



Hochschule Neubrandenburg
University of Applied Sciences

Master-Thesis

Die Digitalisierung des Geldes Vorteile, Nachteile, Prognosen und Auswirkungen auf die Gesellschaft

Studiengang Digitalisierung und Sozialstrukturwandel

vorgelegt von
Schmidt, Alexander

urn:nbn:de:gbv:519-thesis2021-0654-7

Datum der Abgabe: 24.02.2022

- | | |
|-------------|---------------------------------|
| 1. Betreuer | Prof. Dr. Andreas Wehrenpfennig |
| 2. Betreuer | Prof. Dr. Ing. Sven Brämer |



Abstrakt

Die Abnahme des Bargelds und die Zunahme der bargeldlosen Zahlungen sind allgegenwärtig. Ziel dieser Masterarbeit war es, zu bestimmen, welche Vor- und Nachteile eine Abschaffung oder Beschränkung des Bargelds hätten und wie sich diese auf die Gesellschaft auswirken bzw. bereits ausgewirkt haben. Dazu wurden verschiedene in der Öffentlichkeit verbreitete Thesen der Abschaffungsbefürworter untersucht. Außerdem wurden die Verlagerung der Kriminalität in den digitalen Raum und ihre Existenz in der digitalen Welt sowie im Finanzsektor analysiert.

Bargeld ist weder unhygienisch noch ist es kausal für kriminelle Delikte. Eine Abschaffung des Bargelds hätte keine vermindernenden Auswirkungen auf die Kriminalität. Diese hat sich aufgrund ihrer Flexibilität bereits partiell oder ganz im Zuge der zunehmenden Digitalisierung in das Internet verlagert. Zudem ist die Kriminalität ebenso im Finanzwesen in Verbindung mit unbaren Zahlungsmitteln in erheblichem Maße vorhanden. Weiterhin ist Bargeld, verglichen mit dem hohen Aufwand für den Schutz der digitalen Sicherheit unbarer Zahlungsoptionen, nicht kostenintensiver. Eine Abschaffung hätte ebenso keine gesteigerte Inklusion für benachteiligte oder arme Menschen zur Folge. Dafür behindert es die Konjunkturpolitik der Europäischen Zentralbank. Die Abschaffung des Bargelds wird zu Zwecken der unumschränkten Überwachung und dem begehrten allumfassenden Zugriff auf Spareinlagen und digitalisierten personenbezogenen Daten durch Regierungen, Finanzsektor und Tech-Unternehmen forciert. Daher unterliegt die Abnahme des Bargeldes stark exogener Maßnahmen und beruht nur marginal auf der Entscheidung für eine Zahlungsoption durch die Nutzenden. Bargeld stellt eine der letzten Barrieren zwischen vollumfänglicher Überwachung oder vollunempfindlichen Zugriff auf das monetäre Vermögen und den Bargeld Nutzenden dar. Bargeld ist Freiheit.

Abstract

The decline of cash and the increase in cashless payments are omnipresent. The aim of this master's thesis was to determine the advantages and disadvantages of abolishing or restricting cash and how these would affect society or have already done so. To this end, various theses put forward by abolitionists and disseminated in the public domain were examined. In addition, the shift of crime into the digital space and its existence in the digital world and in the financial sector were analyzed.

Cash is neither unhygienic nor is it causal for criminal offenses. Abolishing cash would have no diminishing effect on crime. Due to its flexibility, crime has already shifted partially or completely to the Internet as a result of increasing digitization. Moreover, crime also exists to a considerable extent in the financial sector in connection with non-cash means of payment. Furthermore, cash is not more cost-intensive compared with the high cost of protecting the digital security of non-cash payment options. Its abolition would also not result in increased inclusion for disadvantaged or poor people. Instead, it would hinder the economic policy of the European Central Bank. The abolition of cash is being pushed by governments, the financial sector and tech companies for the purposes of unlimited surveillance and coveted all-encompassing access to savings deposits and digitized personal data. Therefore, the decline of cash is strongly subject to exogenous measures and only marginally based on the decision for a payment option by the users. Cash represents one of the last barriers between full surveillance or full unresponsive access to monetary assets and cash users. Cash is freedom.

Inhaltsverzeichnis

Abbildungsverzeichnis	IV
Tabellenverzeichnis	VI
Abkürzungsverzeichnis.....	VII
1 Einleitung, Zielsetzung und Aufbau	1
1.1 Einleitung	1
1.2 Zielsetzung	2
1.3 Methodik und Ansatz, Aufbau der Thesis.....	2
Teil 1 - Die Abschaffung / Beschränkung von Bargeld.....	4
2 Geld und Bargeld.....	4
2.1 Definition Geld und geschichtliche Entwicklung	4
2.2 Geld aus soziologischer Sicht	5
2.3 Geld aus psychologischer Sicht.....	7
2.4 Die Veränderung des Zahlungsverhaltens in Deutschland von 2008 bis 2021	9
2.4.1 Das Zahlungsverhalten in Deutschland von 2008 bis 2017.....	9
2.4.2 Das Zahlungsverhalten in Deutschland 2020-2021	11
2.4.3 Die Bargeldentwicklung in Berlin, Brandenburg und	
Mecklenburg-Vorpommern von 2012 bis 2021.....	13
2.5 Bargeldumlauf im Euro-System und Deutschland.....	15
3 Pro und Contra Argumente einer Bargeldabschaffung /.....	
Bargeldbeschränkung	16
4 Schritte zur Bargeldbeschränkung -abschaffung in.....	
chronologischer Reihenfolge.....	17
4.1 Abschaffung der 500 € Banknote.....	17
4.2 Absenkung der Meldepflicht für Bargeschäfte	17
4.3 Flächendeckende Barzahlungsobergrenze in Europa.....	18
4.4 Die Einführung der Central Bank Digital Currency (CBDC)	19

5	Untersuchung ausgewählter Thesen der Bargeldabschaffung	20
5.1	Bargeld ist unhygienisch	20
5.2	Bargeld behindert die Geldpolitik der Europäischen Zentralbank	23
5.3	Bargeld ist zeitaufwändig und kostenintensiv	26
5.4	Der Großteil des Bargelds ist für kriminelle Zwecke im Umlauf	29
5.4.1	Schattenwirtschaft	30
5.4.2	Raubüberfälle	35
5.4.3	Geldwäsche	38
5.4.4	Korruption	41
5.4.5	Terrorismusfinanzierung, Drogenhandel und Menschen Schmuggel	46
5.4.6	Conclusio Kriminalität	47
	Teil 2 - Cybercrime und andere Formen unbarer Kriminalität	49
6	Cybercrime, Kryptowährungen und andere Begrifflichkeiten	49
6.1	Cybercrime	49
6.2	Kryptowährungen und digitales (elektronisches) Geld	49
6.2.1	Allgemeines	49
6.2.2	Distributed-Ledger-Technologies und Blockchain	50
6.2.3	Vor- und Nachteile von Kryptowährungen	52
6.3	Die Entwicklung der Cyberkriminalität	52
6.3.1	Ransomware und Hacking	55
6.3.2	Waffen-, Drogen-, Dokumenten- und Datenhandel, Gewalt- und Mordaufträge im Deep Web und Darknet	57
6.3.3	Kriminalität gerichtet auf Kryptowährungen - Hacken und Exit-Scam von Kryptobörsen, Raubüberfälle	61
6.4	Die Verwendung von Internet und Kryptowährungen durch den internationalen Terrorismus und Extremismus	64
6.5	Digitale Geldwäsche	67
6.6	Conclusio Cybercrime	70

7	Andere Formen unbarer Kriminalität - Kriminalität im Finanzwesen	74
7.1	Steuervermeidung, Steuerhinterziehung und Geldwäsche	74
7.1.1	Begrifflichkeiten	74
7.1.2	Offshore-Leaks und FinCen Files	75
7.2	Steuererschleichung, Steuerbetrug und Lobbyismus	80
7.2.1	Wirecard	80
7.2.2	Cum-Ex	82
7.3	Conclusio	84
8	Exempel der Bargeldabschaffung und der gläserne Mensch	85
8.1	Die Better-Than-Cash-Alliance, „The war on cash“ und die	
	„Finanzielle Inklusion“	85
8.2	Bargeldloses Schweden	88
8.3	Der gläserne Mensch	90
8.4	Conclusio	93
9	Fazit	95
	Appendix	100
	Literatur- / Quellenverzeichnis	136

Abbildungsverzeichnis

Abb. 1	Die kleinste und daher eigentlich nicht weiter zerlegbare Einheit eines sozialen Systems, die Kommunikation.....	6
Abb. 2	Gedankliche Verknüpfungen zum Begriff Geld.....	7
Abb. 3	Häufigkeit der Nennung verschiedener Bedeutungen des Begriffs Geld	8
Abb. 4	Ergebnisse der Umfrage unter „Superreichen“	8
Abb. 5	Bekanntheit und Nutzung mobiler Bezahlverfahren	10
Abb. 6	Corona verändert das Zahlungsverhalten in Deutschland	11
Abb. 7	Änderung des Zahlungsverhalten in der Corona-Krise	12
Abb. 8	Verwendung von Zahlungsinstrumenten insgesamt.....	12
Abb. 9	Kontaktloses Bezahlen mit der Karte	13
Abb. 10	Bargeldumlauf im Eurosystem	15
Abb. 11	Gründe für die Einführung eines digitalen Euro.....	19
Abb. 12	Ausgestaltungsmöglichkeiten des CBDC.....	19
Abb. 13	What is the Dirtiest: Cash, Cards or Coins.....	21
Abb. 14	How dirty are payment methods compared to known filthy things?.....	21
Abb. 15	Marktteilnehmer und anfallende Kostenkomponenten im Bargeldkreislauf in Deutschland.....	26
Abb. 16	Beispielhafter Bargeld-Handling Prozess im Handel	27
Abb. 17	Schattenwirtschaft in Prozent des offiziellen BIP	31
Abb. 18	Jahresergebnisse Schwarzarbeit (gekürzt).....	32
Abb. 19	So viel bleibt von einem Euro	33
Abb. 20	Elektronischer Zahlungsverkehr und Kartenbetrug.....	34
Abb. 21	Raubüberfälle auf Spezialgeldtransportfahrzeuge	35
Abb. 22	Überfälle auf Geldboten	35
Abb. 23	Raubüberfälle 2019	36
Abb. 24	Zahl der festgestellten Angriffe auf Geldautomaten	36
Abb. 25	Percentage who paid for their most recent purchase in cash.....	37
Abb. 26	Entwicklung der Überfälle auf Banken, Geldtransporte und Taxen in Schweden.....	37
Abb. 27	Entwicklung der Überfälle auf Geschäfte in Schweden	37
Abb. 28	Schweden Weniger Bargeld mehr Geldwäsche?.....	40
Abb. 29	Betrugsrisiko Bar- und Kartenzahlungen	40
Abb. 30	Bestechung und Korruption.....	41
Abb. 31	Anzahl der Korruptionsstraftaten 2019 - Fallentwicklung	42
Abb. 32	Gesamtwert der Vorteile (in Mio. Euro)	42
Abb. 33	Art der Vorteile auf Nehmerseite	43

Abb. 34	Gesamtwert der Vorteile auf Geberseite	43
Abb. 35	Zielbereiche der Korruption	43
Abb. 36	Gesamtschaden (in Mio. Euro).....	44
Abb. 37	Bargeld und Korruption.....	45
Abb. 38	Kosten von Terroranschlägen.....	47
Abb. 39	Comparison of anonymous Cryptos	51
Abb. 40	Fallaufkommen von Straftaten der CCieS 2019 und 2020.....	53
Abb. 41	3 von 4 Unternehmen sind Opfer geworden.....	53
Abb. 42	Relation zwischen erfassten und aufgeklärten Cybercrime-Fällen Deutschland von 2016 bis 2020.....	54
Abb. 43	The average cost of cybercrime.....	54
Abb. 44	Total cryptocurrency value received by ransomware addresses per year - 2016 – 2020	55
Abb. 45	Kosten für Lösegeld aufgeschlüsselt nach Ländern inkl. Privatanwender	56
Abb. 46	Gesamtkosten + Lösegeld.....	56
Abb. 47	Wie das Tor-Netzwerk funktioniert.....	57
Abb. 48	Number of active darknet markets - 2019 vs. 2020.....	61
Abb. 49	Total Cryptocurrency value received by scam category.....	62
Abb. 50	Annual total cryptocurrency stolen by victim type - Jan 2019 - Dec 2021	63
Abb. 51	Known Physical Bitcoin Attacks 2014-2021.....	63
Abb. 52	Das Hawala-System.....	65
Abb. 53	ISIS schwenkt auf Monero um	66
Abb. 54	Transaktionen mit BTC	67
Abb. 55	BTC-Mixer Service	67
Abb. 56	Differences between a VASP, MSB, Money Transmitter, Digital Asset Customer.....	69
Abb. 57	BTC Volume sent to unhosted Wallets	70
Abb. 58	Abnehmende Barzahlungen und zunehmender elektronischer Zahlungsverkehr in Schweden.....	72
Abb. 59	Schweden: Elektronischer Zahlungsverkehr und Kartenbetrug/Zunehmender Kartenbetrug bei Online-Zahlungen.....	72
Abb. 60	Total cryptocurrency value received by illicit addresses 2017-2021	73
Abb. 61	Die Größe des Leaks – Umfang der Pandora-Papers im Vergleich zu andern Leaks.....	75
Abb. 62	Which US states have the most trusts in the Pandora Papers?	77
Abb. 63	Top 10 banks by reported amount in FinCen Files	78
Abb. 64	How long it takes banks to file a suspicious activity report	78

Tabellenverzeichnis

Tab. 1	Anteil von Zahlungsmitteln nach Umsatz 2008 - 2017	9
Tab. 2	Vergleich der Bevorzugungen von Zahlungsmitteln 2018 und 2020	12
Tab. 3	Prozentuale Entwicklung der Geldzählmengen im Cash-Center Berlin 2012 bis 2021	14
Tab. 4	Prozentuale Entwicklung der Geldzählmengen im Cash-Center Neubrandenburg 2012 bis 2021	14
Tab. 5	Pro und Contra einer Bargeldabschaffung/Bargeldbeschränkung	16
Tab. 6	Darstellung der Überfälle auf Geldboten und Geldtransportfahrzeuge in Berlin 2020/2021	36
Tab. 7	Barzahlungsobergrenzen einzelner Länder der EU	45
Tab. 8	Vor- und Nachteile von Kryptowährungen	52
Tab. 9	Die größten Cyberangriffe 2021	56
Tab. 10	Marktformen im Drogenhandel	59
Tab. 11	Zahlungsformen auf Kryptomärkten	59
Tab. 12	Known Physical Bitcoin Attacks	63
Tab. 13	Schäden durch Steuerumgehung und Steuerhinterziehung in Steueroasen	76
Tab. 14	Schadenhöhe der Cum-Ex-Deals in verschiedenen Ländern	83
Tab. 15	Gesamtzahl der durchgeführten Kontenabrufe des BZSt 2005 - 2021	91

Abkürzungsverzeichnis

Abb.	Abbildung
ACFE	Association of Certified Fraud Examiners
AFI	Allianz für Finanzielle Inklusion
AG	Aktiengesellschaft
AMLD	Anti-Money Laundering Directive (Geldwäscherichtlinie)
App.	Appendix
AO	Abgabenordnung
Art.	Artikel
B2B	Business to Business
B2C	Business to Consumer/Customer
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDB	Bankernas Depå AB
BDGW	Bundesvereinigung Deutscher Geld- und Wertdienste
BDLS	Bundesverband der Luftsicherheitsunternehmen
BDSW	BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT e. V.
BIC	Bank Identifier Code
BIP	Bruttoinlandsprodukt
BIZ	Bank für Internationalen Zahlungsausgleich
BJA	Bundeskriminalamt
BMF	Bundesministerium für Finanzen
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BSA	Bank-Secrecy Act
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTC	Bitcoin
BTCA	Better Than Cash Alliance
BZ	Berliner Zeitung
BZSt	Bundeszentralamt für Steuern
BoE	Bank of England
bspw.	beispielsweise
bzw.	beziehungsweise
C2C	Consumer to consumer
CBCD	Central Bank Digital Currency
CCaaS	Cybercrime as a Service
CDU	Christlich Demokratische Union Deutschlands
CEPS	Centre for European Policy Studies
CO ₂	Kohlendioxid
CPI	Corruption Perceptions Index (Korruptionswahrnehmungsindex)
CRS	Common Reporting Standard
CSO	Central Statistics Office (Statistisches Amt in Indien)
Cum-Cum	Cum cum dividend
Cum-Ex	Cum ex dividend
CVC	Convertible Virtual Currency
DB	Deutsche Bank
DIA	Direzione Investigativa Antimafia
DLT	Distributed-Ledger-Technologien
DoS	Denial of Service
ECOLEF	Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy
e.g.	exempli gratia
i.e.S.	im engeren Sinne
i.w.S.	im weiteren Sinne
EIU	Economist Intelligence Unit
EU	Europäische Union

Europol	Europäisches Polizeiamt
e.V.	eingetragener Verein
EY	Ernst & Young Wirtschaftsprüfungsgesellschaft
EZB	Europäische Zentralbank
FA	Finanzamt
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force on Money Laundering
FBI	Federal Bureau of Investigation
FDP	Freie Demokratische Partei
FinCen	Financial Crimes Enforcement Network (FIU der USA)
FIU	Financial Intelligence Unit (Finanzbehördliche Eingreiftruppe für Geldwäsche)
FSI	Financial Secrecy Index
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GPFI	Globale Partnerschaft für finanzielle Inklusion
GwG	Geldwäschegesetz
HSBC	britische Großbank mit Sitz in London
IBC	International Business Company
ICIJ	International Consortium of Investigative Journalists
ICT	International Institute for Counter Terrorism
IBAN	International Bank Account Number
i.d.R.	in der Regel
i.H.v.	in Höhe von
IKT	Informations- und Kommunikationstechnologien
IP	Internet Protocol
ISIS	Islamischer Staat
ITMC	Ibn Taymiyya Media Center
IWF	Internationaler Währungsfond
KStG	Körperschaftssteuergesetz
Kfz	Kraftfahrzeug
KG	Kommanditgesellschaft
KPMG	Zusammenschluss mehrerer Wirtschaftsprüfungsgesellschaften
KWG	Kreditwesengesetz
KYC	Know Your Customer
Lt.	Laut
m.H.	mit Hilfe
m.H.v.	mit Hilfe von
Mio.	Millionen
Mrd.	Milliarden
MSC	Medienorganisation des Mujahideen Shura Council
NPPS	New payment products and services
NPRM	Notice of proposed rulemaking
Nr.	Nummer
NSA	National Security Agency
NZZ	Neue Zürcher Zeitung
OCCRP	Organized Crime & Corruption Reporting Project
o.D.	ohne Datum
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OK	Organisierte Kriminalität
P2P	Peer to Peer
PayTM	indisches Zahlungsdienstleistungs- und Finanztechnologieunternehmen
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
POS	Point of sale (Ort des Einkaufs)
PSP	Payment Service Provider

PwC	PricewaterhouseCoopers (Wirtschaftsprüfungsgesellschaft)
SdK	Schutzgemeinschaft der Kapitalanleger
SEB	Skandinaviska Enskilda Banken AB
SEK	Schwedische Krone
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
TOR	The Onion Router
u.a.	unter anderem
UIGEA	Unlawful Internet Gambling Enforcement Act
UID	Unique Identifier
UK	United Kingdom
UNODC	United Nations Office on Drugs and Crime (Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung)
US	United States
USA	United States of America
USAID	United States Agency for International Development
VASP	Virtual Asset Service Provider
VZVB	Verbraucherzentrale Bundesverband
WES	World Economic Survey
WTU	Werttransportunternehmen
z.B.	zum Beispiel

1 Einleitung, Zielsetzung und Aufbau

1.1 Einleitung

„Geld bedeutet [...] geprägte Freiheit und hat darum für einen jeder Freiheit beraubten Menschen den zehnfachen Wert. Wenn nur einige Münzen in seiner Tasche klimpern, so ist er schon halb getröstet, selbst wenn er keine Möglichkeit hat, das Geld auszugeben. Geld kann man aber immer und überall ausgeben, um so mehr, als die verbotene Frucht doppelt so süß ist.“

so schreib einst Dostojewski in einem seiner Bücher (Dostojewski 1861/1862:40 f.).

Beschrieb Dostojewski damit bereits 1861/1862 „[...] den individuellen Wert des Bargeldes“ (Hickel 2016:84) als Ausdruck der Freiheit wie Hickel es behauptet oder wird dieses Zitat aus dem „[...] Zusammenhang gerissen“ (Rogoff 2016:88), damit Gegner der Bargeldbeschränkung bzw. Bargeldabschaffung ihren Standpunkt untermauern können wie Kenneth S. Rogoff, amerikanischer Ökonom an der Harvard Universität und bekennender Befürworter einer Bargeldabschaffung in seinem Buch „Der Fluch des Geldes“ entgegnet?

Mit der Befürwortung einer Bargeldabschaffung oder der Umsetzung einer Barzahlungsobergrenze steht Rogoff nicht allein. Weitere Vertreter sind u.a. Peter Bofinger, Professor für Volkswirtschaftslehre an der Universität Würzburg, Willem Hendrik Buiters, amerikanisch-britischer Ökonom, welcher seinerzeit an verschiedenen Akademien lehrte oder Lawrence Henry Summers, amerikanischer Professor für Ökonomie und Politiker in mehreren Ämtern sowie ehemaliger Chefwirtschaftswissenschaftler der Weltbank. Aber nicht nur einzelne Wissenschaftler vertreten diese Meinung. Es haben sich ganze Allianzen gegen das Bargeld gebildet. Die bekannteste ist die sogenannte „Better Than Cash Alliance“, welche mittlerweile 78 Mitglieder zählt. Mitglieder sind Handelsunternehmen wie die Coca-Cola Company und H & M, Banken wie die European Bank for Reconstruction and Development, Zahlungsdienstleister wie MasterCard und VISA, Regierungen aus Afrika - Asien und Lateinamerika, wohltätige Organisationen wie die Bill & Melinda Gates Foundation sowie deutsche Ministerien wie das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung. Ihre eindeutige Botschaft auf der Webseite lautet: „Wir wollen physisches Bargeld nicht abschaffen, sondern dafür sorgen, dass die Menschen die Wahl haben, wie sie Zahlungen leisten und empfangen. Es ist wichtig, dass die Menschen über digitale Zahlungsmöglichkeiten verfügen, die verantwortungsbewusst und 'besser als Bargeld' sind [...]“ sowie „[...] Um es klar zu sagen, wir möchten verhindern, dass Menschen Bargeld verwenden, da dies manchmal die beste oder einzige Zahlungsoption ist. Regierungen, Unternehmen und Menschen suchen nach einem besseren Wertangebot als Bargeld, um Effizienz, Transparenz, Sicherheit, wirtschaftliche Teilhabe von Frauen, finanzielle Eingliederung und integratives Wachstum zu verbessern.“ (Better Than Cash Alliance - Members o.D.).

