



Kryptowährung

**Bitcoin**

im Ermittlungsverfahren

Funktionsweise – Recht – Ermittlungsansätze – Hilfen



## Inhaltsverzeichnis

VORWORT.....	3
ABKÜRZUNGSVERZEICHNIS.....	5
INHALTSVERZEICHNIS.....	8
<b>TEIL I VIRTUELLE WÄHRUNGEN.....</b>	<b>11</b>
<b>1 VON DER ENTSTEHUNG ZUM ZAHLUNGSMITTEL.....</b>	<b>11</b>
1.1 DER BEGRIFF KRYPTOWÄHRUNG.....	12
1.2 KRYPTOWÄHRUNGEN RICHTIG GENDERN 😊.....	12
1.3 VON COINS, TOKENS, ASSETS UND SMART-CONTRACTS.....	12
1.4 FINANZTECHNISCHE UND RECHTLICHE EINORDNUNG VIRTUELLER WÄHRUNGEN.....	14
1.4.1 Anwendbarkeit deutschen Rechts.....	14
1.4.2 Zuständigkeit der Bankenaufsicht.....	16
1.4.3 Einstufung als Finanzinstrumente.....	16
1.4.4 Erlaubnispflicht gewerbsmäßigen Handelns.....	17
1.4.5 Urteil des Kammergerichts Berlin – Doch alles anders?.....	20
1.4.6 Bitcoin und das Finanzamt.....	22
<b>TEIL II KRYPTOWÄHRUNG BITCOIN.....</b>	<b>26</b>
<b>2 DIE FUNKTIONSWEISE VON BITCOIN.....</b>	<b>26</b>
2.1 DER ERSTE BITCOIN.....	26
2.2 DAS BITCOIN-NETZWERK.....	29
2.3 SCHLÜSSELPAARE, KRYPTOGRAPHIE UND SEEDS.....	32
2.4 BITCOIN-ADRESSEN.....	33
2.5 BITCOIN-WALLETS.....	36
2.5.1 Hot-Wallets.....	37
2.5.2 Cold-Wallets.....	40
2.5.3 Brain-Wallet.....	45
2.5.4 Behörden-Wallet.....	46
2.6 BITCOIN-TRANSAKTIONEN.....	47
2.7 DIE BLOCKCHAIN – DAS GEMEINSAME KASSENBUCH.....	51
2.7.1 Das Mining.....	52
2.7.1.1 Deflationäre Auslegung des Bitcoin-Systems.....	55
2.7.1.2 Lohnt sich das?.....	55
2.7.2 Der dezentralisierte Konsens.....	57
2.7.3 Aufbau eines Blocks.....	57
2.7.4 Proof-of-Work – der Umweltsünder.....	59
2.7.5 Mining-Hardware.....	63
2.7.6 Mining-Pools.....	65
2.7.7 Proof-of-Stake – die Lösung?.....	66
2.7.8 Fortschreibung der Blockchain.....	67
2.7.8.1 Soft-Forks – Fortführung einer geänderten Blockchain.....	67
2.7.8.2 Hard-Forks – Abspaltung einer neuen Blockchain.....	69
2.7.9 Die 10-Minuten-Regel.....	70
2.8 ANONYMISIERUNG.....	70
2.8.1 The Onion Routing (TOR).....	72
2.8.2 Bitcoin-Mixer und CoinJoin.....	73
2.8.3 Wasabi-Wallet.....	75
2.8.4 Off-Chain-Transaktionen.....	76
2.8.5 Cross-Chain-Transaktionen.....	77
2.8.6 Grenzen der Anonymisierung.....	83



