	86
	Bedeutung der Reihenfolge	86
	Integrität der Transaktionshistorie.	86
	Ausblick	88
	Zusammenfassung	88
10	Anwenden von Hashfunktionen auf Daten.	89
	Die Metapher	89
	Das Ziel	89
	Funktionsweise	89
	Ausprobieren	91
	Schemata zum Anwenden von Hashfunktionen auf Daten.	93
	Ausblick	97
	Zusammenfassung	97
11	Hashfunktionen in der Realität	99
	Vergleichen von Daten	99
	Erkennen von Änderungen an Daten	100
	Veränderungssensitive Referenzen auf Daten	101

	Veränderungssensitives Speichern von Daten	103
	Verursachen zeitaufwendiger Berechnungen	106
	Verwenden von Hashfunktionen in der Blockchain	109
	Ausblick	110
	Zusammenfassung	110
12	Identifizieren und Schützen von Anwenderkonten	111
	Die Metapher	111
	Das Ziel	112
	Die Herausforderung	112
	Die Idee	112
	Ein kleiner Abstecher in die Kryptographie	112
	Asymmetrische Kryptographie in der Realität	116
	Asymmetrische Kryptographie in der Blockchain	117
	Ausblick	118
	Zusammenfassung	118
13	Autorisieren von Transaktionen	121
	Die Metapher	121
	Das Ziel	122
	Die Herausforderung	122
	Die Idee	122
	Ein kleiner Abstecher in digitale Signaturen	122
	Funktionsweise	125
	Warum das funktioniert	126
	Ausblick	126
	Zusammenfassung	127
14	Speichern von Transaktionsdaten	129
	Die Metapher	129
	Das Ziel	129
	Die Herausforderung	130
	Die Idee	130
	Transformieren eines Buchs in eine Blockchain-Datenstruktur ...	130
	Die Blockchain-Datenstruktur	135
	Speichern von Transaktionen in der Blockchain-Datenstruktur ...	137
	Ausblick	139
	Zusammenfassung	139

15	Verwenden des Datenspeichers	141
	Die Metapher	141
	Eintragen neuer Transaktionen	142
	Erkennen von Änderungen	144
	Ordnungsgemäßes Ändern von Daten	147
	Absichtliche und unabsichtliche Änderungen	148
	Ausblick	149
	Zusammenfassung	149
16	Schützen des Datenspeichers	151
	Die Metapher	151
	Das Ziel	152
	Die Herausforderung	152
	Die Idee	152
	Ein kleiner Abstecher in die Unveränderlichkeit	153
	Funktionsweise: Das große Ganze	153
	Funktionsweise: Die Details	154
	Warum das funktioniert	157
	Die Kosten für das Manipulieren der Blockchain-Datenstruktur ...	157
	Der unveränderliche Datenspeicher in der Realität	157
	Ausblick	158
	Zusammenfassung	158
17	Verteilen des Datenspeichers unter den Peers	161
	Die Metapher	161
	Das Ziel	161
	Die Herausforderung	162
	Die Idee	162
	Funktionsweise: Die Übersicht	163
	Funktionsweise: Die Details	164
	Warum das funktioniert	166
	Ausblick	166
	Zusammenfassung	166
18	Überprüfen und Eintragen von Transaktionen	169
	Die Metapher	169
	Das Ziel	170
	Die Herausforderung	171

	Die Idee.	171
	Funktionsweise: Die Bausteine.	171
	Funktionsweise: Der Rahmen.	175
	Funktionsweise: Die Details.	175
	Warum das funktioniert.	176
	Umgang mit unehrlichem Verhalten.	177
	Ausblick.	178
	Zusammenfassung.	178
19	Auswählen einer Transaktionshistorie.	181
	Die Metapher.	181
	Das Ziel.	181
	Die Herausforderung.	182
	Die Idee.	182
	Funktionsweise.	184
	Folgen der Entscheidung für eine Kette.	189
	Bedrohungen für das Abstimmverhalten.	193
	Die Rolle des Hashpuzzles.	194
	Warum das funktioniert.	194
	Ausblick.	194
	Zusammenfassung.	195
20	Die Kosten der Integrität.	197
	Die Metapher.	197
	Die Rolle der Gebühren innerhalb der Blockchain.	198
	Wünschenswerte Merkmale eines Zahlungsmittels für die Kompensation von Peers.	199
	Ein Abstecher in die Ursprünge der Kryptowährungen.	200
	Ausblick.	201
	Zusammenfassung.	201
21	Das Gesamtbild entsteht.	203
	Vertiefung der Konzepte und Technologien.	203
	Was ist die Blockchain?	205
	Der Zweck der Blockchain: Funktionale Aspekte der Anwendungsschicht.	205
	Eigenschaften der Blockchain: Nichtfunktionale Aspekte.	206
	Interne Funktionsweise: Funktionale Aspekte der Implementierungsschicht.	208
	Abstraktion.	212

	Ausblick	213
	Zusammenfassung	213
<hr/>		
Teil IV	Beschränkungen und wie man sie überwindet	215
<hr/>		
22	Erkennen der Beschränkungen	217
	Die Herausforderung	217
	Technische Beschränkungen der Blockchain	217
	Nicht technische Beschränkungen der Blockchain	221
	Überwinden der Beschränkungen	222
	Ausblick	222
	Zusammenfassung	223
23	Neuerfindung der Blockchain	225
	Die Metapher	225
	Widersprüchliche Ziele der Blockchain	225
	Die Ursachen der Konflikte	226
	Lösen der Widersprüche	227
	Vier Versionen der Blockchain	228
	Folgen	228
	Der Zweck der Blockchain auf dem Prüfstand	230
	Die Verwendung des Begriffs Blockchain im weiteren Verlauf dieses Buchs	231
	Ausblick	231
	Zusammenfassung	231
<hr/>		
Teil V	Verwenden der Blockchain, Zusammenfassung und Ausblick ...	233
<hr/>		
24	Verwenden der Blockchain	235
	Die Metapher	235
	Eigenschaften der Blockchain	235
	Allgemeine Anwendungsmuster	236
	Besondere Anwendungsfälle	238
	Untersuchen von Blockchain-Anwendungen	239
	Ausblick	243
	Zusammenfassung	243

25	Zusammenfassung und Zukunftsausblick	245
	Die Metapher	245
	Weiterentwicklungen und Alternativen	246
	Errungenschaften der Blockchain	251
	Mögliche Nachteile	254
	Die Zukunft	255
	Ausblick	257
	Zusammenfassung	257
	Stichwortverzeichnis	259