Die Argumente der Bargeldabschaffungsbefürworter gegen die Verwendung des Bargelds sind vielfältig. Bargeld ist dreckig, unhygienisch und korreliert aufgrund der Anonymität mit der Kriminalität. Es verleitet zur Steuerhinterziehung, es wird für die Terrorismusfinanzierung sowie für Geldwäsche, Drogenhandel und Menschenschmuggel verwendet. Es fördert weiterhin die Schwarzarbeit und Korruption. Partiiell soll Bargeld sogar kausal für kriminelle Handlungen sein. Weiterhin verursacht Bargeld hohe Kosten durch seine Produktion, Vorhaltung und Versorgung im Geldkreislauf. Eines der wichtigsten Argumente ist jedoch, Bargeld behindere die Geldpolitik der Zentralbanken und das nicht nur innerhalb der Eurozone, sondern weltweit. Der Finanzkrise im Jahr 2008 sollte durch die Geldpolitik mit Hilfe von Zinssenkungen begegnet werden, wie bereits zuvor in anderen Wirtschaftsrezessionen, um so die Weltwirtschaft wieder ankurbeln zu können. Hier erkannten die Zentralbanken jedoch schnell, dass die Zinssenkungen nur begrenzt erfolgen können. Die Grenze des Senkens lag hier bei einem Zinssatz von Null, geschweige denn, dass er in den Negativbereich hätte gesenkt werden können. Zudem war ein Negativzins zu diesem Zeitpunkt undenkbar. Das Senken des Zinssatzes in den negativen Bereich wird durch den Fakt verhindert, dass Geschäftsbanken, Unternehmen und Privatpersonen durch das Vorhalten

von Bargeld außerhalb des Finanzsystems eine Möglichkeit des Ausweichens vor Negativzinssätzen gegeben ist. Ein Negativzins läuft, zumindest auf den gehorteten Betrag bezogen, ins Leere. Der gehortete Betrag hat einen Zinssatz von Null, da er nicht angelegt ist. Es macht aus Sicht der Anleger wenig Sinn, diesen innerhalb des Finanzsystems zu einem negativen Zinssatz anzulegen. Um diesem Denken vorzubeugen, kamen mehrere Wissenschaftler auf die Idee einer Bargeldabschaffung. Denn würde das Bargeld abgeschafft, bestünde keine Möglichkeit des Ausweichens mehr, es gäbe keine Nullzinsgrenze und zusätzlich die Möglichkeit, den Nominalzinssatz ohne Gegenwehr in den negativen Bereich zu senken. Bis zum Jahr 2015 wurde dieser Vorschlag als „[...] Kuriosum aus dem Elfenbeinturm“ (Gersbach/Bundesministerium für Wirtschaft und Energie (BMWi) 2017:3) betrachtet. Es war Andrew Haldane, Chefökonom der Bank of England (BoE), welcher erstmals im Jahr 2015 den Vorschlag innerhalb einer politischen Debatte mit ernster Absicht unterbreitete, dass eine Bargeldabschaffung von Vorteil wäre, um das Potenzial der Geldpolitik der Zentralbanken erhöhen zu können. Auch die bereits genannten Argumente wurden bei der Debatte abermals verwendet. Gersbach geht davon aus, dass diese Argumente sogar mehr ins Gewicht fielen als die Behinderung der Geldpolitik selbst. Erste Schritte zur Bargeldabschaffung wurden bereits eingeleitet und umgesetzt. Einige Länder führten bspw. Obergrenzen für Barzahlungen ein. Die Produktionseinstellung hoher Denominationen wie die 500€ Banknote war ein weiterer Schritt zur Bargeldbegrenzung (Gersbach/ BMWi 2017:3). Aber nicht nur die Produktion der 500€ Note wurde eingestellt. In Venezuela kam es zu Entwertungen der 100 Bolívar Note und in Indien der 500 und 1.000 Rupien Noten (König 2017:342). Weitere Schritte sind bereits in Planung. So soll die Barzahlungsobergrenze auf Vorschlag des Bundesministeriums für Finanzen auf 2.000€ gesenkt werden. Ein wesentlich höheres Ziel hat sich hingegen die Europäische Zentralbank (EZB) mit der Einführung des digitalen Euros (Central Bank Digital Currency - CBDC) gesetzt, denn dieser soll wie der bisherige physische Euro, in Note oder Münze sein, nur eben in digitaler Form. Dabei betont die EZB, dass damit nicht das Bargeld ersetzt werden sondern als parallele Zahlungsform neben dem Bargeld existieren soll (EZB 2021).

1.2 Zielsetzung

Im ersten Teil ist es Ziel der Arbeit, Thesen der Befürworter einer Bargeldabschaffung bzw. Barzahlungsbeschränkung durch Betrachtung von Studien wissenschaftlich zu eruiieren. Die im öffentlichen Raum kursierenden zu untersuchenden Thesen der Bargeldgegner lauten dabei:

„Bargeld ist unhygienisch“

„Bargeld behindert die Geldpolitik der Europäischen Zentralbank“

„Bargeld ist zeitaufwändig und kostenintensiv“

„Der Großteil des Bargelds ist für kriminelle Zwecke im Umlauf“.

Weiterhin wird untersucht, wie sich eine Beschränkung oder Abschaffung des Bargelds auf die gesellschaftliche Ordnung und die Menschen auswirken könnte bzw. ob bereits Auswirkungen aufgrund von Beschränkungen ersichtlich sind. Gleichzeitig wird eine Analyse des derzeitigen Zahlungsverhaltens in Deutschland und dessen Entwicklung in den vorangegangenen Dekaden vorgenommen und eine Prognose hinsichtlich eines zukünftigen Trends der präferierten Zahlungsmethoden in der Gesellschaft getroffen. Geprüft wird weiterhin, wie sich der Bargeldumlauf in Europa entwickelt hat und ob dieser mit dem Zahlungsverhalten korreliert. Der zweite Teil dieser Master-Thesis untersucht die These, dass sich die Kriminalität aufgrund der fortschreitenden Digitalisierung in die digitale Welt verlagert.

1.3 Methodik und Ansatz, Aufbau der Thesis

Gewählt wurde der utilitaristische Ansatz. Nach der Einleitung wird im zweiten Kapitel die Entstehung und die Bedeutung des Geldes aus soziologischer sowie psychologischer Sicht eruiert. Weiterhin werden das Zahlungsverhalten der deutschen Bevölkerung und die Bargeldmengenentwicklung in der Europäischen Union betrachtet. Kapitel drei befasst sich mit den Argumenten und Gegenargumenten einer Bargeldbeschränkung bzw. einer vollständigen Bargeldabschaffung. Nachfolgend wird im Kapitel vier dargestellt, welche Maßnahmen zur Bargeldbeschränkung bereits umgesetzt wurden und welche künftig unternommen werden sollen. Kapitel fünf eruiert Thesen der Befürworter von Bargeldbeschränkungen bzw. einer Bargeldabschaffung. Unter anderem

wird die These untersucht, dass Bargeld Kriminalität begünstigt oder es sogar kausal dafür ist. Darauf aufbauend beschäftigt sich Kapitel sechs mit der Entwicklung der Cyberkriminalität in Bezug auf die verwendeten bargeldlosen Zahlungsoptionen. Darüber hinaus wird die These einer Verlagerung der Kriminalität in den digitalen Raum infolge einer Bargeldabnahme eruiert. Kapitel sieben untersucht die Kriminalität im Finanzwesen in Kooperation mit der Politik. In Kapitel acht werden die Auswirkungen von Bargeldbeschränkungen bzw. Bargeldabschaffung sowie deren Ursachen anhand von Exempeln untersucht. Weiterhin werden die Bestrebungen einer totalen Überwachung der Menschen eruiert. Die Zusammenfassung der Thesis erfolgt im Kapitel neun.

Teil 1 - Die Abschaffung / Beschränkung von Bargeld

2 Geld und Bargeld

2.1 Definition Geld und geschichtliche Entwicklung

Der Begriff des Gelds entstammt dem althochdeutschen „gelt“ (Häußling 2018:121) und bedeutet in seiner Übersetzung Zahlung oder Zahlungsmittel. Nach Häußling übernimmt Geld die Aufgaben:

- (1) als Tauschmittel, welches von den Marktteilnehmern allgemein anerkannt wird,
- (2) als wirtschaftlicher Maßstab für den Wert von Handelsgütern und Dienstleistungen (= Preis) und
- (3) als Wertaufbewahrungsmittel.

Gesellschaftlich und kulturell ist Geld als Substanz in mehreren Schritten durch Funktionen ersetzt worden. In seiner ursprünglichen Form als Tauschmittel war es nicht nur ein Symbol eines Wertes, sondern der Wert selbst. Ausprägungen waren das Naturgeld wie das Vieh, Schmuckgeld wie Ring- bzw. Steingeld und Nutzgeld wie Nahrung oder Bekleidung. In einer weiteren Stufe symbolisierte das Geld, aufgrund der Verwendung von Edelmetallen, als Metallgeld einen „substantziellen Warenwert“ (Häußling 2018:121). Nach der Einführung des Papiergelds symbolisiert das Geld lediglich einen Wert, welcher zuvor jedoch definiert und reguliert werden musste. Durch das Verlassen der materiellen Wertabdeckungsebene entwickelte sich das Bargeld zu einem immateriellen Giralgeld (auch Kreditgeld bzw. Guthaben). Ausprägungen dafür sind bspw. Schecks, Scheck- und Kreditkarten (Häußling 2018:121).

Geschichtlich lässt sich die Entwicklung des Geldes nach Braunschweig und Pichler (2020:13) in drei Epochen gliedern:

„Stufe 1: Magisch-mythisch bedingte Geldsubstanz

- a) Frühzeit in Form von Muschel-, Ring-, Feder-, Perlengeld
- b) Bauernkulturen im indogermanischen Bereich (Viehgeld, Axtgeld, Metallgeld zum Beispiel in Ringform)

Stufe 2: Stoffwertbedingte Geldsubstanz

- a) Babylonien und Ägypten (Gewichtseinheiten Silber, Schekelwährung)
- b) Griechenland (gestempelte Goldbarren, Münzen aus Silber und Gold)
- c) Rom (rechtliche Ordnung des Geldwesens, Kupfermünzen, Münzen mit aufgeprägter Wertzahl)
- d) Reiche der Völkerwanderung (Übernahme des römischen Münzsystems)
- e) Franken und Karolinger (Silberwährung, Karlsfund)
- f) Mittelalter (Barrengeld, Hack Silber, Groschen, Gulden, Thaler)
- g) Neuzeit (Münzordnungen, Scheidemünzen, Kipper und Wipper)

Stufe 3: Funktionsbedingte Geldsubstanz

- a) China (Gerätegeld, Zeichengeld*)
- b) Abendland (Papiergeld, Buchgeld, elektronisches Geld, Kryptowährungen auf Basis der sog. Blockchain-Technologie)“ (Braunschweig/Pichler 2021:13)

In seiner Funktion als Wertaufbewahrungsmittel ermöglichte das Geld das Sparen und die Vermögensanhäufung über die Vorratshaltung natürlicher Güter hinaus. Die Rechen- bzw. Wertstabsfunktion ist jedoch bereits früheren Epochen zuzuordnen (Braunschweig/Pichler 2021:13). Ökonomisch gesehen ist Geld alles, was von der Allgemeinheit als Zahlungsmittel Akzeptanz

* Gerätegeld: „vormünzliche (prämonetäre) Zahlungsmittel, die in Form von Äxten, Beilen, Messern, Hacken, Spaten, Angelhaken, Wurf-, Pfeil- oder Lanzenspitzen aus Metall hergestellt wurden“ Reppa (o.D.). <https://www.reppa.de/lexikon/geraetegeld>. abgerufen am 30.11.2021, Zeichengeld: „Scheine, Buchungen“ (Müller 2017:55)

erfährt und dazu geeignet ist, als Wertaufbewahrungsmittel zu fungieren. Durch seine hohe Liquidität kann es jederzeit als Tausch für Güter oder Dienstleistungen Verwendung erfahren. Bis auf wenige Ausnahmen gehen die Zahlungsmittel- und Rechenfunktion zumeist einher. Kösters und Hebler unterscheiden Geld in Buchgeld (Giralgeld) - geschaffen von Banken - und Bargeld, welches von den jeweiligen Zentralbanken oder Regierungen in Form von Münzen und Scheinen herausgegeben wird. Noten und Münzen geben als alleiniges gesetzliches Zahlungsmittel die umlaufende Menge des Geldes wieder. Das Buchgeld hingegen stellt offiziell kein gesetzliches Zahlungsmittel dar, es wird jedoch als ein solches akzeptiert und kann aufgrund seiner ähnlich hohen Liquidität als gesetzliches Zahlungsmittel ausgezahlt werden. Zu dieser Kategorie zählen ebenso Termin- und Spareinlagen und kurzfristige Wertpapiere (Kösters/Hebler 2005:171).

2.2 Geld aus soziologischer Sicht

Aus soziologischer Sicht lässt sich Geld nach den folgenden Punkten beschreiben:

- In seiner Tauschmittelfunktion stellt Geld ein Mittel für die Interaktion und Kommunikation auf sachlicher und individueller Ebene dar und ermöglicht dadurch „zweckrationale Beziehungen“ (Mikl-Horke 2011:190) zwischen den Beteiligten. Im direkten Tausch haben sie einen Horizontalcharakter, d.h. auf gleichgeordneter Ebene. Eine vertikale Ebene hingegen ist bei Kreditvergabe zwischen Kreditgeber und -nehmer gegeben.
- Geld ist gleichzeitig ein Produktionsfaktor. Je nach Möglichkeit kann es durch seine Anhäufung zum weiteren Gelderwerb verwendet werden. Weiterhin ermöglicht es den Ressourcenerwerb wie bspw. die menschliche Arbeitskraft. Damit wird Geld als Kapital auch bestimmend für die Gesellschaftsstruktur und je nach Einkommen bzw. je nach Konsummöglichkeit zum Ausdruck einer gesellschaftlichen Ungleichheit.
- Geld in Form von Währung wirkt als Repräsentanz für Macht und Autorität und ermöglicht dadurch verhaltenssteuernde und -kontrollierende Aspekte. Im Optimum wird dadurch verantwortungsbewusst ein Geld- bzw. Zahlungsfluss gewährleistet und wohlfahrtssteigernd gelenkt. Dazu sind politische Maßnahmen erforderlich, um zu verhindern, dass Distributionskonflikte entstehen. Es bedarf weiterhin institutioneller Einrichtungen zur Regelung von Rechten und Pflichten bei der Vergabe von Krediten und zur Schaffung von Normen im Umgang und Austausch mit Geld (Mikl-Horke 2011:190 f.).

Luhmann sieht Geld als symbolisch generalisiertes Kommunikationsmedium (Pahl 2017:203) innerhalb seiner Systemtheorie. Dabei sind Systeme nicht dinglich zu verstehen sondern als Zusammensetzung von Operationen. Unterschieden werden biologische, psychische und soziale Systeme, welche auf unterschiedliche Weise operieren. Leben ist die Operation eines biologischen Systems, Bewusstseinsprozesse e.g. das Denken und die Wahrnehmung als Operation der psychischen Systeme und Kommunikation als Operation von sozialen Systemen. Operation ist dabei als mit Aktivität gleichzusetzen, denn nur operierende Systeme können existieren. Systeme produzieren und reproduzieren sich somit selbst. Als Grundvoraussetzung für die Existenz von Systemen führt Luhmann die „System/Umwelt/Differenz und die Autopoiesis“ (Berghaus 2011:38) an (Berghaus 2011:38). Der Begriff der Umwelt ist hier als Teil außerhalb eines Systems zu sehen, welches durch das System selbst festgelegt wird. Differenz ist die Abgrenzung der Systeme zu ihrer Umwelt, trotzdem agieren Systeme offen zur Umwelt. Gleichzeitig ermöglicht die Differenz Entwicklung. Durch ungleiche Veränderung von Umwelt und System, ist das System gezwungen sich auszudifferenzieren, d.h. anzupassen (Berghaus 2011:54). Autopoiesis beschreibt den Vorgang der Selbstreproduktion und bedeutet, dass Systeme sich durch Operationen innerhalb des Systems selbst reproduzieren müssen. Ohne diese Operationen ist eine Existenz des Systems ausgeschlossen. Die Umwelt hat dabei einen entscheidenden Einfluss auf das System, auch Störungen oder Zerstörungen können durch sie ausgelöst werden (Berghaus 2011:52). Für soziale Systeme ist die Kommunikation das Element für die Existenz und Autopoiesis und gleichzeitig die Differenz zur Umwelt (Berghaus 2011:73). Für Luhmann ist Kommunikation „eine Synthese aus drei Selektionen [...] Information, Mitteilung und Verstehen“ (Luhmann 1997:190 zitiert nach

Berghaus 2011:74) und bietet eine Entscheidungswahl zwischen unterschiedlichen Möglichkeiten. Luhmann verstand dies als „Kontingenz“ und „doppelte Kontingenz“ (Luhmann 2018:217). Dies bedeutet, dass sowohl Zwang für eine Entscheidung besteht als auch die Wahl für eine Entscheidung verschiedener Optionen (Berghaus 2011:75). Allerdings gilt dies nur für Optionen, welche auch einen Sinn für das System ergeben, welches grundsätzlich durch das System selbst bestimmt wird, d.h. es wird aus verschiedenen Möglichkeiten selektiert (Berghaus 2011:75). Unter dem Begriff der Kommunikation nach Luhmann ist nicht die klassische Kommunikation zu verstehen, denn Luhmann ordnet dieser im Gegensatz zum klassischen Begriff drei verschiedene Prozesse der Selektion zu: „[...] Selektion einer Information, Selektion der Mitteilung dieser Information und selektives Verstehen oder Mißverstehen dieser Mitteilung und ihrer Information.“ (Luhmann 1995b:115 zitiert nach Berghaus 2011:77). Weiterhin ist Kommunikation nicht ausschließlich auf psychische Systeme, e.g. Personen, begrenzt, sondern schließt soziale Systeme ein (Berghaus 2011:76). Dabei unterscheidet Luhmann den Sender als „Alter“ und den Empfangenden als „Ego“ (Luhmann 2018:195). Alter fallen dabei die ersten beiden Selektionsprozesse und Ego der letztere Selektionsprozess zu (Abb. 1) (Berghaus 2011:78).

Abb. 1 Die kleinste und daher eigentlich nicht weiter zerlegbare Einheit eines sozialen Systems, die Kommunikation

	Zwei informationsverarbeitende Prozessoren In der Regel: Personen Auch möglich: soziale Systeme	
	„Alter“ der/die Andere konventionell: Sender	„Ego“ Ich konventionell: Empfänger
Drei Selektionen	1. Selektion der Information 2. Selektion der Mitteilung	3. Selektion der Annahme/ des Verstehens

Quelle: Berghaus 2011:78

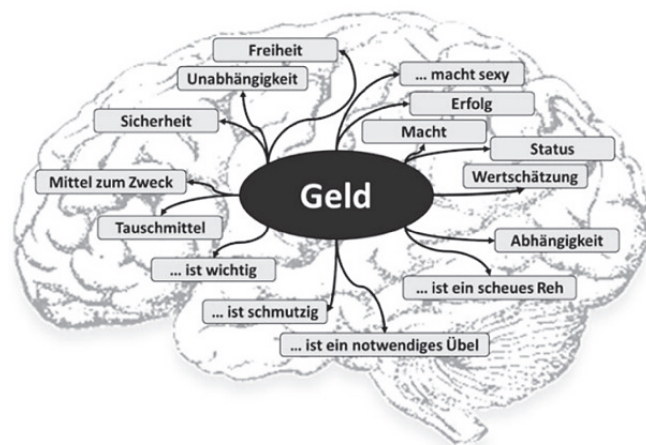
Weiterhin prägt Luhmann den Begriff der Anschlusskommunikation, welcher die Kommunikation erst erfolgreich macht. Kommunikation kann demnach nur erfolgreich sein, wenn sie fortgesetzt wird. Dafür muss nicht zwangsläufig Einigkeit bzw. Konsens bestehen, sondern kann sich auch aufgrund Uneinigkeit bzw. Dissens ergeben (Berghaus 2011:106). Laut Luhmann ist die Kommunikation jedoch „extrem unwahrscheinlich“ (Luhmann 1997:193 zitiert nach Berghaus 2011:108): „Wie soll jemand auf die Idee kommen, einen anderen, dessen Verhalten ja gefährlich sein kann oder auch komisch, nicht nur schlicht wahrzunehmen, sondern es im Hinblick auf die Unterscheidung von Mitteilung und Information zu beobachten? Wie soll der andere erwarten und sich darauf einstellen können, dass er so beobachtet wird? Und wie soll jemand sich ermutigt fühlen, eine Mitteilung (und welche?) zu wagen, wenn gerade das Verstehen des Sinnes der Mitteilung den Verstehenden befähigt, sie abzulehnen? Geht man von dem aus, was für die beteiligten psychischen Systeme wahrscheinlich ist, ist also kaum verständlich zu machen, daß es überhaupt zu Kommunikation kommt.“ (Luhmann 1997:191 zitiert nach Berghaus 2011:108). Kommunikationsmedien vermindern die Unwahrscheinlichkeit der Kommunikation und sind daher „erwartungsleitende Wahrscheinlichkeiten“ (Luhmann 1997:195 zitiert nach Berghaus 2011:111). Medien sind hier als Begrenzung des Spielraums der Auswahlmöglichkeiten zu verstehen und nicht als Beschränkung der Auswahlmöglichkeiten selbst. Innerhalb der eigens gesetzten Grenzen eines Systems regen Kommunikationsmedien die Auswahlmöglichkeiten an. Durch die Begrenzung des Spielraums hingegen wird die Wahrscheinlichkeit einer passgenauen Selektion geschaffen (Berghaus 2011:111). Medien können dabei in verschiedenen Formen auftreten und werden als „Freiheit der vielen Möglichkeiten“ (Berghaus 2011:112) verstanden. Nach Luhmann können Medien „[...] nicht konsumiert werden. Sie regenerieren sich, indem sie Formen schaffen und wieder auflösen.“ (Luhmann 1993b:356 zitiert nach Berghaus 2011:113). Geld als symbolisch generalisiertes Kommunikationsmedium löst die Unwahrscheinlichkeit der 3. Art nach Luhmann, den Prozess der Motivation zur Annahme eines Angebots „um etwas zu kriegen, das man andernfalls nicht bekommen würde“ (Luhmann 2002b:308 zitiert nach Berghaus 2011:118). Geld ermöglicht durch seine binäre Codierung in Zahlung und Nichtzahlung Sachverhalte adressierbar

zu machen, ohne dabei Bezug auf künftige Risiken oder Chancen Bezug nehmen zu müssen. Das System der Wirtschaft hingegen sorgt für die Regulierung einer gegenwärtigen Knappheit, um künftige Bedürfnisse befriedigen zu können. Märkte innerhalb eines Wirtschaftssystems sind keine eigenständigen Systeme, sondern integrieren lediglich mehrere Teilnehmer, e.g. Verbrauchende oder Unternehmen. Um Chancen und Risiken identifizieren zu können, müssen Preise, Preisentwicklungen und Teilnehmer der Märkte beobachtet werden (Pahl 2017:203 f.). Geld als „evolutionäre Errungenschaft“ (Luhmann 2004:33) ermöglichte erst eine Ausdifferenzierung des Wirtschaftssystems sowie eine verbesserte Anpassung an die Umwelt und dient einer langfristigen Absicherung des Fortbestands des Systems (Luhmann 2004:33). Ganßmann versteht unter dem Begriff des Geldes eine Zusammenfassung aller Objekte, welche die Zahlungsmittel-, Tauschmittel-, Wertaufbewahrungs- und Recheneinheitfunktion darstellen können (Ganßmann 2002:26). Ob Objekte als Geld angesehen werden, ist darüber hinaus von Beobachtern abhängig, die dem Objekt diese Funktionstauglichkeit zuschreiben (Ganßmann 2002:24). Maßgebend für die Selektion des Mediums ist laut Luhmann der Begriff des Sinns. Demnach ist ein Medium nicht negierbar, jedoch aber auserwählte Formen des Mediums. Zudem ermöglicht das Medium innerhalb seiner Grenzen die Selektion und Entwurf diverser Formen (Berghaus 2011:121). Welches Medium gewählt wird, bestimmen Systeme nach dem Sinn. Zudem besteht in Systemen „Sinnzwang“ (Luhmann 2018:95). Für alle Medien gilt, so auch für die Medien Sinn oder Geld: „Die Welt ist von nahezu ‚endloser Offenheit‘ (Luhmann 2018:96) für immer wieder neue, andere Sinnformen, die man akzeptieren oder ablehnen kann.“ (Berghof 2011:121).

