
Elfriede Sixt

Bitcoins und andere dezentrale Transaktionssysteme

Blockchains als Basis einer
Kryptoökonomie

 Springer Gabler

Inhaltsverzeichnis

1	Kryptoökonomie	1
2	Was sind Kryptotransaktionssysteme?	5
2.1	Hintergrund und philosophische Betrachtung	5
2.2	Definitionen	8
3	Aktuelle Daten zur Bitcoin-Ökosphäre	17
3.1	Google Trend-Analyse	17
3.2	Anzahl der Transaktionen pro Tag	18
3.3	Entwicklung des Wertes des bitcoin	20
3.4	Anzahl der Projekte auf GitHub	21
3.5	Anzahl der Wallets und Anzahl der Nutzer	22
3.6	Akzeptanz des bitcoins bei den Unternehmen	23
3.7	Akzeptanz beim Konsumenten	23
3.8	Venture-Capital	25
3.9	Bitcoin als Netzwerkgut	26
3.10	Zusammenfassung	27
4	Funktionsweise des Bitcoin-Netzwerks	29
4.1	Dezentralität und Digitalität des Systems	31
4.2	Bedeutung des angewandten Konsens-Algorithmus	31
4.3	(Pseudo-)Anonymität	32
4.4	Bitcoin-Clients und Wallets	34
4.4.1	Bitcoin Core Client/Full-Node Client	34
4.4.2	Sonstige Bitcoin-Clients/Thin-/Light-Clients	36
4.4.3	Wallets/Nutzer des Bitcoin-Netzwerks	36
4.5	Durchführung von Transaktionen im Netzwerk	37
4.5.1	Validierung einer Transaktion im Bitcoin-Netzwerk	39
4.5.2	Aufbau und Funktionsweise der Blockchain	39
4.5.3	Double Spending-Attacke und der Konsens-Algorithmus	43
4.6	Scripte	44

5	Vergleich zum herkömmlichen Finanzsystem	45
5.1	Grundfunktionen des Geldes	47
5.2	Die Geschichte des Geldes	47
5.2.1	Historische Entwicklung des Geldwesens	47
5.2.2	Gold- und Dollarbindung	50
5.2.3	Schaffung von Buchgeld (auch Giralgeld)	51
5.3	Die historische Entwicklung der Geldtheorien	53
5.3.1	Metallismus vs. Chartalismus	53
5.4	Entwicklung der Geldtheorien	55
5.4.1	Klassische Geldtheorie	55
5.4.2	Keynesianische Geldtheorie	56
5.4.3	Neoklassische Geldtheorie	56
5.4.4	Monetarismus	56
5.4.5	Neuklassische Geldtheorie	57
5.4.6	Neukeynesianische Geldtheorie	58
5.5	Bedeutung dieser Entwicklungen für die Kryptowährungen	58
5.5.1	Vertrauen als Grundelement auch für moderne Geldsysteme	59
5.6	Komplementärwährungen	63
5.6.1	Alternativwährungen	63
5.6.2	Zentralisierte virtuelle/digitale Währungen	69
5.7	Trend zur bargeldlosen Gesellschaft	71
6	Innovationsbedarf bei den Finanzsystemen	75
7	Bitcoin als Zahlungsmittel	77
7.1	Globalität des Bitcoin-Netzwerks	77
7.1.1	Unbanked People	78
7.1.2	Länder mit dysfunktionalen Finanzsystemen	78
7.1.3	Auswirkung der Digitalisierung	80
7.1.4	Grenzüberschreitende Geldanweisungen	81
7.1.5	Bedeutung des Bitcoin-Netzwerks für diese Ländern	83
7.2	Transaktionskostenthematik	84
7.2.1	Aus Sicht des Konsumenten	85
7.2.2	Aus Sicht eines Unternehmers	86
7.3	Digitale Geschäftsmodelle und Mikrozahlungen	88
8	Limitationen des Bitcoin-Systems	91
8.1	Komplexität	91
8.2	Sicherheit	92
8.3	Skalierbarkeit des Systems	95
8.4	Lange Bestätigungszeiten	99
8.5	Transaktionskosten als Mining-Belohnung	100

8.6	Hoher Ressourcenverbrauch	102
8.7	Aufbau industrieller Miningkapazitäten	103
8.8	51-Prozent-Attacke	105
8.9	Wechselkursvolatilität	107
8.10	Deflation	108
9	Lösungsansätze für die Limitationen des Bitcoin-Systems	111
9.1	Altcoins (Alternative Kryptowährungen)	111
9.1.1	Litecoin	113
9.1.2	Nextcoin und Peercoin	113
9.1.3	Darkcoin	114
9.2	Sidechains	115
9.3	Das Lightning Netzwerk	117
10	Rechtliche Einordnung	119
10.1	Sind Kryptowährungen rechtlich gesehen „Geld“?	119
10.2	Kryptowährungen im Privatrecht und im Grundgesetz	121
10.2.1	Rechtsgeschäfte mit bitcoins	122
10.3	Funktions- und Anlegerschutz	124
10.3.1	Funktionsschutz der Bitcoin-Technologie an sich	126
10.3.2	Funktionsschutz der Unternehmen der Kryptoökonomie	126
10.3.3	Anwendbarkeit der Geldwäscherichtlinien (AML, KYC)	127
10.4	Rechtliche Qualifikation des bitcoins in den verschiedenen Ländern	130
10.4.1	Standpunkt der Aufsichtsbehörden der Europäischen Union	131
10.4.2	Vereinigte Staaten	134
10.4.3	China	137
10.4.4	Sonstige Länder	138
11	Die Gratis-Bitcoin-Ökosphäre	141
12	Monetarismus, Geldmenge und Politik	145
12.1	Cyber-Libertarianism	148
12.2	Geldsysteme und Privatsphäre	149
12.2.1	NSA und PRISM	150
12.2.2	SWIFT und Datenschutz	153
12.2.3	Kryptografie und die Privatsphäre	155
12.3	Nutzung des bitcoin im Darknet	157
12.3.1	Silk Road	158
12.3.2	OpenBazaar	161
13	Bitcoin 2.0	163
13.1	MultiSig-Transaktionen und Treuhandkonstrukte	164
13.2	Overlays oder auch Blockchain 2.0 Anwendungen	165

13.2.1 Colored Coins Projekt	167
13.2.2 Counterparty	168
13.2.3 BitMesh	168
13.2.4 Factom	169
13.2.5 Ascribe	169
13.2.6 Mirror (früher Vaurum)	170
14 Bitcoin und die Finanzindustrie	173
14.1 Private Blockchains oder Permissioned Distributed Ledger	177
14.2 Das Ripple-Netzwerk	179
14.3 Kryptofinanztransaktionen	182
14.3.1 Patrick Byrne mit T0 und FNY Capital	184
14.3.2 Adam Krellenstein mit Symbiont und Counterparty	184
14.3.3 Blythe Masters mit der Digital Assets Holding	185
15 Sonstige mögliche Anwendungsbereiche für dezentrale Transaktionssysteme	187
16 Ethereum	189
Ausblick	195