
Hans-Georg Fill · Andreas Meier

Blockchain kompakt

Grundlagen,
Anwendungsoptionen und
kritische Bewertung

Unter Mitwirkung von Matthias Egli,
Mark Fenwick, Daniel Gerber, Felix Härer,
Tim Niemer, Edy Portmann,
Sarah Röthlisberger, Anton Sentic,
Bernd Teufel und Stefan Wrbka

 Springer Vieweg

Inhaltsverzeichnis

1	Motivation Betrugsprävention	1
	Literatur.	4
2	Grundlagen zur Blockchain-Technologie	5
2.1	Hash-Funktionen	6
2.2	Merkle-Bäume und Merkle-Proofs	8
2.3	Digitale Signaturen	11
	Literatur.	15
3	Aufbau und Funktion der Blockchain	17
3.1	Datenstruktur der Blockchain	18
3.2	Auswirkungen bei Blockchain-Änderung	20
3.3	Zufallsauswahl und Kryptografisches Puzzle	22
3.4	Das Kriterium der längsten Blockkette	26
	Literatur.	29
4	Anwendungsoptionen	31
4.1	Kryptowährungen.	32
4.1.1	Initial Coin Offering	34
4.1.2	Coins und Tokens	35
4.1.3	Software-Komponenten von Kryptowährungen.	39
4.1.4	Geld-Transaktionen in der Blockchain.	41
4.1.5	Ausblick	45
4.2	Identity Management	49
4.2.1	Zentrales versus dezentrales Identitätsmanagement.	50

	4.2.2	Identitätsmanagement-Systeme	
	4.2.3	Zukunftsperspektive	
4.3		Smart Contracts	
	4.3.1	Smart Contracts als Programmcode	
	4.3.2	Plattformen für Smart Contracts.	
	4.3.3	Solidity – Sprache für Smart Contracts in Ethereum	
	4.3.4	Oracles zur Integration externer Daten.	
	4.3.5	Tokens.	
	4.3.6	Ausblick und Limitationen.	
4.4		Smart Grids	
	4.4.1	Das Stromnetz	
	4.4.2	Einführung von Blockchain im Energiebereich	
	4.4.3	Überblick Blockchain-Projekte im Microgrid-Bereich	
	4.4.4	Chancen und Risiken	
	4.4.5	Ausblick	
4.5		Digitale Stimmzettel	
	4.5.1	Anforderung an ein elektronisches Wahlsystem	
	4.5.2	Klassifikation Blockchain-basierter E-Voting-Systeme.	
	4.5.3	E-Voting-Protokoll mit blinden Signaturen.	
	4.5.4	Spannungsfeld zwischen MyPolitics und OurPolitics.	
	4.5.5	Chancen und Risiken	
4.6		Smart Cities	
	4.6.1	Begriffsbildung Smart und Cognitive City	
	4.6.2	Herausforderungen für digitale urbane Räume.	1
	4.6.3	Einsatz von Blockchain bei der Schweizerischen Post.	1
	4.6.4	Lessons Learned.	1
	4.6.5	Ausblick	1
		Literatur.	1

...	51	5 Rechtliche Fragen	119
...	54	Mark Fenwick und Stefan Wrba	
...	54	5.1 Smart Contracts	120
...	55	5.2 Kryptoobjekte	125
...	57	5.3 Regulierungsdesigns	129
		Literatur	131
...	60	6 Kritische Einschätzung	133
...	62	Literatur	136
...	66		
...	70	Glossar	137
...	72		
...	73	Stichwortverzeichnis	141
...	79		
...	82		
...	85		
...	86		
...	87		
...	87		
...	89		
...	90		
...	95		
...	97		
...	99		
...	100		
...	103		
...	107		
...	110		
...	111		
...	113		