2.3 Geld aus psychologischer Sicht

In einer Umfrage unter 100 Passanten in verschiedenen deutschen Städten zur Frage, was den Menschen Geld vor allem bedeutet, filterten Sauerland und Höhs die am häufigsten genannten Antworten heraus (Abb. 2). Dabei wurde mit dem Begriff Geld Bedeutungen wie bspw. „Freiheit“, „Unabhängigkeit“, „Sicherheit“, „Mittel zum Zweck“ aber auch „Macht“ assoziiert (Sauerland/Höhs 2019:12).

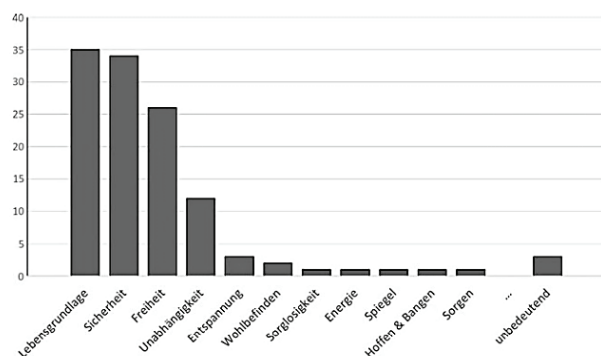
Abb. 2 Gedankliche Verknüpfungen zum Begriff Geld



Quelle: Sauerland/Höhs 2019:12

Eine weitere Studie am selben Forschungsinstitut durch im Jahr 2013 brachte folgende am häufigsten genannten Antworten auf die Vervollständigung der Frage „Geld bedeutet für mich...“ dargestellt in Abb. 3. Demnach wurde Geld vorrangig als Lebensgrundlage gesehen und mit weiteren Begrifflichkeiten wie „Sicherheit“, „Freiheit“ und „Unabhängigkeit“ assoziiert (Sauerland/Höhs 2019:12).

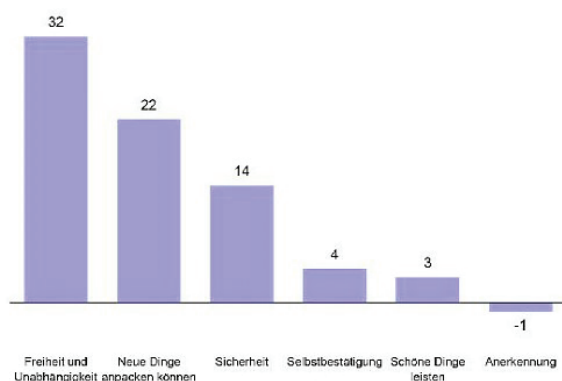
Abb. 3 Häufigkeit der Nennung verschiedener Bedeutungen des Begriffs Geld



Quelle: Sauerland/Höhs 2019:13

Zitelmanns Umfrage unter Hochvermögenden lieferte ähnliche Ergebnisse (Abb. 4). Freiheit und Unabhängigkeit, das Vermögen neue Dinge anzugehen und die Sicherheit rangierten auch hier auf den vordersten Plätzen. Auch hier ergab die Umfrage, dass der Begriff des Geldes nicht damit assoziiert wurde, sich „schöne Dinge zu leisten“ (Zitelmann 2017:326).

Abb. 4 Ergebnisse der Umfrage unter „Superreichen“



Quelle: Zitelmann 2017:326

Sauerland und Höhs kommen daher zu dem Schluss, dass die Probanden der Studien mit dem Begriff Geld keine negativen Schlüsse assoziieren. Vielmehr wird mit Geld Freiheit und Unabhängigkeit verbunden und erklärt damit aus ihrer Sicht das Streben nach mehr Geld. Erkennbar wird auch, dass die Befragten keineswegs materielle Gegenstände wie bspw. bestimmte Produkte mit Geld assoziieren, sondern dass sie vorrangig nach der Ermöglichung ihrer Selbstverwirklichung streben, um so ihre Existenz zu sichern und ihre Leidenschaften zu erfüllen. Im Umkehrschluss bedeutet dies, dass für die Probanden, welche angaben, zu wenig Geld als Mangel zu empfinden, dies einen Ausdruck für eingeschränkte Freiheiten darstellen könnte, wenn sie Geld mit Freiheit assoziieren. Der Anteil, welcher angab, über zu wenig Geld zu verfügen, belief sich bei der Studie auf über 80 % der Befragten. Weiterhin kommt die Studie zur Erkenntnis, dass Probanden, welche bereits über genügend Geld verfügen, wertschätzen, dass der Mangel an Freiheit beseitigt werden konnte (Sauerland/Höhs 2019:13 f.). Ausgehend davon, dass Geld der Repräsentant menschlicher Bedürfnisse ist, ist der Umgang mit Geld kennzeichnend für bewusste oder unbewusste Bedürfnisse. Zum Ausdruck kommen dabei u.a. Ängste, Konflikte oder Probleme mit dem Selbstwertgefühl. Menschen, welche negative Entwicklungen befürchten und mangelndes Vertrauen in andere Personen haben, neigen eher dazu, Geld zu horten, um Krisen oder Katastrophen vorbeugen zu können. Weiterhin ist aufgrund dessen ein ständiges Streben nach mehr Geld zu verzeichnen, da sie das Volumen des eventuell benötigten Geldes nicht einzuschätzen vermögen. Menschen, welche hingegen ihr Geld verschwenden, sehen eventuell im Ausgeben

ihres Geldes den Beweis für ihre Existenz. Daher ist die Hortung von Geld bei ihnen nicht vorzufinden (Sauerland/Höhs 2019:15). Breier stimmt mit Sigmund Freud überein, dass Geld ein Mittel für die Selbsterhaltung und für die Gewinnung von Macht ist. Geld ist essenziell für die Absicherung der eigenen Existenz und notwendig, um Krisen zu überwinden. Weiterhin gewährt es die Möglichkeit einer Reaktion und folglich daraus auch Freiheiten. Zudem gewährt Geld Macht in Bezug auf die Einflussmöglichkeiten auf Geschehnisse und hilft bei der Handhabung von Problemen. Dies wiederum gibt ein Gefühl der Sicherheit. Auch die Motivation von Menschen stellt für Breier eine Form der Macht dar, da auch hier eine Beeinflussung durch Geld möglich ist (Breier 2017:60).

2.4 Die Veränderung des Zahlungsverhaltens in Deutschland von 2008 bis 2021

Die Deutsche Bundesbank führt Studien zum Zahlungsverhalten in Deutschland in Drei-Jahres-Abständen durch. Analysiert werden im Folgenden die Zusammenfassung des Zahlungsverhalten von 2008 bis 2017 in der vierten Studie aus dem Jahr 2017. Anschließend wird die fünfte Studie aus dem Jahr 2020 behandelt.

2.4.1 Das Zahlungsverhalten in Deutschland von 2008 bis 2017

Das Zahlungsverhalten der Deutschen wurde von 2008 bis 2017 vorrangig von Bargeldzahlungen dominiert. 74% aller Transaktionen wurden bar durchgeführt. Im Vergleich zum Jahr 2014 ist hier jedoch bereits ein Rückgang der Barzahlungen von 5% zu verzeichnen. Bezogen auf den Zahlungsbetrag wurden Barzahlungen vorrangig für Beträge zwischen 5 € (zu 96%) und 50 € verwendet. Vorwiegend wird die Barzahlung zwischen privaten Personen, an Automaten und für außer Haus Verpflegung benutzt. Der Anteil der Barzahlungen ist im Jahr 2017 erstmalig auf 48% aller Zahlungen bezogen auf den Gesamtumsatz gesunken, im Jahr 2014 betrug der Anteil noch 53,2% (Tab. 1, und App. 1). Im Wert der Zahlungen beträgt der Rückgang damit 6% aller erfassten getätigten Zahlungen. Somit ist hier ein substituierender Trend der Bargeldzahlungen durch bargeldlose Zahlungen von der ersten Erhebung anno 2011 bis anno 2017 eindeutig erkennbar (Tab. 1 und App. 1). Im Gegensatz dazu ist eine Zunahme von ca. 6% der Verwendung von Debitkarten (e.g. Girocard mit PIN – Persönliche Identifikationsnummer oder ohne) auf 35% zu verzeichnen. Insgesamt liegen die Transaktionen bei 19% mit einer Zunahme von 4% im Jahr 2014. Die Zahlung mit Kreditkarten erfolgt meist bei höheren Beträgen, diese liegen im Schnitt bei 81 € (App. 2). Der Anteil an kontaktlosen Zahlungen stieg in 2017 erstmals auf 1,1%, welcher in den Vorjahren 0-0,1% betrug. Zahlungen mit Smartphone oder Kunden- bzw. Prepaidkarten fallen kaum ins Gewicht. Die Erfassung von Zahlungen an Freunde und Bekannte per App wurden erstmalig im Jahr 2017 erfasst und betragen 5%. Dies ist ein recht hoher Anteil, wenn bedacht wird, dass diese zumeist erst im Jahr 2017 Einzug gehalten haben. Im Onlinehandel werden Internetzahlungen präferiert. Deren Anteil am Gesamtumsatz stieg um knapp 4% (Deutsche Bundesbank 2018:8 f.).

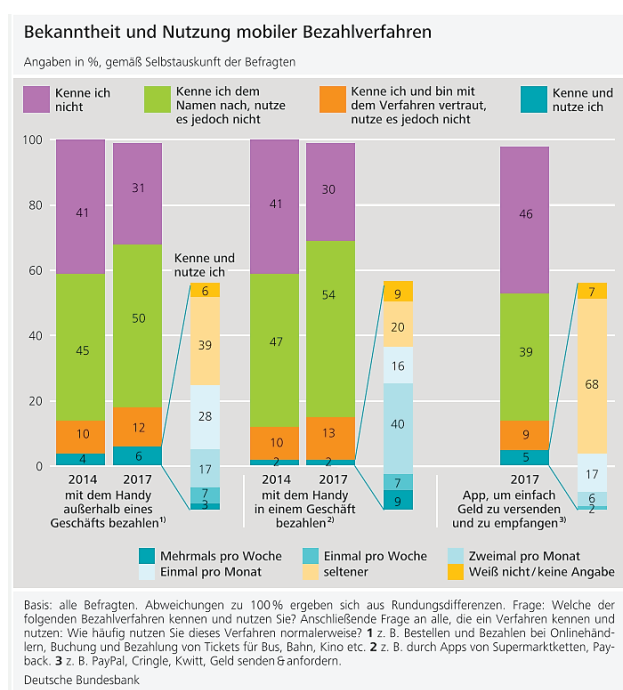
Tab. 1 Anteil von Zahlungsmitteln nach Umsatz 2008 - 2017

Zahlungsinstrument	Umsatz in €	Anteil in %			
		2017	2014	2011	2008
Barzahlung	297.901,48	47,6	53,2	53,1	57,9
Girocard	212.576,36	34	29,4	28,3	25,5
Kreditkarte	27.578,11	4,4	3,9	7,4	3,6
Kontaktloskarte	7.103,04	1,1	0,1	0,1	0
Kundenkarte	411,71	0,1	0,1	0,1	0,2
Vorausbezahlte Karte	83,83	0	0	0,1	0,6
Mensa-/Stadionkarte	180,01	0	0	0	0
Überweisung	34.749,06	5,6	5,3	8,2	8,9
Lastschrift	15.180,80	2,4	3	0,7	1,9
Internetbezahlverfahren	23.258,40	3,7	2,8	1,7	0,3
Mobile Bezahlverfahren	123,76	0	0	0	0
Sonstige	1.005,63	0,2	0,1	0,2	0,4
Unbar (ohne Angabe)	5.949,32	1	2,3	0	1
Summe	626.101,51				

Quelle: Deutsche Bundesbank 2018:24

88% aller Befragten gaben an, zukünftig weiterhin mit Bargeld zahlen zu wollen. Eine Bargeldabschaffung bzw. Bargeldeinschränkung durch Bargeldobergrenzen lehnen sie ab und zeigen sich trotz langsam ändernder Vorlieben für die Bezahllart mit der klassischen Bezahlmethode zufrieden. Indes ist bereits in der Entwicklung von 2011- 2017 ein Trend zu anderen Bezahlmöglichkeiten erkennbar. Alternativen werden bevorzugt durch jüngere Personen gesucht, welche u.a. auch angaben, ihr Girokonto bei verfügbarer Möglichkeit bei einem Internetanbieter zu führen. In der Altersklasse der 18-24-Jährigen sind sogar 24% dazu bereit, Geld an Freunde oder Bekannte mit dem Mobiltelefon zu transferieren (Deutsche Bundesbank 2018:9 f.). Die Nutzung mobiler Zahlverfahren ist bis dato aber noch gering und beschränkt sich zum großen Teil auf das Bezahlen im Internet oder bei Zahlungen von Fahrkarten für öffentliche Verkehrsmittel. Die Befragten, welche bereits mobile Zahlverfahren kennen, aber vom Gebrauch Abstand nahmen, gaben an, dafür entweder kein Bedarf in dieser Zahlmethode zu sehen oder dass es aus ihrer Sicht zu unsicher ist. Weiterhin wurden die Nichtverwendung mit der Komplexität oder fehlende technische Voraussetzungen begründet (Abb. 5) (Deutsche Bundesbank 2018:26).

Abb. 5 Bekanntheit und Nutzung mobiler Bezahlverfahren



Quelle: Deutsche Bundesbank 2018:27

Bei Zahlungen größerer Beträge von über 500 € werden durch die Befragten unbare Zahlungsmöglichkeiten präferiert. Diese kommen ein- bis zweimal im Jahr bei 67% der Befragten für langlebige Wirtschaftsgüter in Frage und bei 61% für die Zahlung von Urlaubsreisen. Die Schenkung von Geld hingegen wird zu 77% in bar vorgenommen. Die 500 € Note wurde bis dato von 20% der Befragten verwendet. Der höhere Anteil der Verwendung dieser hohen Denomination lag jedoch bei 35% der Befragten im Sparen (Deutsche Bundesbank 2018:29). Bei der Frage nach den Eigenschaften von Zahlungsmethoden für ihre Präferenz wurden folgende Angaben durch mehr als 90% der Befragten gemacht (App. 3):

- Verlostsicherheit,
- guter Ausgabenüberblick,
- unkomplizierte Nutzung und Vertrautheit und die
- Wahrung der Privatsphäre/Anonymität (Deutsche Bundesbank 2018:30).

Von allen genannten Zahlungsmethoden erfüllt Bargeld bis dato die gewünschten Eigenschaften. Lediglich Debitkarten verfügen über einen höheren Schutz vor Verlust (Deutsche Bundesbank

2018:33). Bei der Frage nach künftigen Präferenzen für Zahlungsmethoden gaben 88% an, weiterhin Barzahlungen nutzen zu wollen. 2% plädierten für eine völlige Abschaffung des Bargelds, während der verbleibende Anteil von 10% eine Substitution des Bargelds durch andere Bezahlungsmethoden bevorzugt. Die Abschaffung des Bargelds sehen die Befragten kritisch und äußern u.a. folgende Bedenken geordnet nach Gewichtung (App. 4):

- Menschen höheren Alters hätten Probleme mit anderen Bezahlmethoden
- schwerere Erziehung der Kinder im Umgang mit Geld
- geringere Verschuldungskontrolle
- geringere Anonymität
- Eingriff in Persönlichkeitsrechte (Freiheit) (Deutsche Bundesbank 2018:38).

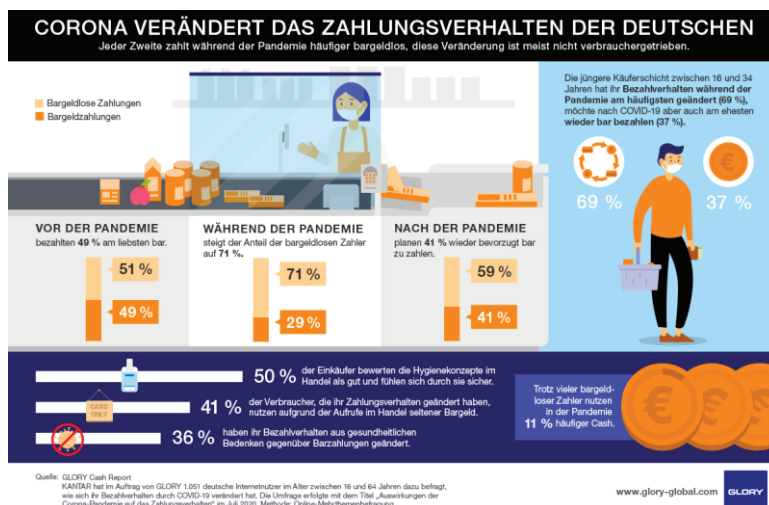
Die Majorität der Befragten geht nicht d'accord, eine Abschaffung könne einen Beitrag zur Eindämmung von Schwarzarbeit leisten. Sie waren auch nicht davon überzeugt, dass Hygiene (Infizierung mit Bakterien und Viren durch Bargeld) ein plausibler Grund für eine Abschaffung wäre. Lediglich wenn eine Abschaffung helfen würde Kosten einzusparen, ergab ein relativ ausgeglichenes Verhältnis der Beteiligten (Deutsche Bundesbank 2018:37). Die Bundesbank kam in 2018 aufgrund ihrer Recherche zu folgender Prognose:

- künftig mehr Kartenzahlungen durch Kontaktlostechnologie
- Zunahme von Einkäufen im Onlinehandel
- Zunahme der Käufe mit Smartphone und Tablet und
- Barzahlungen werden weiter abnehmen (Deutsche Bundesbank 2018:40 ff.).

2.4.2 Das Zahlungsverhalten in Deutschland 2020-2021

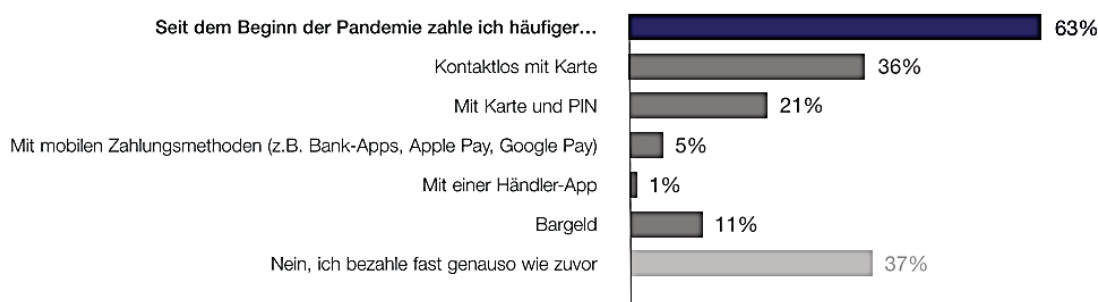
Mitte 2020 führte das Marktforschungsinstitut KANTAR eine Umfrage unter 1.050 16-64-jährigen zum Zahlungsverhalten im Auftrag der Firma GLORY durch. Gefragt wurde nach Änderungen im Zahlungsverhalten vor und nach der Corona-Pandemie (Glory Global Solutions (Germany) GmbH 2020:25). Laut der Umfrage gaben 63% der Befragten an, inzwischen bevorzugt andere Zahlungsmittel als Bargeld zu verwenden. 52% präferierten dabei Kartenzahlungen oder Bezahlungen per Smartphone. Bei den Kartenzahlungen wurde zu 36 % auf Kontaktlosverfahren zurückgegriffen, 21% bevorzugten Kartenzahlungen mit PIN (Abb. 6, Abb. 7) (Glory Global Solutions (Germany) GmbH 2020:25).