<b>TEIL III</b>	<b>BITCOIN IN DER PRAXIS</b>	<b>85</b>
<b>3</b>	<b>DIE VERWENDUNG VON BITCOIN</b>	<b>85</b>
3.1	VOM SICHEREN UMGANG MIT VERMÖGENSWERTEN	85
3.2	WIE BEKOMMT MAN BITCOINS?	89
3.2.1	<i>Handelsplattformen</i>	90
3.2.2	<i>Geldautomaten (ATM)</i>	94
3.2.3	<i>Face-to-Face Handel</i>	100
3.2.4	<i>Erbe, Geschenk, Spenden und Donations, Airdrops und Bounties</i>	101
3.3	BITCOINS ALS ZAHLUNGSMITTEL	102
3.4	BITCOIN ALS SPEKULATIONSOBJEKT	103
3.5	BITCOIN ALS GESCHÄFTSMODELL	106
3.6	ANDERE ANWENDUNGSMÖGLICHKEITEN DER BLOCKCHAIN-TECHNOLOGIE	107
3.7	BLICK ÜBER DEN TELLERRAND	108
3.7.1	<i>Die Zukunft – Neue blockchain-basierte Finanzinstrumente</i>	108
3.7.1.1	Decentralized Finance (DeFi)	108
3.7.1.2	Non Fungible Token (NFT)	111
3.7.1.3	Ausblick Metaversum	114
3.7.2	<i>Nicht Blockchain, sondern Tangle: IOTA</i>	116
3.8	BITCOIN ALS TÄTERWÄHRUNG	118
<b>TEIL IV</b>	<b>DIGITALE FINANZERMITTLUNGEN</b>	<b>121</b>
<b>4</b>	<b>BITCOIN IM ERMITTLUNGSVERFAHREN</b>	<b>121</b>
4.1	TATHANDLUNGEN IM ZUSAMMENHANG MIT BITCOIN	122
4.1.1	<i>Angriffe gegen das Bitcoin-Protokoll</i>	122
4.1.2	<i>Bitcoin als Tatobjekt</i>	124
4.1.2.1	Betrug und Untreue	124
4.1.2.2	Bitcoin-„Diebstahl“	130
4.1.2.3	Fremdnütziges Bitcoin-Mining	135
4.1.2.4	Einbetten illegalen Materials in die Blockchain	139
4.1.2.5	Erpressung „digital“	142
4.1.2.6	Bitcoin und Geldwäsche	148
4.1.2.7	Finanzierung von Terrorismus und Extremismus	149
4.2	BEGINN DER ERMITTLUNGEN	151
4.3	ERMITTLUNGUNTERSTÜTZUNG	152
4.3.1	<i>Wie es NICHT funktioniert</i>	153
4.3.2	<i>Antrag Digitale Finanzermittlungen</i>	155
4.4	ERMITTLUNGSZIEL	157
4.4.1	<i>Ziel „Identifizierung von Transaktionsbeteiligten“</i>	158
4.4.2	<i>Ziel „Auswertung sichergestellter Wallets“</i>	163
4.4.3	<i>Das „unechte“ Ermittlungsziel</i>	164
4.5	ERMITTLUNGSKONZEPT	164
4.5.1	<i>Mit oder ohne Profi-Werkzeug?</i>	165
4.5.2	<i>OSINT, MS Office, Test-Lizenzen</i>	165
4.5.3	<i>Professionelle Analyse-Tools</i>	169
4.5.3.1	Chainalysis Reactor	170
4.5.3.2	CipherTrace Inspector	172
4.5.3.3	Coinbase Tracer	173
4.5.3.4	TRM Forensics	174
4.5.4	<i>Alternative Analyse-Tools</i>	176
4.5.5	<i>Klassische kriminalistische Ermittlungen</i>	178
4.6	JUSTIZIELLE RECHTSHILFE UND DIGITALE FINANZERMITTLUNGEN IM AUSLAND	179
4.7	FORMULIERUNG EINES AUSKUNFTSERSUCHENS	181
4.8	ABSCHÖPFUNG VIRTUELLER WÄHRUNGEN	184
4.8.1	<i>Finden von Bitcoins beim Tatverdächtigen</i>	185