Abb. 6 Corona verändert das Zahlungsverhalten in Deutschland



Quelle: Glory, https://www.glory-global.com/de-de/resources/de_de/infografik/corona-ver%C3%A4ndert-das-zahlungsverhalten-der-deutschen/, abgerufen am 17.05.2021

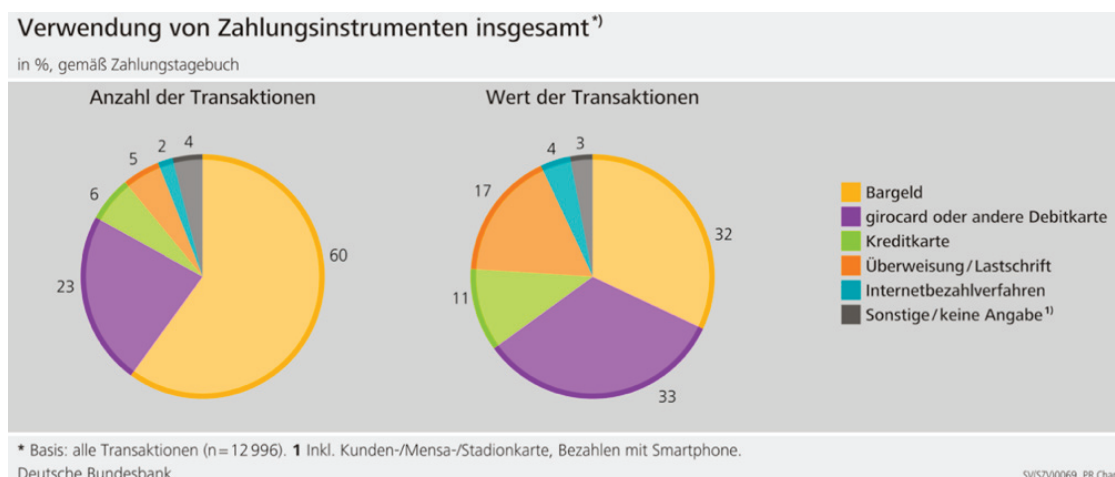
Abb. 7 Änderung des Zahlungsverhalten in der Corona-Krise



Quelle: Glory Global Solutions (Germany) GmbH 2020:27)

Hauptgründe für die Änderung im Zahlungsverhalten waren u.a. die Aufforderung der Händler bzw. Ladenbesitzer während der Corona-Krise unbar zu zahlen und Bedenken hinsichtlich eines Infektionsrisikos bei der Verwendung von Bargeld (Glory Global Solutions (Germany) GmbH 2020:25). Zu ähnlichen Ergebnissen kommt die Bundesbank in ihrer Studie von 2020. Auch hier wurde festgestellt, dass die Kartenzahlungen deutlich zugenommen haben. Auslöser dafür ist aus ihrer Sicht die Corona-Pandemie (Deutsche Bundesbank 2021:3). Während das kontaktlose Zahlen Zulauf erfahren hat, ist jedoch das Zahlen per Smartphone für viele Befragte noch zu unsicher oder zu komplex (Deutsche Bundesbank 2021:5).

Abb. 8 Verwendung von Zahlungsinstrumenten insgesamt



Quelle: Deutsche Bundesbank 2021:18

Nach dem Wert der Transaktionen hat sich die Zahlungsart der Kartenzahlung gegenüber dem Bargeld verbessern können. Geringere Beträge werden aber nach wie vor bevorzugt bar entrichtet (Abb. 8) (Deutsche Bundesbank 2021:18). In der Wertigkeit der Kriterien für die Bevorzugung von Zahlungsmitteln hat sich eine leichte Verschiebung in der Reihenfolge ergeben:

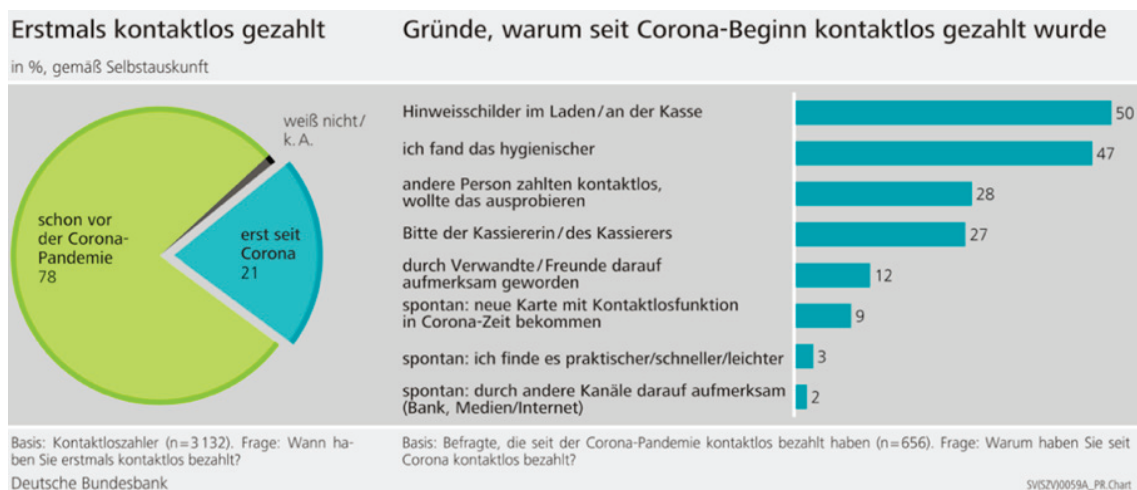
Tab. 2 Vergleich der Bevorzugungen von Zahlungsmitteln 2018 und 2020

2018 ¹	2020 ²
<ul style="list-style-type: none"> Verlustsicherheit guter Ausgabenüberblick unkomplizierte Nutzung und Vertrautheit Wahrung der Privatsphäre/Anonymität 	<ul style="list-style-type: none"> Verlustsicherheit Wahrung der Privatsphäre guter Ausgabenüberblick unkomplizierte Nutzung

Quellen: ¹ Deutsche Bundesbank 2018:30, ² Deutsche Bundesbank 2021:17

Die Hauptgründe für die bevorzugte Zahlung mit Karte sind identisch zur Glory-Studie: die Aufforderung durch die Ladeninhaber/Händler und hygienische Gründe in Bezug auf ein Infektionsrisiko (Abb. 9) (Deutsche Bundesbank 2021:40).

Abb. 9 Kontaktloses Bezahlen mit der Karte



Quelle: Deutsche Bundesbank 2021:40

Auch hier wird ersichtlich, dass die Zahlungen mit Bargeld stetig abnehmen. Ob sich das Zahlungsverhalten nach der Corona-Pandemie wieder rückentwickelt, bleibt abzuwarten. Zumindest gaben bei der Glory-Umfrage 47% der Befragten an, ihr Zahlungsverhalten wieder bevorzugt auf das Bargeld auszurichten. Erstaunlich ist dabei, dass insbesondere die jüngeren Generationen (Altersgruppe 16-24 Jährige mit 53%) wieder das Bargeld präferieren (Glory Global Solutions (Germany) GmbH 2020:29).

2.4.3 Die Bargeldentwicklung in Berlin, Brandenburg und Mecklenburg-Vorpommern von 2012 bis 2021

Die WSN Sicherheit und Service GmbH (WSN) ist eines der größten mittelständischen Geld- und Werttransportunternehmen. Die WSN ging am 02.12.2002 aus der 1990 gegründeten Wach- und Schließgesellschaft Neubrandenburg GmbH hervor und unterhält mehrere Geschäftsstellen in Mecklenburg-Vorpommern und eine Geschäftsstelle in Berlin. Hauptaufgabengebiet ist die transparente und sichere Bargeldlogistik und das Bereitstellen sowie das Auszählen von Kundengeldern in den Cash-Centern (CC) Berlin und Neubrandenburg. Eine interne Auswertung der Zählraten der WSN bestätigt den fortschreitend abnehmenden Trend der Barzahlungen. Die folgenden Zählraten (Angabe in %) sind gesplittet nach den CC der Geschäftsstellen Berlin sowie Neubrandenburg im Zeitraum 2012 bis 2020. Im CC Berlin werden Noten und Münzen aus den Bundesländern Berlin und Brandenburg verarbeitet, das CC in Neubrandenburg ist für die Verarbeitung der Gelder in Mecklenburg-Vorpommern sowie zu geringen Teilen Brandenburgs zuständig. Das höchste Zählergebnis des CC Berlin im Bereich der Münzen konnte im Jahr 2012 identifiziert werden (Tab. 3). Seit diesem Jahr ist eine stetige Abnahme der Münzgeldmenge zu verzeichnen. Ausnahmen bilden die Jahre 2015 und 2016 mit einem kurzfristigen Anstieg zu den Vorjahren, jedoch konnte die Höchstmenge von 2012 nicht wieder erreicht werden. Im Jahr 2021 betrug das Münzgeldvolumen nur noch 49% des Höchstvolumens (App. 5). Das Jahr 2018 konnte für Berlin nicht in der Auswertung berücksichtigt werden, da aufgrund eines Sicherheitsfehlers die Zählraten der Monate 9-12 nicht mehr verfügbar sind. Bei der Notenzählung wurde im Jahr 2015 die Höchstmenge identifiziert. Im Jahr 2021 betrug das Notengeldvolumen nach stetiger Abnahme lediglich 70% des Höchstvolumens (App. 6). App. 7 zeigt die Abnahme des gesamten Geldvolumens um 30,4% im benannten Zeitraum im Vergleich zum Höchstwert im Jahr 2015 (Schmidt 2022 2 f.).

Tab. 3 Prozentuale Entwicklung der Geldzählmengen im Cash-Center Berlin 2012 bis 2021

Jahr	Note in %	Münze in %	Gesamt in %
2012	76,40	100,00	76,72
2013	89,79	85,76	89,81
2014	86,27	84,44	86,30
2015	100,00	94,31	100,00
2016	99,72	91,50	99,69
2017	91,66	74,62	91,53
2019	80,76	69,13	80,68
2020	78,01	56,08	77,81
2021	69,75	48,55	69,56

Quelle: Schmidt 2022:2

Die höchsten Zählsummen im Bereich der Noten- und Münzzählung wurde in CC Neubrandenburg im Jahr 2013 identifiziert. Im vorangegangenen Jahr ist ein geringeres Notengeld- und Münzgeldvolumen zu verzeichnen. Wie Tab. 4 (o.a. App. 8) zeigt, ist die Notengeldmenge seit dem Jahr 2015 moderat rückläufig, nimmt jedoch in den Jahren 2020 und 2021 jeweils um ca. 2% zu. Die ursprüngliche Höhe von 100% aus dem Jahr 2013 konnte jedoch nicht erreicht werden.

Tab. 4 Prozentuale Entwicklung der Geldzählmengen im Cash-Center Neubrandenburg 2012 bis 2021

Jahr	Note in %	Münze in %	Gesamt in %
2012	96,61	87,52	96,41
2013	100,00	100,00	100,00
2014	94,53	88,58	94,40
2015	92,56	85,98	92,41
2016	89,48	77,13	89,22
2017	91,60	75,22	91,25
2018	83,60	69,67	83,30
2019	82,45	67,92	82,14
2020	84,79	51,45	84,07
2021	86,16	47,43	85,32

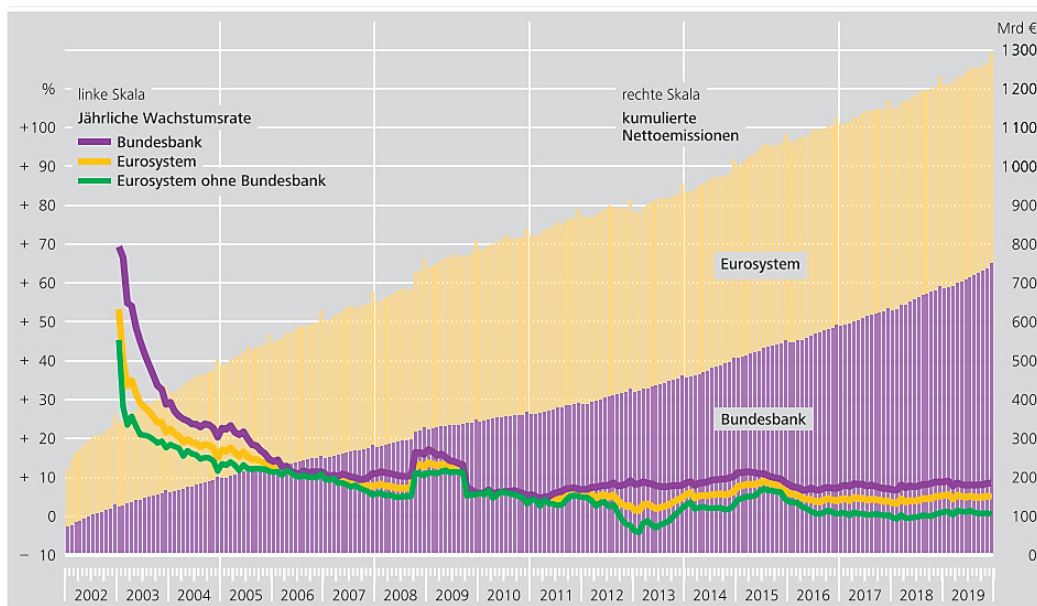
Quelle: Schmidt (2022:5)

So entsprach die Gesamtsumme im Jahr 2021 86,16% (gerundet 86%) im Verhältnis zum eruierten Höchstwert im Jahr 2013. Die Abnahme beträgt somit 14% in einem Zeitraum von acht Jahren. Dies entspricht aufgrund des hohen Wertes von Noten verglichen mit Münzen in etwa der Abnahme der gesamten Geldmenge (App. 10). Die Abnahme in der Münzgeldzählung fällt bedeutend höher im Vergleich zur Notengeldzählung aus (App. 9). Der Höchstwert, eruiert im Jahr 2013, nimmt in den Folgejahren stetig ab. Im Jahr 2021 betrug die Gesamtzählsumme lediglich 47,43 % (gerundet 47%) des Höchstwertes und verzeichnet damit eine Abnahme um 53% innerhalb eines Zeitraums von acht Jahren. Im Durchschnitt beträgt die Abnahme p.a. ca. 1,77 % in der Notenzählung und ca. 8,63 % in der Münzgeldzählung. Die Pandemie hat den Rückgang der Bargeldmenge gering beeinflusst in Bezug auf die Zahlung mit Noten. Zum einen ist es ein Indiz für die Nutzung von Noten als Wertaufbewahrungsmittel während der beiden Lockdowns (1. Lockdown 22.03.2020-04.05.2020, 2. Lockdown 13.12.2020-01.05.2021). Zum anderen ist anzunehmen, dass die Bedeutung des Bargelds auf die Demografie des Bundeslandes MV zurückzuführen ist. Der Anteil der Bevölkerung älter als 65 Jahren liegt hier bei 26-33%, während sie im Großraum Berlin lediglich 10-15% beträgt. Laut statistischer Erhebung aus dem Jahr 2021 präferieren insbesondere die Altersgruppen von 35-65 und älter Bargeldzahlungen (Schmidt 2022:5 f.).

2.5 Bargeldumlauf im Euro-System und Deutschland

Mit einem Zuwachs von sechs Prozent per anno stieg die Bargeldausgabe in der letzten Dekade stetig an. Zum Jahresende 2014 betrug sie über 1,3 Billionen € (Abb. 10). Mit großem Abstand zu anderen Emittenten gab die Deutsche Zentralbank mehr als die wertmäßige Hälfte an Banknoten aus (App. 11) (Deutsche Bundesbank, 2020a:2).

Abb. 10 Bargeldumlauf im Eurosystem



Quelle: Deutsche Bundesbank, 2020a:3

Insbesondere in Krisenjahren, wie bspw. die Finanzkrise im Jahr 2008, nahm die Barknotenauszahlungen zu. Dies verdeutlicht, dass Bargeld bei den Menschen ein hohes Vertrauen besitzt und nicht ausschließlich in Alltags- bzw. Wirtschaftsleben von hoher Bedeutung ist, sondern auch sehr als Wertaufbewahrungsmittel geschätzt wird (Deutsche Bundesbank, 2020a:2). Für die täglichen Dinge des Lebens werden dabei am häufigsten die 50 € Banknoten verwendet, größere Banknoten fungieren hauptsächlich als Wertaufbewahrung. Insbesondere bei der 200 € Banknote wurde nach dem Stopp der Ausgabe der 500 € Note im April 2019 ein starker Ausgabeanstieg verzeichnet. Bereits Ende 2019 waren über 80 Milliarden € in Form von 200 € Noten im Umlauf und entsprach damit 365 Millionen Scheinen (App. 12) (Deutsche Bundesbank, 2020a:5). Festzustellen ist, dass trotz abnehmender Bargeldnutzung ein zunehmender Bargeldumlauf in Deutschland und Europa zu verzeichnen ist.

3 Pro und Contra Argumente einer Bargeldabschaffung / Bargeldbeschränkung

Nach Morscher, Schlothmann und Horsch gibt es sowohl Argumente für die Bargeldabschaffung oder Bargeldbeschränkung als auch dagegen, welcher einer Abwägung bedürfen, dargestellt in Tab. 5:

Tab. 5 Pro und Contra einer Bargeldabschaffung/Bargeldbeschränkung

Pro Abschaffung/Beschränkung	Contra Abschaffung/Beschränkung
abnehmende Geldfälschungen bei Noten und Münzen	Abhängigkeit von Technik und deren Sicherungsproblematiken, dazu zählen die Verfügbarkeit von Internet und die Notwendigkeit von entsprechenden Geräten sowie der Fakt, dass Europa über kein größeres Unternehmen im Kreditkartenbereich verfügt und somit ausländische genutzt werden müssten
Hygiene: Verringerte Krankheitserregerübertragungen	Datenschutz: der sogenannte „Gläserne Bürger“ (Morscher et al. 2017:16): keine Anonymität mehr bei elektronischen Zahlungen, Daten könnten unrechtmäßig gesammelt, gespeichert, ausgewertet und zu Zwecken der Gewinnerzielung verwendet werden
Höhere Bankensystemstabilität, „Bank runs“ (Morscher et al. 2017:18) können verhindert werden	Staaten und Banken haben volle Kontrolle und Macht über den Einzelnen und damit höhere Durchsetzungsmöglichkeit einer Negativzinspolitik, von Kontrollen des Kapitalverkehrs oder der Durchsetzung von Steuern und Gebühren
Verringerung der Kriminalität - Schattenwirtschaft und Schwarzarbeit, Hinterziehen von Steuern, Verhinderung oder Reduzierung des Terrorismus, Raubüberfälle auf Banken wären ausgeschlossen bei kompletter Abschaffung.	bessere Kontrolle über die Ausgaben bei den Verbrauchern
eventuelle Zeiteinsparungen beim Point of Sale (POS), Möglichkeit einer automatisierten Abrechnung	keine freie Wahl für Barzahlungen, da bares Geld entfällt
Kosten der Transaktion, Münz- und Notenherstellung inkl. dem verwendeten Material und Herstellungskosten, Transportkosten, Kosten für Noten- und Münzrecycling usw. entfallen	Opportunitätskosten der Bargeldabschaffung: Energie, Technik, Netz- und Internetausbau etc.
eventuell verringerte Belastung der Umwelt + (Mögliche) reduzierte Umweltbelastung	höherer Energieverbrauch bei elektronischen Zahlungen, mehr Technik, Netz- und Internetausbau etc. (Morscher et al. 2017: 16 ff.)

Quelle: eigene Darstellung in enger Anlehnung an Morscher et al. 2017:16 ff.

Weitere Gründe für die Nichtabschaffung des Bargelds sind für Thiele die Zug-um-Zug Zahlung. Diese gewährleistet den Schutz vor Insolvenz, da eine Vorleistung weder für den Käufer noch für den Verkäufer notwendig ist. Für eine Zahlung mit Bargeld wird keine Technik benötigt, was besonders in Krisenzeiten von Vorteil ist. Thiele betont weiterhin, dass Bargeld keine Beschränkung im Zugang hat, d.h. es kann von Jedermann genutzt werden. Das ist vor allem für die Menschen wichtig, welchen der Zugang zu unbaren Zahlungsmethoden verwehrt ist (Thiele 2017). In Bezug auf bargeldlose Zahlungen ist Schweden ein Vorzeigeland. Dort werden kaum noch Barzahlungen vorgenommen. Über Bargeld verfügt nur noch jede vierte Bankfiliale und Geldautomaten wurden rückgebaut. Die logische Konsequenz ist, dass infolgedessen die Zahl der Banküberfälle drastisch abnahm. Die Innovationen im Bereich der elektronischen Möglichkeiten von Zahlungen lassen einen Trend erahnen. Zahlungen sind bereits on- oder offline möglich, selbst wenn keine eigene Technik zur Verfügung steht. Über Geldsummen kann bereits mit Hilfe von Fingerabdruckverfahren, Iris-scannung oder Gesichtsscannung verfügt werden. Aber auch die Identifikation mittels DNA findet bereits Verwendung. Für die Zahlung kleinerer Beträge stehen die Möglichkeiten der Verwendung von Prepaidkarten oder mobilen Wallets (digitale Geldbörse) zur Verfügung. Die Vorteile für Banken liegen dabei auf der Hand. Zum einen könnten Kosten für die Versorgung mit Bargeld eingespart und zum anderen könnte auf elektronisches Geld Provision und Gebühren erhoben werden. Aus technischer Sicht gibt es mehrere Gründe für die Bargeldabschaffung. Barzahlungen sind unhygienisch, mit Risiken behaftet und ineffizient in Bezug

auf die Kosten des Transports, der Vorhaltung in Geräten wie Automaten, Lagerung und im Recycling. Aus Innovationssicht ist elektronisches Geld daher für Banken die effizientere Wahl. Wobei zu berücksichtigen ist, dass trotz unzähliger Studien in Bezug auf Kosten und Effizienz behaupten, elektronisches Geld im Vorteil zu sehen, bis dato keine wissenschaftliche Evidenz dafür existiert. Zudem werden Kosten und Aufwand von Sicherungsmaßnahmen elektronischer Systeme gegen Cyberkriminalität oftmals bei den Studien nicht mit einbezogen. Eine weitaus wichtigere Begründung wäre hier der Verlust der Anonymität in Verbindung mit der Bekämpfung von Kriminalität. Bargeldströme können aufgrund ihrer Anonymität nicht zurückverfolgt werden. In hohen Denominationen sind größere Beträge einfach transportierbar und eignen sich daher für die organisierte Kriminalität. Elektronische Geldströme hingegen sind nachzuverfolgen, da sie Spuren hinterlassen und dokumentiert werden. Das wiederum hat zum Vorteil, dass Delikte wie Geldwäsche oder illegale Geschäfte erschwert werden könnten. Auch wird angenommen, dass bei einer Bargeldabschaffung ein Rückgang der Schattenwirtschaft i.H.v. 15% zu erreichen wäre. Zweckdienlich wäre es ebenso für die Einkommenskontrolle und Einkommensbesteuerung. In Bezug auf die Geldpolitik der Zentralbanken wäre die Durchsetzung einer Negativzinspolitik vereinfacht. Ohne das Vorhandensein von Bargeld wäre es den Menschen nicht mehr möglich, bei Einführungen oder Erhöhung von Negativzinsen Bargeldabhebungen vorzunehmen, um Negativzinsen auszuweichen. „Günstigerer Zahlungsverkehr, weniger Kriminalität, effektivere Geldpolitik – ist die Sachlage wirklich so eindeutig? Gegner dieses Vorschlags sehen das nicht so – und haben gute Argumente.“ (Bacher/Beck 2015:39)

4 Schritte zur Bargeldbeschränkung -abschaffung in chronologischer Reihenfolge

4.1 Abschaffung der 500 € Banknote

Am 4. Mai 2016 verkündete der Rat der Europäischen Zentralbank (EZB) auf seiner Webseite aufgrund einer Prüfung der Stückelungsstruktur die Produktion des 500 Euro Scheins für immer einzustellen. Erreicht werden soll, illegale Handlungen mit der hohen Banknote einzuschränken. Zum Ende des Jahres 2018 sollte demnach die Produktionseinstellung vollzogen werden. Zeitgleich wurden neue 100 € und 200 € Banknoten eingeführt. Bisherige vorhanden Stückelungen wurden von dieser Regelung nicht tangiert. Weiterhin bleibt die 500 € Note ein gesetzliches Zahlungsmittel (Europäische Zentralbank 2016). Der Rat der EZB folgte damit der Auffassung der Europäischen Kommission, Bargeld allgemein und insbesondere hohe Noten würden vor allem für kriminelle Zwecke verwendet (Europäische Kommission 2016:11).

4.2 Absenkung der Meldepflicht für Bargeschäfte

Am 26.06.2017 trat das Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen in Deutschland in Kraft (Bundesministerium für Finanzen 2017). Die EU-Geldwäscherichtlinie (EU 2015/849) vom 23.06.2017 und die EU- Verordnung über die Übermittlung von Angaben bei Geldtransfers (Verordnung (EU) 2015/847) vom 20.05.2015 wurden bei der Novelle des Geldwäschegesetzes (GwG) in Deutschland umgesetzt. § 10 Abs. 6 GwG enthielt die bedeutendste Veränderung bzw. Anpassung. Demnach sollen Meldepflichten für Barzahlungen von 15.000 € auf 10.000 € abgesenkt werden. Zudem wurde eine Schriftformpflicht bei grenzüberschreitenden Bargeldbewegungen eingeführt, welche zuvor mündlich übermittelt werden konnten (Durgeloh Oliva 2020). Gründe für die Überarbeitungen waren u.a.:

- „Ströme von illegalem Geld können die Integrität, Stabilität und das Ansehen des Finanzsektors schädigen und eine Bedrohung für den Binnenmarkt der Union sowie die internationale Entwicklung darstellen. Geldwäsche, die Finanzierung des Terrorismus und organisierte Kriminalität sind nach wie vor bedeutende Probleme, die auf Ebene der Union angegangen werden sollten.
- Die Solidität, Integrität und Stabilität der Kreditinstitute und Finanzinstitute sowie das Vertrauen in das Finanzsystem insgesamt könnten schweren Schaden nehmen, wenn Straftäter und ihre Mittelsmänner versuchen, die Herkunft von Erträgen aus Straftaten zu verschleiern

oder Geld aus rechtmäßigen oder unrechtmäßigen Quellen terroristischen Zwecken zuzuführen. Geldwäscher und Geldgeber des Terrorismus könnten versuchen, die Freiheit des Kapitalverkehrs und die Finanzdienstleistungsfreiheit, die der integrierte Finanzraum der Union bietet, für ihre kriminellen Aktivitäten auszunutzen.

- Geldwäsche und Terrorismusfinanzierung finden häufig in internationalem Kontext statt. Maßnahmen, die nur auf nationaler oder selbst auf Unionsebene erlassen würden, ohne grenzübergreifende Koordinierung und Zusammenarbeit einzubeziehen, hätten nur sehr begrenzte Wirkung. Aus diesem Grund sollten die von der Union auf diesem Gebiet erlassenen Maßnahmen mit den im Rahmen der internationalen Gremien ergriffenen Maßnahmen vereinbar und mindestens so streng sein wie diese. Insbesondere sollten sie auch weiterhin den Empfehlungen der Financial Action Task Force on Money Laundering (FATF, Finanzbehördliche Eingreiftruppe für Geldwäsche) und den Instrumenten anderer internationaler Gremien, die im Kampf gegen Geldwäsche und Terrorismusfinanzierung aktiv sind, Rechnung tragen
- Hohe Barzahlungen können sehr leicht für Geldwäsche und Terrorismusfinanzierung missbraucht werden. Um die Wachsamkeit zu erhöhen und die mit solchen Barzahlungen verbundenen Risiken zu mindern, sollten Personen, die mit Gütern handeln, von dieser Richtlinie erfasst werden, wenn sie Barzahlungen von 10 000 EUR oder mehr tätigen oder entgegennehmen. Die Mitgliedstaaten sollten niedrigere Schwellenwerte, zusätzliche generelle Barzahlungsbeschränkungen und weitere strengere Vorschriften erlassen können.“ (Europäischer Rat/Europäische Kommission 2015:1 f.).

Der Personenkreis der Meldepflichtigen wurde zudem stark ausgeweitet. Gemäß § 2 GwG sind nun u.a. Unternehmen zur Meldung und Identitätsprüfung verpflichtet, zu denen folgende Beispiele zählen: „[...] Banken, Finanzagenturen, Versicherungen und Spielbanken“. Unter meldepflichtige Personen fallen: „[...] beispielsweise Rechtsanwälte, Notare, Wirtschaftsprüfer, Makler und Gewerbetreibende wie z.B. Juweliere, Kfz- oder Antiquitätenhändler“ (Deutscher Bundestag 2017:3). Bei der Bezahlung mit einem Bargeldwert ab 10.000 € müssen dabei folgende Daten des Käufers erfasst werden: „[...] Vor- und Nachname, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Wohnanschrift“ (Deutscher Bundestag 2017:3). Diese Angaben hat der Händler aufzuzeichnen und aufzubewahren (Europäisches Verbraucherschutzzentrum Deutschland 2020). Seit dem Jahr 2020 plädiert das Bundesministerium für Finanzen für eine EU-weite Absenkung des Betrages von 10.000 € auf 2.000 €. Ab einem Betrag von 2.000 € sollen somit Käufer die Pflicht haben, sich per Ausweis identifizieren zu müssen (Redaktion beck-aktuell 2020). Zumindest für den anonymen Kauf von Edelmetallen wie Gold und Silber gilt seit dem 01.01.2020 diese Barzahlungsobergrenze i.H.v. 2.000 € mit Registrierungspflicht (Europäisches Verbraucherschutzzentrum Deutschland 2020).

4.3 Flächendeckende Barzahlungsobergrenze in Europa

Bereits im Jahr 2016 wurde in Deutschland über die Einführung einer solchen Zahlungsgrenze i.H.v. 5.000 € diskutiert und durch das Finanzministerium geprüft (Hirdina 2016:1).

Derzeit wird eine EU-weite Barzahlungsobergrenze i.H.v. 10.000 € von der Europäischen Kommission geplant. Dabei wurden folgende Vorschläge für eine Gesetzeserlassung unterbreitet:

1. Einrichtung einer neuen Behörde
2. Vereinheitlichung der Regeln innerhalb der EU
3. Aktualisierung der Richtlinien mit anschließender Umwandlung in nationales Recht (Vorschriften über Aufsichtsbehörden, zentraler Meldestellen in den EU-Ländern)
4. EU-weite Barzahlungsobergrenze von 10.000 €

zum Zwecke der Bekämpfung von Geldwäsche und Finanzierung von Terrorismus. Auch Bitcoins sollen einer stärkeren Regulierung unterworfen werden, um eine Nachverfolgung von Kapitalströmen zu gewährleisten. Anonyme Krypto-Wallets sollen zudem verboten werden (tageschau 2021).

4.4 Die Einführung der Central Bank Digital Currency (CBDC)

Für das Jahr 2026 ist die Einführung eines digitalen Euro geplant. Beschlossen wurde dies im Juli 2021. Ausgegeben werden soll dieser, wie das Bargeld, von der EZB sowie den zuständigen Zentralbanken der Länder und soll von Unternehmen und privaten Personen genutzt werden. Dabei betont die EZB, dass der digitale Euro nicht das Bargeld ersetzen, sondern eine weitere Zahlungsmöglichkeit darstellen soll. Mit ihm soll u.a. die Bezahlung vereinfacht werden und Inklusion sowie Verfügbarkeit verbessern (EZB 2021). Die von der EZB angegebenen Vorteile des digitalen Euro sind in Abb. 11 zu sehen.

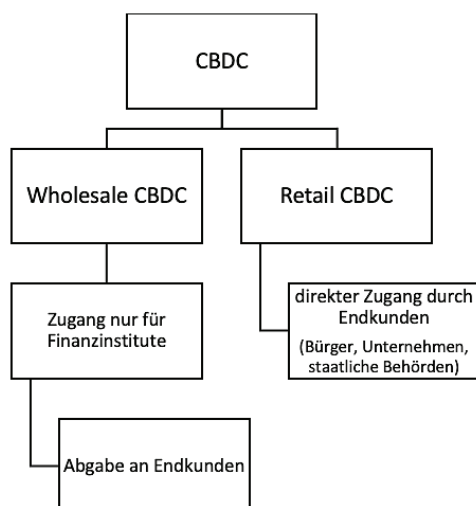
Abb. 11 Gründe für die Einführung eines digitalen Euro



Quelle: EZB 2021. abgerufen am 11.08.2021

Einer Studie der Bank für Internationalen Zahlungsausgleich (BIZ) zufolge wird eine Einführung einer CBDC bereits durch 10% aller Zentralbanken auf kurzfristigem und von weiteren 20% der Zentralbanken auf mittelfristigem Weg für die Öffentlichkeit geplant. China ist dem bereits voraus mit dem Test einer digitalen Zentralbankwährung seit Mitte April 2020 (Bitkom 2020a:3). Die EZB betont weiterhin, dass mit dem digitalen Euro der Schutz der Privatsphäre geleistet wäre, damit ein Vertrauen in die Währung erhalten bleibt (EZB 2021). Derzeit wird noch über die Ausgestaltung der CBDC diskutiert. Der Transfer soll über eine Distributed Ledger Technologie (DLT) erfolgen, zudem soll die CBDC digital programmierbar sein. Insgesamt gibt es zwei Überlegungen. Eine Variante ist die „Wholesale CBDC“ (Bitkom 2020a:8), die zweite ist die „Retail CBDC“ (Bitkom 2020a:8). Je nach Ausgestaltung wird die CBDC entweder gleich an den Endverbraucher verteilt oder wie bisher über Geschäftsbanken abgewickelt (Abb. 12) (Bitkom 2020a:8).

Abb. 12 Ausgestaltungsmöglichkeiten des CBDC



Quelle: eigene Darstellung in enger Anlehnung an Bitkom 2020a:8

Die zur Verwendung stehende Höchstgrenze pro Nutzer soll auf 3.000 € begrenzt sein und ausschließlich der Bezahlung dienen. Die Speicherung erfolgt in digitalen Wallets. Wie bereits beschrieben, sollen Datenschutz und Privatsphäre gewährleistet werden, allerdings nur im Rahmen der geltenden Geldwäschegesetze (Mai/Wiener Zeitung 2021). Beträge über 3.000 € sollen dabei automatisch auf Girokonten umgebucht werden (Donath/Golem 2021). Das Konzept der EZB weist jedoch ein Problem in Bezug auf den Datenschutz bei der Retail Variante auf. Teilweise ist eine Anonymität gegeben trotz Berücksichtigung von Geldwäschegesetzen. Die Identität des Benutzers und die Historie der Transaktionen werden nicht offengelegt durch sogenannte Anonymity Vouchers (Anonymitätsgutscheine), die einer Zahlung beigelegt werden können. Allerdings ist die Anzahl dieser begrenzt. Sind diese verbraucht, sind weitere Zahlungen nicht anonym, d.h. sämtliche Transaktionsdaten können durch Banken eingesehen werden (Groß/Klein/Sandner 2020:548 f.).

5 Untersuchung ausgewählter Thesen der Bargeldabschaffung

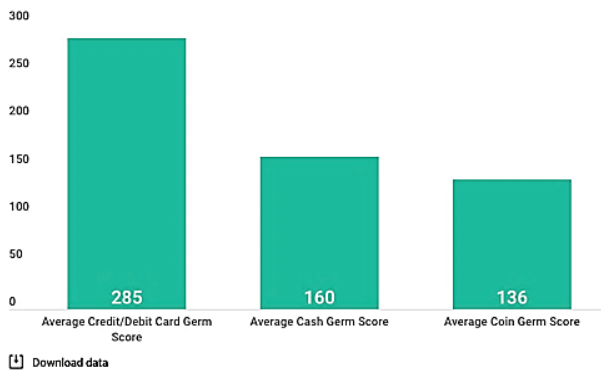
Im folgenden Abschnitt werden ausgewählte Thesen der Bargeldgegner und Befürworter der Bargeldabschaffung oder Bargeldbeschränkung näher untersucht.

5.1 Bargeld ist unhygienisch

In einer von MasterCard in Auftrag gegebenen Studie an der Universität Oxford über den Hygienezustand von Bargeld wurde festgestellt, dass sich auf EU-Banknoten im Durchschnitt 26.000 gesundheitsgefährliche Bakterien befinden. 2014 führte MasterCard eine Befragung durch, wie die Teilnehmer der Studie verschiedene Gegenstände hygienisch einstufen (App. 13). Dabei stellte sich heraus, dass trotz der veröffentlichten Studie und den eigenen Erkenntnissen, wie unhygienisch das Bargeld sei, die Menschen innerhalb der EU weiterhin Bargeld benutzen und sich nicht gegen die Bakterien schützen. Zitiert wird durch MasterCard auch Dr. Jim O'Mahony vom Cork Institute of Technology in Irland, biowissenschaftlicher Dozent, dass es schon lange bekannt sei, dass es eine Korrelation zwischen hygienischen Problemen und Bargeld gäbe. Weitere wissenschaftliche Studien belegen aus ihrer Sicht die Kontaminierung des Bargelds mit Mikroben und Bakterien. MasterCard gibt an, dass sich die Menschen zwar der Gefahr bei der Verwendung bewusst sind, sie jedoch keine hygienischen Maßnahmen ergreifen würden. Die Menschen würden dies jedoch erst erkennen, wenn sie mit anderen unhygienischen Handlungen wie das Anfassen von Türklinken beim Toilettengang oder dem Anfassen von Rolltreppengeländern konfrontiert würden. Weiterhin raten sie an, insbesondere in Zeiten wie Grippeausbrüchen oder „Winterdurchfall“ (MasterCard 2014) auf bargeldlose Zahlungsmöglichkeiten auszuweichen. Chris Kangas - Head of Contactless Payments bei MasterCard Europe - bemängelt, dass trotz dieser Erkenntnisse Bargeld verwendet wird und ist der Meinung, die Menschen sollten „[...] die unschöne Angewohnheit der Bargeldnutzung“ (MasterCard 2014) aufgeben. Zum einen seien Kontaktloszahlungen wesentlich innovativer und zum anderen würde es die Hygiene unterstützen, da Menschen sich so gegen Bakterien schützen können, welche bei Barzahlungen übertragen werden (MasterCard 2014). Im Jahr 2020 untersuchte LendEDU unter Verwendung eines wissenschaftlichen Gerätes, welches die Keimbelastungen misst, unterschiedliche Gegenstände auf ihre Verkeimung. Es sollte dabei u.a. geklärt werden, wie schmutzig Geld und verwendete Zahlkarten sind. Daraus ergaben sich folgende Ergebnisse. Getestet wurden 41 unterschiedliche Kredit- und Debit Karten (Vorder- und Rückseite), 27 unterschiedliche Geldscheine sowie 12 verschiedene Münzen. Eine Verkeimung mit dem Wert 10 ist dabei bspw. in Lebensmittelbetrieben das Optimum. Bei dem Test stellte sich heraus, dass die höchste durchschnittliche Keimzahl i.H.v. 285 auf Kredit- und Debit Karten festgestellt wurde. Sie lag zudem auch noch weit höher als die durchschnittliche Keimbelastung auf Banknoten mit 160 und auf Münzen mit 136 (Abb. 13) (Brown/LendEDU 2020).

Abb. 13 What is the Dirtiest: Cash, Cards or Coins

On Average, What's the Dirtiest: Cash, Cards, or Coins?



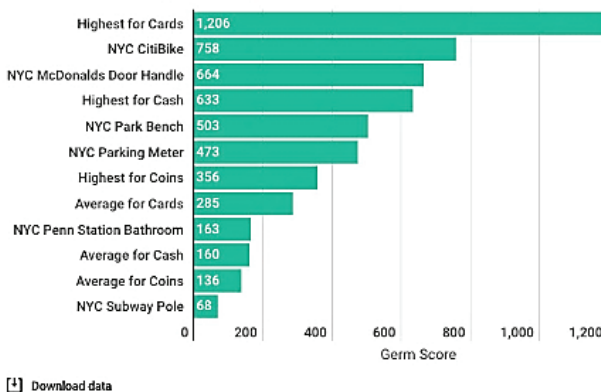
After testing 41 different credit and debit cards, 27 different bills, and 12 different coins, these were the average germ scores for each form of payment.

Quelle: Brown/LendEDU 2020. abgerufen am 17.07.2021

Das Ergebnis überraschte selbst die Testenden, da sie erwartet hatten, Bargeld sei in der Keimbelastung am höchsten. Weiterhin wurde die Verkeimung von anderen Gegenständen mit der Keimbelastung von Bargeld und Kredit- und Debitkarten verglichen. Die höchste Verkeimung wurde dabei auf einer Bezahlkarte mit einer Keimzahl von 1.206 festgestellt. Die durchschnittliche Verkeimung bei Kreditkarten lag mit 314 gefundenen Keimen noch über den der Debitkarten mit einer Keimzahl von 243 (App. 14). Die höchste festgestellte Verkeimung auf einer Banknote lag dabei im Vergleich bei 633 auf einem 20\$ Schein aus dem Jahr 2009. LendEDU verglich Zahlkarten und Bargeld mit anderen Gegenständen wie bspw. der Türklinke eines McDonalds Eingangs, U-Bahn-Haltestangen in Manhattan oder Toiletten in der Penn-Station im Raum New York. Dabei wurde festgestellt, dass Debit- und Kreditkarten keimbelasteter waren als der Türgriff im Eingangsbereich von McDonalds oder ein getestetes City Bike. Banknoten hingegen reihten sich auf dem vierten Rang ein (Abb. 14).

Abb. 14 How dirty are payment methods compared to known filthy things?

How Dirty Are Payment Methods Compared to Known Filthy Things?



Note: A higher germ score indicates a dirtier surface and vice versa. It is recommended that a food establishment surface should have a germ score of 10 or less.

Quelle: Brown/LendEDU 2020. abgerufen am 17.07.2021

Sean Perry - ein von LendEDU im Interview befragter Hygieneexperte und Gründer eines großen Reinigungsunternehmens - brachte zum Ausdruck, dass grundsätzlich bei Geld auf die Hygiene geachtet werden sollte, um eine Verkeimung verzehrter Nahrungsmittel zu verhindern. So sollten

aber auch Zahlkarten mindestens halbjährlich gereinigt werden (Brown/LendEDU 2020). Bereits im Jahr 2010 wurde die Keimbelastung von 1.280 Banknoten aus dem Lebensmittelbereich in zehn unterschiedlichen Ländern der Welt (Australien, Burkina Faso, China, Irland, Niederlande, Neuseeland, Nigeria, Mexiko, Vereinigtes Königreich und Vereinigte Staaten) getestet. Dabei wurde die Erkenntnis erlangt, dass die Höhe der Keimbelastung von mehreren Faktoren abhängt. Zum einen hängt die Keimbelastung vom Alter der Banknote ab, d.h., je mehr sie im Umlauf gewesen ist, desto höher ist die Keimbelastung. Zum anderen war das Material, aus dem die Banknote bestand, ein entscheidender Faktor für die Verkeimung. Hier gab es Unterschiede, da Banknoten auf Polymerbasis oder Baumwollbasis produziert wurden. Weiterhin wurden Banknoten auf krankheitserregende Keime untersucht. Dabei stellte sich heraus, dass erst nach Anwendung von Anreicherungsmethoden eine Isolation von Krankheitserregern möglich war. Die Erreger wurden somit in der vorhandenen geringen Keimbelastung als nicht gesundheitsgefährdend eingestuft. Auch hier wurden als Vorsichtsmaßnahmen das Händewaschen und in Lebensmittelbereichen das Tragen von Handschuhen nahegelegt (Vriesekoop/Russell/Alvarez-Mayorga et al. 2010:1497). Auch Thiele hält fest, dass für die Keimbelastung u.a. die Materialverwendung ein wichtiger Faktor ist. So beruft sich Thiele auf australische Wissenschaftler, welche feststellten, dass die Keimbelastung auf Banknoten auf Polymerbasis deutlich geringer ist. Weiterhin wird angeführt, dass die auf den Banknoten festgestellte Keimbelastung zu gering ist, um Krankheiten verursachen zu können. Natürlich sollten Hygieneregeln Beachtung finden, vor allem in Bereichen mit Lebensmitteln. Hier sorgen aber das Händewaschen und das Tragen von Einweghandschuhen Abhilfe. Bargeldlose Zahlungsmethoden sind mit Berufung auf Experten aus Thieles Sicht nicht gesünder. Außerdem ist Thiele der Meinung, dass aufgrund der niedrigen Keimbelastung das Immunsystem der Menschen trainiert wird und damit sogar gesundheitsfördernd sein könne (Thiele, S. 2017). Fassbinder führt zudem an, dass Geld mit Sicherheit keimbelastet ist, aber bei Abklatschuntersuchungen festgestellt wurde, dass sich nur eine sehr geringe Menge an Keimen bei Berührung mit Banknoten löst und auf die Hände gelangt. Festgestellt werden konnte, dass sich eine Keimzahl von 100 bei einer Belastung von 1.000 lösen konnte. Weiterhin waren die meisten Keime davon nicht einmal gesundheitsgefährdend. Die geringe Zahl der Keime müssten für dann auch noch über das Zuführen in den Mund oder offene Wunden in den Körper gelangen, um Krankheiten auslösen zu können (Fassbinder 2019). Trotz dieser Studien hält sich die Meinung, Bargeld sei gesundheitsgefährdend hartnäckig. Mit dem Aufkommen der Corona-Krise wurde dieses Thema wieder in den Fokus gerückt, oftmals auch unter Bezugnahme auf die MasterCard-Studie. Es wurde die Frage gestellt, inwieweit Bargeld für eine Verbreitung des Virus verantwortlich gemacht werden könnte bzw. ob es ratsam wäre, Bargeld in Zeiten der Krise zu verwenden. Von der BIZ wurde festgestellt, dass es einen starken Anstieg von Suchanfragen im Internet zu diesem Thema gab. Jedoch betont auch Harris hier, dass es wissenschaftlich nicht belegt ist, das Virus könne durch Bargeld übertragen werden. Weiterhin führt Harris an, dass die Keimbelastung mindestens genauso hoch wäre wie auf anderen täglich benutzten Gegenständen wie bspw. Türgriffen (Harris 2020). Die Weltgesundheitsorganisation (WHO) twitterte im Jahr 2020 zum Thema Infektionen in Bezug auf Bargeld: „Das Risiko, sich durch Berühren von Münzen, Banknoten, Kreditkarten und anderen Gegenständen mit dem neuen #coronavirus zu infizieren, ist sehr gering.“ (World Health Organization 2020). Auch Bundesbankvorstand Beermann wies in einer Pressemitteilung darauf hin, dass eine Infektionsgefahr durch Bargeld sehr gering ist, sogar geringer als bei unzähligen anderen Alltagsgegenständen. Hier führt Beermann an, dass die besonders hoch im Umlauf befindlichen 5 bzw. 10 Euro Banknoten über einen „Schutzlack“ (Deutsche Bundesbank 2020b) verfügen, welcher dadurch eine hohe Verschmutzung bzw. daraus eventuell folgende Infektion verhindert. Infektologe René Gottschalk, welcher die Leitung des Gesundheitsamts der Stadt Frankfurt am Main innehat, schließt die Gefahr der Infektion mit dem Corona Virus via Bargeld aus, da es nicht entscheidend ist, wie lange sich Viren auf Noten befinden. Der essenzielle Faktor eines Infektionsweges ist dabei ausschlaggebend und genau diesen sieht Gottschalk bei Banknoten nicht gegeben. Für Gottschalk stellen die häufigste Infektionsmöglichkeit Tröpfchen dar, welche beim Husten, Niesen und ebenso Sprechen gegeben sind. Weiterhin gibt Gottschalk zu bedenken, dass wenn eine Infektion wirklich via Banknoten übertragen werden würde, die Zahl der Infektionsfälle wesentlich höher wäre (Deutsche Bundesbank 2020b).