4.8.2	Die Behörden-Wallet im Detail.....	186
4.8.2.1	Grundsätzliche Anforderungen an eine Behörden-Wallet .....	187
4.8.2.2	Weniger geeignete Wallet-Typen .....	188
4.8.2.3	Der künftige Standard in NRW: ZITIS-Wallet .....	189
4.8.2.4	Alternativen.....	191
4.8.3	Vorläufige Sicherung virtueller Währungen .....	194
4.8.3.1	Konto, Account, Wallet oder Adresse? .....	196
4.8.3.2	Pfändung durch Beschlagnahme .....	197
4.8.3.3	Pfändung durch Vermögensarrest.....	199
4.8.3.4	Vorläufige Sicherung im Ausland.....	201
4.8.3.5	Transfer vorläufig gesicherter Bitcoins .....	202
4.8.3.6	Verwaltung und Notveräußerung.....	203
4.8.3.7	Mitteilung an Verletzte.....	204
4.8.3.8	Rückgabe nicht eingezogener Bitcoins .....	204
4.8.4	Verwertung eingezogener Bitcoins.....	205
4.9	DOKUMENTATION .....	207
<b>TEIL V</b>	<b>ANHANG.....</b>	<b>211</b>
<b>5</b>	<b>INFORMATIONEN, ANLEITUNGEN UND HILFEN.....</b>	<b>211</b>
5.1	DER ARBEITSPLATZ DES DIGITALEN FINANZERMITTLERS.....	211
5.1.1	Ausstattung Hardware .....	211
5.1.2	Ausstattung Software.....	212
5.1.3	Datenaufbereitung und Auswertung mit MS-Excel.....	213
5.1.4	Arbeitserleichternde Tastenkombinationen .....	221
5.2	VORLAGEN .....	222
5.2.1	Muster „Antrag Digitale Finanzermittlungen“ .....	222
5.2.2	Muster „Bestandsdatenanfrage“ .....	224
5.2.3	Muster „Info-Blatt - Auffinden von Wallets“.....	225
5.2.4	Muster „Beschlüsse und Anordnungen bei Beschlagnahme“ .....	226
5.2.4.1	Muster „Beschlagnahmebeschluss, Beschlagnahmeanordnung bei Gefahr im Verzug“.....	226
5.2.4.2	Muster „Pfändungsbeschluss bei Beschlagnahme ggü. Schuldner.....	227
5.2.4.3	Muster „Pfändungsbeschluss bei Beschlagnahme gegenüber Dienstleister“ .....	228
5.2.5	Muster „Beschlüsse und Anordnungen bei Vermögensarrest“ .....	230
5.2.5.1	Muster „Arrestbeschluss, Arrestanordnung bei Gefahr im Verzug“.....	230
5.2.5.2	Muster „Pfändungsbeschluss bei Vermögensarrest ggü. Schuldner“.....	232
5.2.5.3	Muster „Pfändungsbeschluss bei Vermögensarrest gegenüber Dienstleister“ .....	233
5.2.5.4	Muster „Freezing Order“ .....	235
5.2.6	Muster „Bericht Digitale Finanzermittlungen“.....	236
5.2.6.1	Muster „Ziel Täteridentifizierung“ .....	236
5.2.6.2	Muster „Ziel Wallet-Analyse“ .....	242
5.2.6.3	Muster „Technische Umsetzung der vorläufigen Sicherung virtueller Währungen“.....	247
5.2.6.4	Muster „Glossar als Beiblatt zum Bericht“ .....	250
5.3	MULTISIGNATUR-WALLET SCHRITT FÜR SCHRITT MIT ELECTRUM .....	252
5.3.1	Eingesetzte Hardware und Software.....	252
5.3.2	Download und Verifikation.....	253
5.3.3	Installation der Multisignatur-Wallet.....	256
5.3.4	Überprüfung und Konfiguration .....	262
5.3.5	Gemeinsames Signieren einer Transaktion .....	266
5.4	INFOS, QUELLEN UND RECHTLICHES .....	271
5.4.1	Informationen im Internet.....	274
5.4.2	Abbildungsverzeichnis .....	276
5.4.3	Stichwortverzeichnis.....	280
5.4.4	Glossar.....	282
5.4.5	Literaturverzeichnis .....	298