5.2 Bargeld behindert die Geldpolitik der Europäischen Zentralbank

Bargeld stellt eine sogenannte „Nullzinsschranke“ (Letzgas 2017:67) dar. Die Zentralbanken der Länder können zwar Negativzinsen auf Bargeldvolumen einführen, jedoch würden die Geschäftsbanken den Negativzins nicht an ihre Kunden weitergeben, so Letzgas im Jahr 2017. Befürchtet wurde, dass die Kunden der Banken das Geld von ihren Konten abheben, um es sicher vor dem Negativzins aufbewahren zu können. Folglich sind die Zentralbanken damit in ihrem Handeln eingeschränkt in Bezug auf geldpolitische Maßnahmen in Bereichen der Inflation und Stagnation. Aufgrund dessen plädieren einige Wirtschaftswissenschaftler wie Rogoff oder Buiter für eine Abschaffung des Bargelds. Dies hätte zur Folge, dass negative Zinsen auf digitalem Geld erhoben werden könnten, ohne eine Geldflucht auszulösen, da dies bei elektronischem Geld nicht mehr möglich wäre. Ziel ist es dabei, die Menschen zu zwingen, ihr Vermögen zu investieren und daraus folgend ein Wirtschaftswachstum zu erzielen (Letzgas 2017:72). Ziel der Zentralbanken ist u.a., die Inflation aufrecht zu erhalten. Beim Bestehen einer bargeldlosen Gesellschaft wäre die Überlegung, Zinsen zu senken bei Gefahr einer Rezession obsolet. Die Negativzinspolitik würde es ermöglichen, entweder niedrige oder hohe Inflationsraten anzustreben. Rogoff sieht diesen Fakt als sehr vorteilhaft für die Geldpolitik der Zentralbanken an. Dadurch ließen sich aus seiner Sicht beim Anstreben einer niedrigen Inflationsrate Relativpreisverzerrungen verhindern, welche i.d.R. bei Preisstaffelungen oder bei Festsetzungen von Löhnen eintreten (Rogoff 2016:140). Um dies erreichen zu können, plädiert Rogoff nicht unbedingt für eine sofortige Abschaffung des kompletten Bargeldbestandes. Bspw. könnten im ersten Schritt der Einzug aller großen Banknoten erfolgen. Ausgenommen davon wären lediglich die 5 \$ oder 10 \$ Banknoten. In einem weiteren Schritt würden diese ebenso abgeschafft und bspw. durch Münzen kleineren Wertes ersetzt werden. Um im Falle der Reduzierung auf 5 \$ und 10 \$ aber auch Hortungen von Münzen zu vermeiden, schlägt Rogoff vor, Barzahlungsobergrenzen einzuführen. Aus seiner Sicht hätte aber bereits die Beschränkung auf Banknoten kleineren Wertes zur Folge, dass die Kriminalität erschwert werde und die übermäßige Hortung von Bargeld verhindert werden könne, da die Kosten für eine Aufbewahrung oder Transport deutlich steigen würden. Weiterhin plädiert Rogoff für eine Gebühreneinführung für das Einzahlen hoher Bargeldbeträge. Die wichtigste Folge aus seiner Sicht stellt aber die Verhinderung der Hortung dar, da diese die Umgehung von Negativzinsen ermöglicht (Rogoff 2016:152). Hauptziel einer „deutlichen Negativzinspolitik“ (Rogoff 2016:232) sind nach Rogoff die Ankurbelung des Wirtschaftswachstums und das Beseitigen einer Deflation. Für ihn wäre damit eine bessere Finanzstabilität gegeben, da durch die Negativzinsen die Dauer einer „ultralockeren Geldpolitik“ (Rogoff 2016:232) deutlich verringert werden könnte. Dies hätte aus seiner Sicht eine wesentlich schnellere Erholung der Wirtschaft zur Folge (Rogoff 2016:232). Natürlich ist Rogoff auch bewusst, dass manche Menschen Negativzinsen für ethisch bedenklich halten. Andere hingegen befürchten Inflationen, welche durch eine Aufhebung der Nullzinsgrenze wesentlich niedriger ausfallen würde. In Bezug auf eine Entschuldung von Staaten sieht Rogoff in Negativzinsen eine Optionserweiterung neben bereits bestehenden Entschuldungsinstrumenten. Es müsse nur darauf geachtet werden, eine missbräuchliche Anwendung zu verhindern. Seiner Ansicht nach wäre dies die Zahlung eines geringen Preises im Gegensatz zur Erschaffung der Möglichkeit einer Nullzinsdurchbrechung bei auftretenden Rezessionen. Erst dann wäre eine Geldpolitik auch wirkungsvoll (Rogoff 2016:243). Wie bereits angeführt sieht Rogoff darin die Möglichkeit für die Zentralbanken die Geldpolitik für:

- (1) die Stabilisierung der Privatwirtschaft
- (2) die Kreditvergabe bei Finanzkrisen als letztinstanzlicher Kreditgeber und
- (3) die Entschuldung von Staaten zu nutzen.

Voraussetzung dafür ist eine Kontrollmöglichkeit von Währungen und Rechnungseinheiten von Privatverträgen (Rogoff 2016:268). Den Staaten wäre damit geholfen, schneller auf finanzielle Krisen reagieren zu können. Wie bereits geschildert, plädiert Rogoff beim Auftreten von Problemen bei der Bargeldabschaffung wie bspw. der Run auf Banken kleinere Schritte, wie bspw. Bankgebühren auf Einzahlungen höherer Beträge von Geschäftsbanken auf Zentralbankkonten, welche wiederum an die Bankkunden weitergereicht werden würden (Rogoff 2016:281). Am wir-

kungsvollsten wäre die Bargeldabschaffung in Koordination in allen Entwicklungsländern (Rogoff 2016:282). Buiter schlägt drei verschiedenen Methoden zur Durchbrechung der Nullzinsgrenze vor:

1. Abschaffung des Bargelds
2. Besteuerung von Bargeld
3. Sicherstellung, dass Bargeld nicht das „Numéraire“ (Standardgut) ist (Buiter 2009:9).

Er negiert keineswegs die Aussage, dass Menschen Ausweichmethoden für eine Wertaufbewahrung suchen würden, wenn die Zinsraten negativ sind. Zum einen ist dies auch gewollt, da die Beträge auf den Konten freigegeben und in andere Werte oder Verbrauchsgüter investiert werden würden. Auf keinen Fall jedoch würden Menschen bei einer der drei Methoden auf Bargeld ausweichen. Eine Ankurbelung des Verbrauchs würde erreicht werden, wenn die Menschen auf nicht haltbare Güter ausweichen. Bei dauerhaften Gütern, vorausgesetzt sie haben einen dauerhaft gleichbleibenden Wert im Gebrauch, würde der Preis im Geld um den Prozentsatz sinken, den der negative Nominalzinsatz in gleicher Periode hätte. Somit wäre auch keine dauerhafte Wertaufbewahrung gegeben. Den Banken entsteht dabei kein Verlust, sie könnten sogar Erlöse generieren. Es macht für Buiter keinen Unterschied, ob eine Bank einen Kredit zu einer Verzinsung von 8% vergibt, den sie selbst für 5% von der Zentralbank bezieht oder ob sie einen Kredit zu -2% Verzinsung vergibt, den sie zu einer Verzinsung von -5% von der Zentralbank bezieht. Entscheidend ist hier lediglich das Resultat der Differenz der Verzinsung des Kredits und der Verzinsung der Kapitalanlage. Auf die Frage, wie künftige Sparer bei einem Minuszins von ihrem Vermögen leben könnten, wenn sie dieses für die Altersvorsorge angelegt haben, schlägt Buiter erst einmal vor zu prüfen, was reale Zinsraten bedeuten. Im Falle einer starken Deflation wären die Sparer immer noch im Vorteil und sie können von ihrem Sparbetrag leben. Weiterhin bringt Buiter zum Ausdruck: „Falls das für manche ein Absturz in die Armut darstellen sollte und sich deshalb soziale Probleme zeigten, dann gehen Sie zu Ihrem Finanzamt oder dem für Soziales zuständigen Minister. Aber belästigen Sie damit nicht die Zentralbank.“ (Buiter 2009:9). Die Durchbrechung der Nullzinsgrenze wäre von Vorteil als geldpolitisches Instrument der Zentralbanken. Weiterhin bestünde nicht die Annahme, dass aufgrund einer Absenkung der Zinsraten unterhalb der Nullzinsgrenze eine Wirksamkeitsveränderung der geldpolitischen Politik zur Folge hätte. Schlimmer wäre der Fall, wenn die Zentralbank bei Erreichen der Nullzinsgrenze untätig bleiben würde. Alternative Maßnahmen zum Negativzins wären eventuell die Erhöhung der Geldmenge, Erleichterung von Krediten oder ein Aufweichen der Sicherheitserfordernisse bei Ausleihungen der Zentralbank. Diese Maßnahmen bewirken jedoch eine Gefährdung der Unabhängigkeit der Zentralbank. Daher „[...] verstehe [er] wirklich nicht, warum Zentralbanken die Optionen zur Entfernung der unteren Nullgrenze nicht aggressiv verfolgen.“ (Buiter 2009:9) (Buiter 2009:8 f.). Einlagen bei den Banken sind eine Form der Hortung von Geld. Das Problem von Bankeinlagen ist, dass im Falle einer Zahlungsunfähigkeit, Einlagen nicht ausgezahlt werden können und so die Kunden ihr angelegtes Geld verlieren. Bargeld hingegen birgt kein Ausfallrisiko, da es sich dabei um Geld der Zentralbanken handelt. Es bietet damit die Möglichkeit bei der Gefahr einer Bankeninsolvenz des Schutzes vor Ausfall, die Opportunitätskosten liegen dann im Zinsverlust zusätzlich zu einem gewissen Diebstahlrisiko. Der Fakt der Ausfallsicherheit beim Abholen von Geldbeträgen kann jedoch das Insolvenzrisiko einer Bank forcieren. Wie bereits mehrfach geschehen, kann es dadurch zu einem Bank-Run kommen, in dem die Kunden der Bank ihre Einlage in hohem Umfang der Bank entziehen, in der Befürchtung, die Bank könne aufgrund Illiquidität keine Gelder mehr auszahlen. Oftmals sind kleine finanzielle Krisen Auslöser für Bank-Runs. Dies wiederum kann zu einer Übertragung auf andere Anleger verschiedener weiterer Banken führen und so eine weltweite Finanzmarktdestabilisierung auslösen. Aber nicht nur Bargeld ist dieses Risiko inhärent, wie das Beispiel einer Krise von Northern Rock zeigte (Mai 2017: 5 f.). Das Vereinigte Königreich wurde im Jahr 2007 erstmalig mit einem Bankensturm konfrontiert. Northern Rock war ein kleines Finanzunternehmen, jedoch war es von hoher Bedeutung für Privatkunden und gleichzeitig wichtiger Geber von Hypotheken. Aufgrund von Unsicherheiten kam es hier zu einem Bankensturm. In den Nachrichten wurden Menschenmassen gezeigt, welche ihr Geld abheben wollten, um es so sichern zu können (Bruni/Llewellyn 2009:7). Infolge der Unsicherheiten kam es durch die Anleger zu Massenüberweisungen ihrer Einlagen auf andere Banken.

Dieses Geschehen verdeutlicht, dass das Risiko nicht nur bei Bargeld besteht, sondern ebenso bei Giralgeld. Eine Bargeldabschaffung würde nicht das Problem eines Bank-Runs beseitigen. Anleger könnten auch weiterhin ihr vorhandenes Vermögen durch Überweisungen auf andere Banken sichern und damit Finanzkrisen auslösen. Die Gefahr eines Bank-Run könnte nur verhindert werden, wenn Giralgeld durch ein Vollgeld* substituiert würde. Die Geldschöpfung läge dann ausschließlich bei Zentralbanken bei dem ausschließlichen Vorhandensein einer „Geldsorte“ (Mai 2017: 6). Dies setzt aber zwingend eine Umformung des gesamten Finanzsystems voraus (Mai 2017: 5 f.). In Bezug auf die Verhinderung der Zahlung von Negativzinsen wäre auch hier eine Verteilung höherer Vermögen auf mehrere Banken denkbar. Das korreliert mit dem Betrag, auf den die Zentralbank Negativverzinsung erhebt. Grundsätzlich wäre es aber dadurch möglich, der Negativzinspolitik auszuweichen. Thiele, Niepelt und Krüger argumentieren weiterhin, dass eine Bargeldabschaffung keineswegs die größte Ursache einer niedrigen Inflation, welches die Wachstumsschwäche ist, beseitigen könnte. Daher sollten politische Maßnahmen eher auf Konsolidierungen der Haushalte und auf Reformen in den Strukturen gerichtet sein (Thiele/Niepelt/Krüger 2015:3 f.). Insbesondere die Bargeldschaffung zum Zwecke der Negativzinspolitik stellt für Mai ein hohes Risiko dar. Zum einen würde es zu einem Verlust in das Vertrauen in die Öffentlichkeit als auch in die Euro-Währung führen. Weiterhin könnte als Ausweichmaßnahme das Umschichten in Privatwährungen, welche keiner Negativzinsen unterliegen, gewählt werden, um ihr Vermögen zu schützen. Einfache Privatwährungen wären bspw. Geschenkkarten, Bonuskarten oder digitale Währungen. Weiterhin wäre auch eine Umschichtung in Fremdwährungen möglich. Auch eine Anlage in illiquide Formen wie Immobilien wären denkbar, was jedoch zu einer Immobilienblase führen könnte. Je höher die Ausprägung eines Ausweichens auf Substitute einer Währung wären, umso geringer wären die geldpolitischen Einflussmöglichkeiten der Zentralbanken (Mai 2017:6 f.). Zu einer Senkung der Nullzinssätze ist es bereits 2014 und 2015 in Dänemark und in der Schweiz gekommen. Es konnten dabei keine erhöhten Abzüge von Vermögen festgestellt werden (Mai 2017:7). Jedoch gab es andere Folgen einhergehend mit der Negativzinspolitik. Kopenhagen ist in Dänemark die drittteuerste Stadt der Welt im Ranking des Forschungsinstituts der Economist Intelligence Unit (EIU). Die hohen Lebenshaltungskosten gelten im Übrigen nicht nur für Kopenhagen, sondern für ganz Dänemark. Grund dafür sind hohe Steuern, teure Lebensmittel und allen voran hohe Immobilienpreise. Inzwischen zeigen sich die Auswirkungen der Null- und Negativzinspolitik verbunden mit einer lockeren Kreditvergabepolitik deutlich. In einer Warnung des Internationalen Währungsfonds (IWF) hieß es, dass der Anstieg der Immobilienpreise und Zinsen für Darlehen dauerhaft zu einer Beeinträchtigung des Privatverbrauchs führen können und das zu einer wirtschaftlichen Instabilität führen könne. Nykredit, wichtigster Finanzier von Immobilien befürchtet, dass der Immobilienmarkt außer Kontrolle gerät und dabei die Gefahr besteht, dass die Kreditnehmer einen Zinsanstieg ausblenden. Festgestellt wurde, dass die Einwohner Dänemarks aufgrund der Negativzinsen immer weiter in die Verschuldung geraten, da sie immer höhere Kredite mit sehr kurzer Laufzeit aufnehmen. Diese haben zwar zur Folge, dass Menschen weniger Geld zurückzahlen müssen als sie aufgenommen haben, jedoch blenden sie die Gefahren einer Zinserhöhung aus. Inzwischen gilt Dänemark als das Land, in dem Immobilienfinanzierungen vorrangig über Kreditaufnahmen vorgenommen werden. Deutlich wird dies an den Immobilienpreisen im Land. Allein im Wohnungsmarkt war ein Zuwachs von 11% zu verzeichnen. In Teilen Kopenhagens lag der Zuwachs bereits bei 16% (Rentzsch 2017). Eine Studie der Schweizerischen Bankiervereinigung zu Auswirkungen der Negativzinspolitik in der Schweiz ergab im Jahr 2019 folgende Ergebnisse: Die negativen Zinsen bewirkten eine Vermögensumverteilung der Sparer von den Banken zum Export hin. Die Exportwirtschaft zieht daraus einen positiven Nutzen, Sparer hingegen bekommen keine Rendite mehr und bei den Banken hat es zu einer Verringerung der Marge bei Zinsen geführt. Die expansive Geldpolitik hat zur Folge, dass die Verbraucher der Schweiz aufgrund der Schwächung der internationalen Bonität die Kos-

* Die Theorie des Vollgeldes wurde von Henry Simons entwickelt und besagt, dass Geld nicht durch Gold gedeckt sein soll. Weiterhin soll es Banken nicht gestattet sein, neues Geld (Giralgeld) durch Schöpfung zu erschaffen. Lediglich das durch Sparenden zur Bank gebrachte Geld darf als Kredit wieder herausgegeben werden. Daraus entsteht eine „1:1 Einlagensicherung“ (Brodbeck 2014:41).

ten tragen müssen. Aus diesen Gründen lehnt die Schweizerische Bankiervereinigung eine Notwendigkeit eines Negativzinses ab (Gasser/Benz/Hess 2019:20). Eine weitere Gefahr besteht im Zusammenhang mit dem Negativzins. Sparer könnten ein gegenteiliges als erwünschtes Verhalten zeigen. Anstatt ihr Geld auszugeben, welches das Ziel einer Negativzinspolitik ist, könnten sie mehr sparen als zuvor. Conrads gibt außerdem zu bedenken, Negativzinsen wären keine verhältnismäßige Lösung für ein geringes Wirtschaftswachstum. Die Gründe für eine Wirtschaftswachstumsschwäche liegen seiner Meinung nach in überholten und veralteten Strukturen und in Mängeln der Wirtschaftspolitik, welche nur durch umfassende Reformen dauerhaft zu bewältigen wären. Weiterhin gibt er verfassungsrechtliche Schwierigkeiten bei einer Bargeldabschaffung zu bedenken, da Euro-Banknoten und Euro-Münzen in Europäischen Verträgen als gesetzliches Zahlungsmittel legitimiert sind. Darüber hinaus verlangt Conrads eine Abwägung zwischen der Beschränkung von Freiheitsrechten der Menschen und der Beschränkung von Barzahlungen (Conrads 2018:16).

5.3 Bargeld ist zeitaufwändig und kostenintensiv

Am Kreislauf des Bargelds in Deutschland nehmen fünf Parteien teil:

- Deutsche Bundesbank,
- Wertdienstleister (e.g. WTU),
- Banken
- Konsumenten und
- Handel.

Die Deutsche Bundesbank übernimmt die Produktion und in Verbindung mit weiteren EU-Notenbanken Prüfungstätigkeiten und die Wiederherstellung (Recycling) des Bargelds. Die Wertdienstleister sichern die Versorgung zwischen der Bundesbank und den Geschäftsbanken mit Bargeld. Banken übernehmen die Versorgung und Bereitstellung für ihre Kunden - Handel und Konsumenten. Der Handel und auch die Konsumenten verwenden das Bargeld zur Zahlung oder nutzen es als Wertaufbewahrungsmittel. Dabei wechselt eine produzierte Banknote im Geldkreislauf ca. 150-mal seinen Besitzer. Innerhalb dieses Wechsels wird die Note von der Bundesbank durchschnittlich sechsmal einer Prüfung unterzogen. Bei dem Erwerb von Gütern oder Dienstleistungen findet sie im Durchschnitt bis zu 130-mal Verwendung. Zusätzlich wird sie ca. 15-mal bei C2C*-Geschäften verwendet (Kleine/Krautbauer/Weller 2013: 1 f.). Im Bargeldkreislauf entstehen dadurch ungleich hoch verteilte Kosten. Einige Beteiligte können Einnahmen erzielen, andere wiederum wie bspw. der Handel haben ausschließlich Kosten zu tragen (Abb. 15) (Kleine et al. 2013:4).

Abb. 15 Marktteilnehmer und anfallende Kostenkomponenten im Bargeldkreislauf in Deutschland

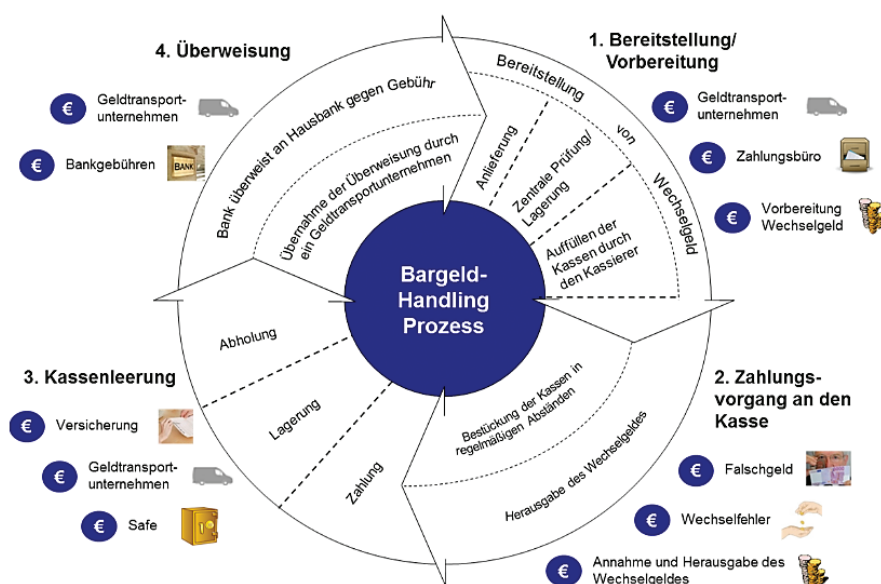


Quelle: Kleine et al. 2013:3

* C2C = Consumer to consumer, Geschäfte zwischen Verbrauchenden

Die Bundesbank generiert durch die Geldausgabe in Deutschland und im Ausland sogenannte Seigniorage-Einnahmen. Sie ist die einzige Institution, die keine Zinszahlungen leisten muss, da sie das Prägemonopol besitzt. Verrechnet werden die Seigniorage-Einnahmen mit den Herstellungskosten der Banknoten (Kleine et al. 2013:3). Wie bereits geschildert, versorgen die Geschäftsbanken die Endverbraucher und den Handel mit Bargeld. Dafür müssen sie das benötigte Geld zum Nennwert bei der Zentralbank leihen oder einen anderen Gegenwert stellen. Die Bundesbank erzielt Zinseinnahmen durch die Verleihung oder generiert aus den von den Geschäftsbanken verkauften Vermögenswerten Gewinne. Diese Einnahmen werden unter Seigniorage-Einnahmen verstanden (Europäische Zentralbank 2017). Ein anderer Begriff dafür ist Geldschöpfungsgewinn. Die Werttransportunternehmen (WTU) verlangen für ihre Dienstleistungen Gebühren, um die fixen und variablen Kosten decken zu können. Diese sind u.a. Kosten des Transports, Löhne, Gehälter, Gebäudekosten oder Versicherungskosten. Banken entstehen Kosten für das Bargeldhandling wie bspw. Ein- und Auszahlungen. Zusätzlich verlieren sie Zinseinnahmen, da sie das Geld für die weitere Verwendung vorhalten müssen. Weiterhin müssen Banken die Gebühren für Versorgung und Versicherung tragen. Einnahmen erzielen die Banken bspw. mit Kontoführungsgebühren und verrechnen diese mit ihrem Aufwand. Beim Handel ist es vom Aufwand ähnlich wie bei den Banken mit dem Unterschied, dass der Handel auf die Bezahlung mit Bargeld keine Gebühren erheben kann. Somit kann er auch keine Einnahmen aus dem Bargeld generieren. Die fünfte Partei, die Verbraucher, ziehen Vorteile aus der Anonymität der Barzahlungen. Ihnen entstehen Opportunitätskosten in Form von Zinsverlusten und tragen die Beschaffungskosten (Kleine et al. 2013:3 f.). Die gesamten Kosten des Bargeldkreislaufs belaufen sich auf über 8 Mrd. Euro für die Volkswirtschaft. Für die Verbraucher und die private Wirtschaft sind diese noch höher. Hier sind zusätzlich die Transferzahlungen zu berücksichtigen, so dass insgesamt ein Zinsverlust i.H.v. 12 Mrd. Euro entsteht. Die Deutsche Bundesbank, einziger Profiteur des Barkreislaufs, erzielte allein in 2011 4 Mrd. Euro. Annähernd 1,9 Mrd. Euro davon konnten im Ausland generiert werden. Verrechnet mit den Herstellungskosten und Recyclingaufwand i.H.v. 250 Mio. Euro ließ sich ein volkswirtschaftlicher Gesamtgewinn i.H.v. 1,7 Mrd. Euro erzielen. Geschäftsbanken hingegen erzielen nicht genügend Einnahmen, um die Kosten für das Handling mit Bargeld decken zu können. Durch fehlende Automatisierung von Prüfprozessen, welche zu 80% händisch durchgeführt werden, entstehen privatwirtschaftliche Kosten i.H.v. annähernd 4 Mrd. Euro per anno. Die Seigniorage unberücksichtigt, belaufen sich die volkswirtschaftlichen Kosten, ebenso auf ca. 4 Mrd. Euro per anno. Für den Handel entstehen ebenso hohe Kosten. Diese setzen sich aus vielen verschiedenen Kosten zusammen, wie Abb. 16 darstellt (Kleine et al. 2013:5 ff.).

Abb. 16 Beispielhafter Bargeld-Handling Prozess im Handel



Quelle: Kleine et al. 2013:7

Allein für die Kassentätigkeiten und Prozesse im BackOffice entstehen Kosten i.H.v. ca. 5,7 Mrd. Euro. Zusätzlich entstehen Kosten durch das Falschgeldhandling und Aufwendung für Sicherungsmaßnahmen, so dass Gesamtkosten von ca. 6,7 Mrd. Euro festzuhalten sind. Den Verbrauchern entstehen Kosten i.H.v. 1,3 Mrd. Euro per anno. Diese setzen sich aus Zinsverlusten bspw. durch Horten der Gelder sowie die noch höheren Transaktionskosten zusammen (Kleine et al. 2013:8). Bei allen bisher aufgezählten Kosten müssen zusätzlich noch die gesellschaftlichen Kosten Berücksichtigung finden. Diese entstehen bei illegalen Geschäften in der Schattenwirtschaft wie Schwarzarbeit und Glücksspiel (Kleine et al. 2013:7). Kleine kommt aufgrund seiner Berechnungen zu dem Schluss, dass Barzahlung nicht die kostengünstigste Zahlungsmethode ist, denn verglichen mit den Gesamtkosten des Kartenzahlungsverkehrs i.H.v. 800 Mio. Euro liegen diese erheblich darüber. Aber auch aus Sicht der geringeren Transaktionszahlen bei Kartenzahlungen sind diese deutlich geringer. Kleine schließt daraus, dass Bargeld lediglich bis zu einem Betrag von ca. sechs Euro geringere Kosten als Kartenzahlungen verursachen würde. Daher plädiert er grundsätzlich für Kartenzahlungen (Kleine et al. 2013:9). Er schlägt folgende Maßnahmen vor, um Anreize für die Erhöhungen von Kartenzahlungen zu erzielen:

- „Einführung von spezifischen Transaktionsgebühren, um Anreize zu schaffen, das wirtschaftlichste Zahlungsinstrument auszuwählen
- Implementierung von Gebühren für Ein- und Auszahlungen von Bargeld an Automaten sowie am Bankschalter, um die Verwendung von Bargeld mit augenscheinlich sichtbaren Kosten zu versehen
- Einführung von gesetzlichen Höchstgrenzen für Bargeldtransaktionsvolumen wie beispielsweise in Italien (>1.000 Euro) oder Griechenland (>1.500 Euro)
- Verbot/ Einschränkung der Barzahlung von Handwerksdienstleistungen zu Gunsten von Kartenzahlungen
- Verbot/ Einschränkung von Barzahlungen für Zigaretten- und andere bargeldbasierte Automaten“ (Kleine et al. 2013:12 f.).

Notwendig wären diese Schritte, um Zahlungen mit Bargeld weiter zu verringern (Kleine et al. 2013:12 f.). Krüger und Seitz kritisieren die Studie von Kleine et al., da sich diese nur auf Interviews mit Experten bezieht. Weiterhin sind sie der Auffassung, dass essenzielle Faktoren keine Berücksichtigung finden, welche vorteilhaft durch die Zahlung mit Bargeld sind. Das sind bspw. die Fragen zum Datenschutz und Anonymität, Schutz der Privatsphäre bei Barzahlungen und Diebstahl der Identität bei Kartenzahlungen. Weiterhin stellt Bargeld ein wichtiges Instrument der Liquidität in Krisenzeiten dar. Das ist bspw. dann der Fall, wenn unbare Zahlungen aufgrund eines Ausfalls der Technik nicht mehr möglich sind. Zusätzlich liegt bei vielen Studien zur Kostenermittlung eine Verzerrung der Ergebnisse vor, da lediglich Banken und Händlern an Umfragen teilnehmen und deren Antworten nicht tiefgründiger untersucht werden. Bei Umfragen unter Verbrauchern wird oftmals das Design und dessen Beeinflussung nicht berücksichtigt (Krüger/Seitz 2014:68). Mai ist der Meinung, dass bisher keine fundierte Aussage über die volkswirtschaftlichen Gesamtkosten der Zahlungssysteme getroffen wurde. Oftmals enthalten viele Studien lediglich geschätzte Kostenwerte, welche den Beteiligten bei der Verwendung unterschiedlicher Zahlungsmethoden entstehen. Weiterhin bestehen zwischen den Studien Differenzen in Bezug auf das gewählte Land, nach Ansatz, nach der Verfügbarkeit der Daten oder der Durchschnittsgröße der Transaktionen. Weiterhin gibt Mai zu bedenken, dass unbare und bare Zahlungen jeweils eigene Strukturen aufweisen und beide Zahlungsmethoden der Stückkostendegression unterworfen sind. Folglich werden durch die Höhe des verwendeten Bargeldbetrages die Stückkosten sowohl für Barzahlungen als auch für unbare Zahlungsmethoden stark beeinflusst (Mai 2017:16 f.). Cabinakova, Knümann und Horst kommen in ihren Berechnungen zu anderen Ergebnissen als Kleine, Krautbauer und Weller. Gemessen an der Dauer eines Zahlvorgangs benötigt eine Barzahlung durchschnittlich 22,3 Sekunden. Kartenzahlungen mit PIN-Eingabe hingegen benötigen 29,3 und mit Unterschrift 38,3 Sekunden laut ihrer Studie am Point of Sale (POS). Abhängig ist es zusätzlich von der Höhe des zu leistenden Betrages. Je größer dieser ist, umso länger dauert der Bezahlvorgang. Ausgenommen hiervon ist die Kartenzahlung mit Unterschrift. Bei Barzahlungsvorgängen mit Bargeld ermittelten sie für einen Betrag geringer als 10 €

einen Wert von unter 18 Sekunden, mit steigendem Betrag wie bspw. 50 oder 100 € bereits 32 Sekunden und mehr. Weiterhin spielt das Alter des Zahlenden eine erhebliche Rolle. Je höher das Alter, umso höher ist die Zeit des Bezahlvorgangs. Dies gilt jedoch für jede Form von Zahlungsmittel. Bezugnehmend auf Transaktionen sind Barzahlungen am effizientesten für den Handel. Pro Transaktion fallen hier Kosten von 0,24 € an. Die Zahlung per Girocard liegt nur knapp darüber. Am kostenintensivsten sind Kreditkartenzahlungen aufgrund ihrer hohen Transaktionskosten. Bezogen auf den Umsatz ist die Girocard-Zahlung am kostengünstigsten für den Handel. Die Gesamtkosten aller Zahlungsmethoden für den Handel belaufen sich auf 5.432 Mio. Euro. Darauf entfallen für Barzahlungen ca. 3.775 Millionen Euro. Die Differenz wird von Kartenzahlungen (Girocard, Lastschrift und Kreditkarte) verursacht. Nicht berücksichtigt wird der Umsatz i.H.v. 13 Milliarden Euro durch Kauf auf Rechnung oder Gutscheinen und 6 Mrd. € durch andere als die bereits aufgeführten Kartenzahlungen wie bspw. mit Maestro-Karten sowie deren Kosten i.H.v. 344 Mio. €. Zusammengefasst ergibt sich eine Gesamtsumme von 5,7 Mrd. €, die einem Gesamtumsatz i.H.v. 410 Mrd. € gegenübersteht (Cabinakova/Knümann/Horst 2019:104 ff.). Bei ihren Berechnungen kommen Cabinakova et al. zu dem Schluss, dass insbesondere bei der Zahlung von kleinen Beträgen Barzahlungen aufgrund geringer Fixkosten von Vorteil sind. Etwas höher liegt hier der Anteil der variablen Kosten verglichen mit Zahlungen via Girocard und elektronischen Lastschriftverfahren (ELV), aber weit unter denen für die Zahlung via Kreditkarte. Bis zu einem Betrag von ca. 20 € ist aus ihrer Sicht die Zahlung mit Bargeld am kostengünstigsten, ab einem Betrag darüber die Zahlung mit Girocard. Zusammenfassend betrachtet sind die Zahlungen per Girocard und ELV kostenintensiver als die Barzahlung bis zu einer Summe von ca. 50 Euro. Werden die Kosten für den Zeitaufwand ausgeklammert, stellen Barzahlungen die kostengünstigste Zahlungsmethode dar, jedoch ist grundsätzlich eine Mischung aus allen genannten Zahlungsarten am vorteilhaftesten für den Handel. Nicht berücksichtigt in der Studie wurden die Kontaktloszahlungen (Cabinakova et al. 2019:107 f.).

5.4 Der Großteil des Bargelds ist für kriminelle Zwecke im Umlauf

Rogoff geht davon aus, dass der Großteil der sich im Umlauf befindlichen Banknoten für nicht legale Zwecke verwendet wird. Dabei schätzt er, dass bevorzugt in Unternehmen dank eines Cash-Managements nur wenig Bargeld verwendet wird. In Einzelhandelsgeschäften bspw. ergab der Anteil des Bargelds laut einer Studie aus den 90er Jahren unter 2% der gesamten Bargeldmenge. Davon ausgehend besteht die Vermutung, dass in Bezug auf die zunehmenden Kartenzahlungen die Barzahlungen bis dato noch wesentlich mehr abgenommen haben. Auch die hinzugerechneten Bargeldbeträge in Geldautomaten und Tresoren würden nicht die hohe Umlaufmenge des Bargelds erklären (Rogoff 2016:68). Weiterhin bezieht sich Rogoff auf eine EZB-Studie aus dem Jahr 2008, welche die Bargeldverwendung und den Bargeldbesitz untersuchte. Diese ergab, dass lediglich 57% der befragten Teilnehmer Bargeld für kleinere Transaktionen bei sich hätten. Unter 3% der Befragten hielten Bargeld von 1.000-5.000 € vor und gerade einmal ein halbes Prozent hatte Beträge von 10.000 € als Barvermögen. Die Studie lieferte aus seiner Sicht keine Erklärung für die um Umlauf befindlichen großen Banknoten im Wert von 200 € und 500 €. Eine weitere Studie zur Verwendung von Bargeld führte die EZB unter Unternehmen durch. Beide Studien zusammengefasst ergaben, dass lediglich 100 Milliarden Euro von den gesamten 750 Milliarden Euro im Umlauf befindlichen Banknoten den Verbrauchern und Unternehmen zugerechnet werden konnten. Weiterhin ergaben die Studien, dass sich der Großteil der hohen Banknoten nicht im europäischen Inland befand. Daher wurde die Vermutung angestellt, diese befänden sich nicht innerhalb des legalen steuerrechtlichen Wirtschaftskreislauf. Aus Rogoffs Sicht sind aufgrund der technischen Fortschritte alternativer Zahlungsmethoden hohe Banknoten unzeitgemäß und „vermutlich etwas viel Schlimmeres“ (Rogoff 2016:72 f.). Nachfragebedarf besteht nach wie vor für Banknoten geringeren Werts im Handel, jedoch findet nach Rogoffs Meinung der größte Teil des Bargelds nicht in der legalen Wirtschaft Verwendung (Rogoff 2016:79). Daher steht für Rogoff fest, „[...] dass Bargeld eine wesentliche Rolle bei einer großen Bandbreite krimineller Aktivitäten spielt, darunter Drogenhandel, organisierte Kriminalität, Erpressung, Behördenkorruption, Menschenhandel und natürlich Geldwäsche.“ (Rogoff 2016:11). Aufgrund einer Studie, durchgeführt von Ecorys und dem Centre for European Policy Studies (CEPS), kommt die Europäische Kommission zu dem Schluss, dass Barzahlungsbeschränkungen die Finanzierung

des Terrorismus „[...] zwar nicht spürbar eindämmen“ (Europäische Kommission 2018:1), aber dennoch von Nutzen sein könnten. Die Studie bezog sich dabei auf die Zahlung hoher Barbeträge, welche nur einen geringen Anteil aller Barzahlungen haben (Europäische Kommission 2018:1 f.). Die Ergebnisse der Studie, auf die sich die Europäische Kommission berief, waren dabei folgende: In Bezug auf die Finanzierung von terroristischen Aktivitäten und auf etwaige Meldepflichten hätte eine Beschränkung von Barzahlungen keine erheblichen Auswirkungen. Zum einen sind die Summen zu gering und werden dadurch nicht durch definierte Schwellenwerte registriert. Zum anderen gehen diese bereits mit anderen illegalen Handlungen einher wie der Kauf von Waffen und unterliegen keiner Beeinträchtigung. Weiterhin sind manche Tätigkeiten nicht aufspürbar, da es sich um gewöhnliche Aktivitäten handelt wie die Vermietung eines Lkws. In Bezug auf Geldwäsche hingegen wird eine Barzahlungsbeschränkung oder Herabsetzen der Meldepflicht für die Zahlung mit Bargeldsummen befürwortet, da eine Transaktionsanonymität beseitigt wird. Weiterhin würden diese Wirkung zeigen, da es sich hier um bargeldgenerierende Straftaten handelt wie bspw. der Drogenhandel. Eine Beschränkung des Bargelds wäre bspw. auch bei dem Erwerb höherwertiger Güter wirkungsvoll. Weit effektiver wäre jedoch ein Barzahlungsverbot mit einer gleichzeitigen Meldepflicht für die Bekämpfung von Geldwäsche. In Bezug auf die Hinterziehung von Steuern hätten Beschränkungen des Bargelds einen bedingten Einfluss. Weiterhin hängen diese auch eher mit anderen Faktoren zusammen. Darüber hinaus unterliegen Steuerhinterziehungen, welche nicht auf Bargeld angewiesen sind, keiner Erfassung. Aus diesem Grund wird ein Verbot von Barzahlungen präferiert (De Groen/Busse/Zarra 2017:132 ff.) Im Folgenden werden einzelne Delikte der Kriminalität in Bezug auf die Verwendung mit Bargeld näher untersucht.

5.4.1 Schattenwirtschaft

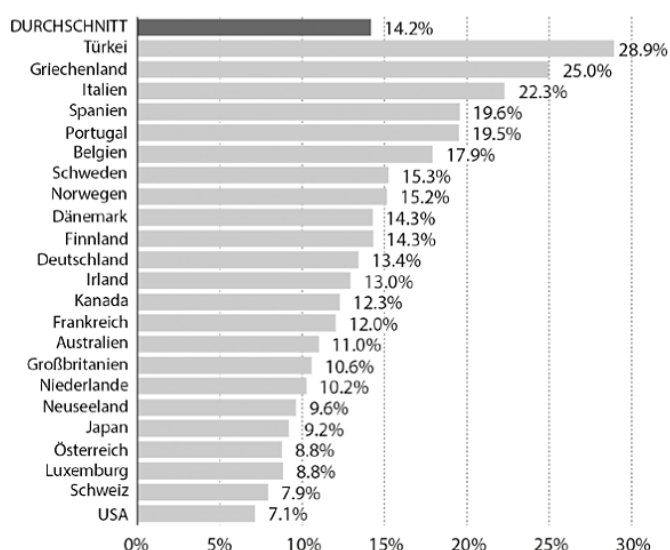
Schattenwirtschaft kann sich sowohl auf legale als auch illegale Aktivitäten beziehen. Legale sind bspw. alle Aktivitäten, welche nicht aufgezeichnet werden, um damit einen finanziellen Vorteil zu erzielen, welcher aus nicht gezahlten Steuerverpflichtungen oder Sozialversicherungspflichten generiert wird wie bspw. Schwarzarbeit. Illegale Aktivitäten in Bezug auf Schattenwirtschaft sind bspw. Produktfälschungen, der Handel mit Drogen oder Betrugsdelikte (Mai 2018:134). Gemäß dem deutschen Schwarzarbeitsbekämpfungsgesetz handelt es sich u.a. um Fälle von Schwarzarbeit, wenn:

- Arbeitnehmer bei einem Arbeitgeber in Beschäftigung sind und steuer- bzw. sozialversicherungsrechtliche Pflichten nicht beachtet werden,
- Sozialleistungsbezieher von Arbeitslosengeld I oder II ohne Mitteilung an den Leistungsträger eine Tätigkeit aufnehmen,
- ein Gewerbe ausgeübt wird, ohne die erforderliche Gewerbeerlaubnis zu besitzen oder
- die Ausübung eines Handwerks vorgenommen wird, ohne eine vorgeschriebene Eintragung in die jeweilige Handwerksrolle zu besitzen.

Die bei der Ausführung der Tätigkeit benutzten Güter und Materialien zählen zu der Schattenwirtschaft und müssen bei der Ermittlung der Schwarzarbeit berücksichtigt werden (Enste 2019a:152). Unter dem Begriff der Schattenwirtschaft verstehen Boumans und Schneider „[...] alle wirtschaftlichen Aktivitäten, die vor amtlichen Behörden aus monetären, regulatorischen und institutionellen Gründen verborgen bleiben“ (Boumans/Schneider 2019:90). Finanzielle Gründe sind die Umgehung der Zahlungen von Sozialabgaben oder Steuern. Die Vermeidung bürokratischer staatlicher Regelungen sind unter regulatorischen Gründen zu verstehen, während institutionelle Gründe die Umgehung von Gesetzen zur Korruption und politischen Einrichtungen beinhalten sowie eine mangelhafte Rechtsstaatlichkeitsauffassung implizieren. Boumans und Schneider verstehen hier aber ausschließlich jegliche legalen Aktivitäten, welche bei ordnungsgemäßer Meldung im nationalen Bruttoinlandsprodukt (BIP) erfasst worden wären. Illegale und/oder kriminelle Tätigkeiten und Aktivitäten zählen ihrer Auffassung nach nicht zum Begriff der Schattenwirtschaft. Auch sonstige Haushaltsarbeiten oder das Heimwerken werden davon nicht erfasst (Boumans/Schneider 2019:90). Rogoff geht davon aus, dass der größte Anteil des Bargeldes und dessen Verwendung in der Schattenwirtschaft Menschen jeglicher Art betrifft. Vorrangig gehen

diese legalen Tätigkeiten nach, neigen jedoch dazu, durch das Entziehen aus Gesetzesvorschriften, das Nicht-Zahlen von Steuern oder das Vermeiden von Beschränkungen in der Tätigkeit, steuerliche Vorteile zu erzielen. Grundsätzlich handeln sie den Gesetzen entsprechend mit nur zeitweiliger Steuerhinterziehung. Aus seiner Sicht hilft das Bargeld dabei, da durch seine Verwendung die Möglichkeit einer Entdeckung wesentlich geringer ist. Durch Studien wurde nachgewiesen, dass diese Menschen von ihrem pflichtwidrigen Handeln wissen, jedoch gehen sie von einer gewissen Interpretationsspanne bei Gesetzen aus, deren Befolgungen sich nur schwer kontrollieren lassen (Rogoff 2016:81). Ausgehend von niedrigen Steuersätzen und einer Gewichtung auf die Einkommenssteuer in den USA, ist Rogoff der Auffassung, dass die Treue zu bestehenden Gesetzen und Regeln höher ist als im Großteil anderer entwickelter Länder. Den Umfang der Steuerhinterziehung in Europa zu erfassen ist im Gegensatz zu den USA schwer umzusetzen aufgrund der Verwendung von indirekten Verfahren für die Hochrechnungen sowie fehlender Veröffentlichungen von Ergebnissen zufällig durchgeführter Steuerprüfungen. Der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zufolge soll sich die Steuerhinterziehung bei der Mehrwertsteuer um 4-17% bewegen. Weitere Studien schätzen, dass das Ausmaß der Schattenwirtschaft in Europa höher ist als in den USA. Begründet wird dies durch höhere Steuersätze und komplexerer Gesetzesgestaltung im Vergleich zu den Vereinigten Staaten. Allerdings gibt es erhebliche Differenzen in den Schätzungen. Zum einen liegt ihnen ein hohes Maß an Unsicherheit inne. Weiterhin wird von den Statistikern der Regierungen eine hohe Fehlerquote bei den Einkommenserfassungen eingestanden. Daher ist es nicht verwunderlich, dass die Schätzungen teilweise sehr weit auseinander liegen. Es sind auch nur eingeschränkte Informationen zur Schattenwirtschaft verfügbar und laut Rogoff bedarf es für Schätzungen die Verwendung indirekter Verfahren. Ein weiterer Kritikpunkt ist die unterschiedliche Begriffsdefinition der Schattenwirtschaft in den Studien und Erhebungen. In einigen Erhebungen werden illegale Aktivitäten berücksichtigt, andere beziehen sich ausschließlich auf die Steuerhinterziehung legaler Aktivitäten. Nach Schneiders Methode, welche den Arbeitsmarkt und finanzielle Aspekte wie bspw. die Erwerbsquote berücksichtigt, liegt die durchschnittliche Quote bei 14,2% des offiziellen BIP (Abb. 17) (Rogoff 2016:84 f.). Nicht berücksichtigt wurden hier illegale und kriminelle Aktivitäten (Rogoff 2016:86).

Abb. 17 Schattenwirtschaft in Prozent des offiziellen BIP



Quelle: Schneider 2016, aktualisiert nach Schneider, Buehn und Montenegro 2010 in Rogoff 2016:86

Kritik an den Studien zur Schätzung der Schattenwirtschaft üben auch Schneider und Enste. Zum einen gibt es verschiedene Berechnungsmethoden zur Ermittlung des Umfangs der Schattenwirtschaft und zum anderen beziehen sie sich auf unterschiedliche Größen. Somit haben alle Verfahren jeweils ihre Probleme und führen daher zu Schätzungen, welche ungenau und unzuverlässig sind (App. 15) (Enste/Schneider 2007:284). Laut Deutschem Zoll, welcher zuständig ist für die

Ermittlung von Schwarzarbeit, entstand allein im Jahr 2018 ein Schaden i.H.v. 835 Millionen in Deutschland durch Schwarzarbeit (Abb. 18). Schwarzarbeit und Korruption sind zwar im Vergleich zu anderen Ländern vergleichsweise gering, dennoch bewirken sie aber Einbußen im Umsatz i.H.v. bis zu 30 Prozent (Enste 2019b:1 f.).

Abb. 18 Jahresergebnisse Schwarzarbeit (gekürzt)

Sachverhalte	2016	2017	2018	2019	2020
Schadenssumme der straf- und bußgeldrechtlichen Ermittlungen - in Mio. Euro -	812,7	967,3	834,8	755,4	816,5

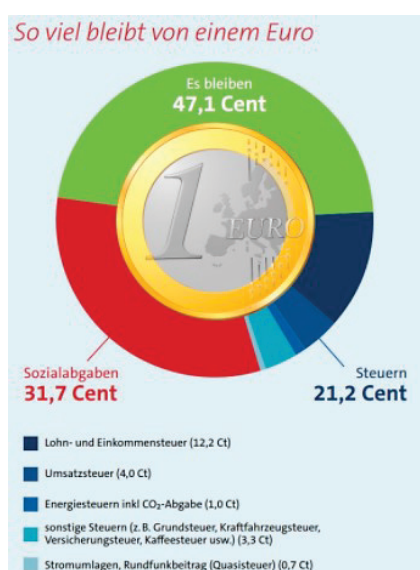
Quelle: Zoll Pressemitteilung, o.D., https://www.zoll.de/SharedDocs/Pressemitteilungen/DE/Jahresbilanzen/2021/z97_jahresstatistik_fks_2020_jahresergebnisse.html?nn=286846, abgerufen am 23.07.2021

Während der Corona-Pandemie nahm der Anteil der Schwarzarbeit um ca. 2% auf 11% gemessen am BIP zu. Im Wert entspricht dies einer Erhöhung i.H.v. 32 Milliarden Euro auf 348 Milliarden Euro. Begründet wird dies mit Einbußen im Einkommen durch Kurzarbeit und höherer verfügbarer Zeit. Schneiders Prognose von sinkender Schwarzarbeit von 9,2 auf 9,1% in Deutschland ist nicht eingetreten (fuldainfo 2020). Aber auch wenn die Verfahren zur Ermittlung der Schäden unterschiedlich sind, so ist es doch unstrittig, dass durch die Schattenwirtschaft Schäden i.H.v. Milliarden für den Staat und Sozialsysteme verursacht werden. Ein Rückgang der Schwarzarbeit bspw. würde sich daher positiv auf Sozialsysteme und Steuereinnahmen des Staates auswirken. Zweifel hegen Kleine, Krautbauer und Weller jedoch in der Wirksamkeit eines Bargeldverbotes. Sie gehen davon aus, dass dann künftig neben unbaren Zahlungsmitteln Substitute wie Gold oder Fremdwährungen Verwendung finden werden (Kleine/Krautbauer/Weller 2013:8 f.). In einer Studie untersuchte Schneider im Jahr 2017 die Korrelationen zwischen Bargeld und illegalen Handlungen. Dabei wurde untersucht, ob das Bargeld lediglich ein Instrument für die Schattenwirtschaft ist oder ob es eine treibende Kraft darstellt. Im ersten Ergebnis der ersten Teilstudie kommt Schneider zu dem Schluss, dass eine völlige Abschaffung des Bargelds eine Reduktion der Schattenwirtschaft von bis zu 20% zur Folge hätte (Schneider 2017a:7). In der zweiten Teilstudie wurde der Einfluss der Einführung einer Bargeldobergrenze auf die Schattenwirtschaft untersucht. Hier kommt Schneider zu dem Ergebnis, dass eine Bargeldobergrenze keine bedeutende Auswirkung auf die Größe dieser hat. Andere Faktoren wie bspw. die Rechtsstaatlichkeit, Steuerbelastung und Inflation hingegen haben einen sehr hohen Einfluss auf die Schattenwirtschaft. In der dritten Teilstudie wurde durch Schneider eine Befragung unter 1.056 Teilnehmern durchgeführt. In der Umfrage sollte u.a. eruiert werden, inwiefern eine Bargeldbeschränkung oder ein Bargeldverbot Auswirkungen auf die Schattenwirtschaft haben könnte. Unter den Teilnehmern wurden dabei jene ausgewählt, welche aus Anonymitätsgründen bisher Bargeldzahlungen für Dienst- und Handwerksleistungen präferierten. Dabei stellte sich heraus, dass 33% künftig bargeldlos zahlen würden und 41% zukünftig Substitute wie Geschenke oder Gutscheine für die Bezahlung wählen würden. 13% würden die Leistungen ablehnen und lediglich 13% würden steuerkonform den Rechnungsbetrag entrichten. Im Gesamtergebnis der Studie kommt Schneider zu dem Ergebnis, dass Bargeld in der Schattenwirtschaft eine wichtige Funktion hat, sie jedoch nicht kausal für sie ist und nur einen eingeschränkten Einfluss auf die Schattenwirtschaft ausübt (Schneider 2017a:8). Michler sieht im Bargeld ebenfalls nicht die erstrangige Kausalität für die Größe der Schattenwirtschaft. Für Michler liegen diese in „unzureichenden ordnungspolitischen Rahmenbedingungen“ (Michler 2015:15) wie bspw. die hohe Steuerbelastung (Michler 2015:15). Boumans und Schneider stellen nach einer weltweiten Umfrage des ifo World Economic Survey (WES) im Jahr 2019 geeignete Politikmaßnahmen für die Bekämpfung der Schattenwirtschaft nach Meinung der WES-Autoritäten in einer Rangfolge fest:

1. „Verbesserung der Rechtsstaatlichkeit
2. Erzwingung elektronischer Zahlungsverfahren
3. häufiger durchgeführte steuerliche Prüfungen und höhere Strafen bei Steuerhinterziehung“ (Boumans/Schneider 2019:94).

Abgeschlagen davon mit lediglich 9,8% war das „Setzen von Höchstgrenzen für Bargeldzahlung“ (Boumans/Schneider 2019:94) und mit 16.1% die „geringere Regulierung von Arbeitsvorschriften“ (Boumans/Schneider 2019:94). Bei den vorher genannten Optionen wurde eine Zustimmung von 20% und mehr gemessen. Zweitmeiste Antwort innerhalb der Europäischen Union (EU) war „geringere Sozialversicherungskosten“ (Boumans/Schneider 2019:94). Auch gaben 24,1% in der EU das Senken von Steuern als geeignetes Mittel an (Boumans/Schneider 2019:94). Die Steuerbelastung und Abgaben zur Sozialversicherung der deutschen Durchschnittshaushalte beliefen sich im Jahr 2021 auf ca. 52,9%. Dies bedeutet, dass den Haushalten gerade einmal 47,1% ihres Einkommens zur freien Verfügung stand (Abb. 19). Der sogenannte „Steuerzahlergedenktag“ (Warneke 2021:1) fiel auf den 13.07.2021, d.h. deutsche Arbeitnehmer, zusammengesetzt aus Angestellten, Beamten und Arbeitern, haben bis zu diesem Tag ausschließlich für öffentliche Abgaben gewirtschaftet (Warneke 2021:5).

Abb. 19 So viel bleibt von einem Euro



Quelle: Bund der Steuerzahler e.V. (2021). <https://www.steuerzahler.de/steuerzahlergedenktag/?L=0>. abgerufen am 24.07.2021

Auf lange Sicht ist für Warneke daher das Senken der Steuern unter die 50% Grenze ein wichtiges politisches Ziel, um die Belastungen für die Haushalte zu reduzieren (Warneke 2021:5 ff.). Der Bund der Steuerzahler geht d'accord, befürchtet jedoch, dass die Steuerbelastung weiterhin steigen wird und damit Anreize von Erwerbstätigkeiten sinken (Bund der Steuerzahler e.V. 2021).

5.4.1.1 Fazit

Ob die Kriminalität durch eine Bargeldobergrenze oder im extremen Fall der völligen Abschaffung des Bargelds verringert werden kann, ist fraglich. Natürlich würde im ersten Moment eine Verringerung die Schattenwirtschaft beeinträchtigt und eventuell teilweise in legale Bereiche verlagert werden. Fakt ist jedoch, dass die Ursachen für die Schattenwirtschaft in hohen Steuern und Sozialabgaben zu suchen sind. Aus diesem Grund wird auch nach einer Abschaffung kein nennenswerter Rückgang der Schattenwirtschaft zu verzeichnen sein (Schneider 2017b:23 f.). Weiterhin zeigen Studien auf, dass nicht ausschließlich Bargeld in der Schattenwirtschaft Verwendung findet. Nicht legale Zahlungsmethoden im Internet und über das Darknet mit digitalen Währungen gewinnen immer mehr an Zulauf (Deutsche Bundesbank 2019:49). Ein weiterer Grund für eine Ablehnung der Abschaffung von Bargeld ist, dass es bis dato keinen empirischen Beweis gibt, wie erfolgreich diese sich faktisch auswirken würde (Deutsche Bundesbank 2019:59). Auch Noack und Philipper äußern Bedenken, da es keine wissenschaftlichen Belege dafür gibt, eine Abschaffung könne die Schattenwirtschaft bekämpfen. Stattdessen vermuten sie, dass es eine Zunahme der Cyberkriminalität bewirken würde, zumal bereits in der heutigen Zeit illegale Transaktionen digital in der Finanzwelt vorgenommen werden. Weiterhin vermuten sie, die Kosten der

Bekämpfung der digitalen Kriminalität und die Schäden durch Cyberkriminalität könnten weitaus höher sein. Darüber hinaus geben sie zu bedenken, dass Menschen sehr wohl durch Überfälle oder Falschgeld Bargeld verlieren können, aber die Wahrscheinlichkeit Opfer von cyberkriminellen Handlungen zu werden, weitaus höher liegen kann (Noack/Philipper 2016:13). Conrads bezweifelt ebenso eine Korrelation zwischen einer geringeren Bargeldverfügbarkeit und geringerer Kriminalität. Zahlungen für illegale Aktivitäten wären zudem bereits auf unbarem Wege möglich. Auch die Zahlungsmittel könnten geändert werden wie bspw. in Fremd- und Kryptowährungen oder Substitute wie Naturalien. Zu berücksichtigen ist ebenso, dass das private Guthaben aus Steuerhinterziehungen oder illegitim erwirtschaftetem Geld sich zum Großteil auf Konten in Steueroasen befindet. Daher bezweifelt Conrads eine Wirksamkeit einer Einschränkung oder Abschaffung des Bargelds (Conrads 2018:15). Die Bundesbank geht ebenso von einer ansteigenden Verlagerung krimineller Aktivitäten im Internet durch die Digitalisierung aus. Als Beispiel nennt sie den Drogenhandel über das Internet, welcher bereits im Jahr 2017 24% höher lag als im Vorjahr und damit insgesamt 5% aller im Internet erfassten Straftaten betrug. Eine Anonymität von illegalen Handlungen kann auch leicht über das bestehende Bankensystem mit Hilfe von Briefkastenfirmen gewährleistet werden (Deutsche Bundesbank 2019:48). Eine steigende Verlagerung der Kriminalität in die digitale Welt könnte bspw. in Schweden angenommen werden. Während in den letzten Jahren die unbaren Kartenzahlungen durchschnittlich um 7% stiegen, nahmen die Barzahlungen rapide ab. Gleichzeitig wurde eine starke Zunahme der Kartenbetrugsdelikte registriert (Abb. 20) (Mai 2017:13).

Abb. 20 Elektronischer Zahlungsverkehr und Kartenbetrug



Quelle: Mai 2017:14

Selbst Formen der Schwarzarbeit haben sich bereit im Internet etabliert. Das sogenannte Crowdsourcing beschreibt eine Mischung aus Ausschreibung und Outsourcing. Definiert werden sie als „[...] Tätigkeiten, die ursprünglich durch einzelne VertragspartnerInnen – in der Regel ArbeitnehmerInnen – erbracht wurden, in der Form ausgelagert (outgesourced) [werden], dass sie einer größeren Anzahl von Personen (der Crowd) über eine internetbasierte Plattform angeboten und von diesen dann abgearbeitet werden.“ (Risak 2016 Kapitel 2.1 zitiert nach Baumann/Hübscher/Klotz 2017:11 f.). Zwischen den beauftragenden Unternehmen und den Internetplattformen entsteht jedoch kein arbeitsvertragliches Verhältnis, da diese nur als Mittler fungieren. Die ‚Crowdworker‘ (Leimeister et al. 2016: 80 zitiert nach Baumann/Hübscher/Klotz

2017:12), welche die Aufträge über die Plattformen annehmen und abarbeiten sind meist Selbstständige. Baumann, Hübscher und Klotz sehen darin eine hervorragende Voraussetzung für eine völlig neue Form der Schwarzarbeit. Aus ihrer Sicht entsteht hier eine Mischung aus Schwarzarbeit und virtuellem Arbeiten, so dass sie den Begriff des virtuellen Schwarzarbeitens gebrauchen (Baumann/Hübscher/Klotz 2017:11 f.). Als Ursache für die Schwarzarbeit führen sie in Rückgriff auf die Studie von Popescu, Cristescu, Stanila et al. hohe Steuern und Sozialabgaben an. Aber auch niedrige Arbeitslöhne und fehlende behördliche Aufsicht bzw. Kontrolle sind weitere Gründe (Baumann/Hübscher/Klotz 2017:16) und somit deckungsgleich zur Schattenwirtschaft in Bezug auf Bargeld.

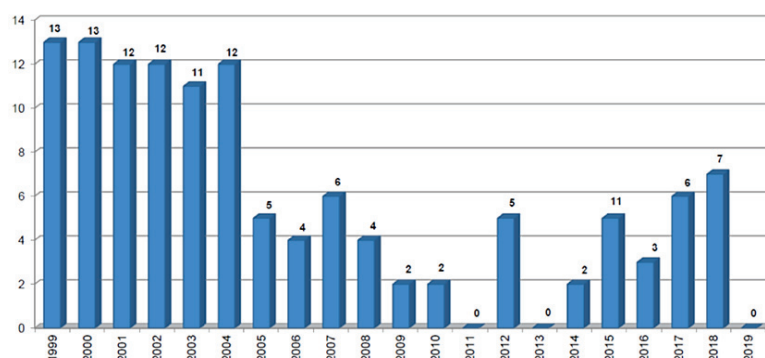
5.4.2 Raubüberfälle

In diesem Abschnitt soll überprüft werden, ob das Risiko von Überfällen sinkt, wenn sich der Bargeldumlauf verringert bzw. wenn das Bargeld abgeschafft würde. Dabei wird vorrangig auf Überfälle von WTU fokussiert. Hennies bspw. geht fest davon aus und darüber hinaus gäbe es eine Kostenreduktion in Bezug auf Präventivmaßnahmen und Zahlungen für entsprechende Versicherungen (Hennies 2016:4).

5.4.2.1 Vergleich der Sicherheitslage von Deutschland und Schweden

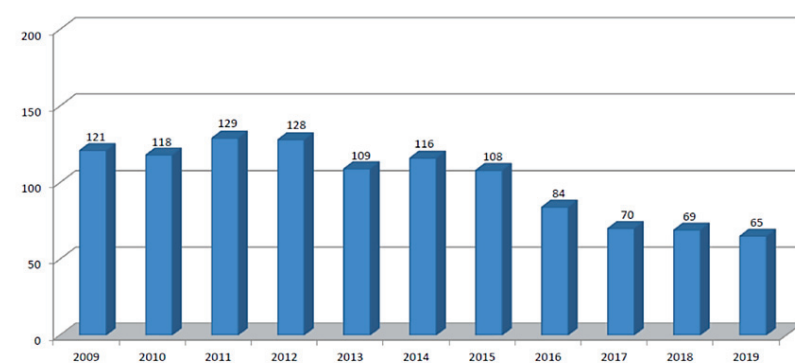
Laut der Bundesvereinigung Deutscher Geld- und Wertdienste (BDGW) kam es im Jahr 2018 zu sieben Raubüberfällen auf Spezialgeldtransportfahrzeuge. In den Vorjahren lag die Zahl der Überfälle bei sechs bzw. drei Raubüberfällen (Abb. 21). Die Überfälle auf Geldboten lagen im Jahr 2017 bei 70, im Jahr 2018 bei 69 und im Jahr 2019 bei 65. Insgesamt ist hier daher eine rückläufige Tendenz zu erkennen (Abb. 22). Abb. 23 zeigt weitere Überfalldelikte auf Tankstellen, Spielhallen und Geldinstitute (BDSW/BDGW/BDLS 2021:83 ff.).

Abb. 21 Raubüberfälle auf Spezialgeldtransportfahrzeuge



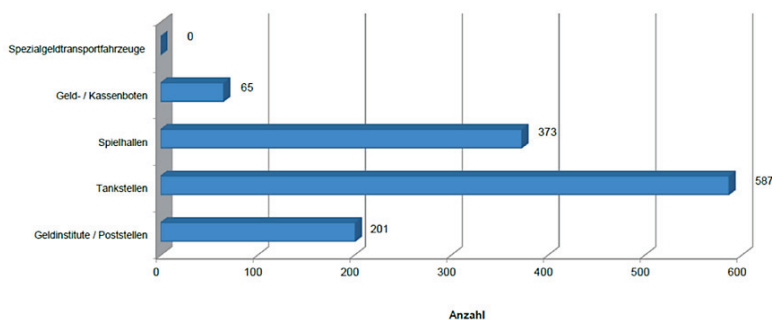
Quelle: BDSW/BDGW/BDLS 2021:83

Abb. 22 Überfälle auf Geldboten



Quelle: BDSW/BDGW/BDLS 2021:84

Abb. 23 Raubüberfälle 2019



Quelle: BDSW/BDGW/BDLS 2021:85

In den Jahren 2020 und 2021 begann eine Überfallserie auf Geldboten und Geldtransportspezialfahrzeuge in Berlin. Im Mai 2021 konnten bereits acht Überfälle mit steigender Brutalität der Täter damit allein in der Bundeshauptstadt verzeichnet werden, dargestellt in Tab. 6.

Tab. 6 Darstellung der Überfälle auf Geldboten und Geldtransportfahrzeuge in Berlin 2020/2021

Überfälle in chronologischer Reihenfolge	Tatwaffe
16.06.2020 Berliner Volksbank ¹	Reizgas
31.07.2020 Postbank-Filiale am Hermannplatz in Neukölln ¹	Reizgas
04.08.2020 Berliner Volksbank, Bundesplatz in Wilmersdorf ¹	Schusswaffen
15.12.2020 Ikea-Möbelhaus in Schöneberg ¹	Schusswaffen
17.12.2020 Park Center Treptow ¹	Reizgas
02.02.2021 Commerzbank Blissestraße in Wilmersdorf ¹	Schusswaffen
19.02.2021 Kurfürstendamm ²	Schusswaffen
26.05.2021 Bank in Neukölln in den Gropius-Passagen ³	Schusswaffen

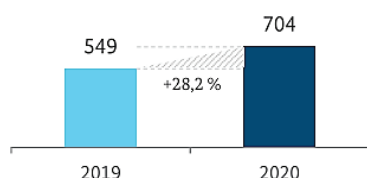
Quellen:

- (1) Berliner Zeitung (BZ), 19.02.2021, <https://www.bz-berlin.de/berlin/sieben-geldtransporter-ueberfaelle-in-acht-monaten-in-berlin>, abgerufen am 05.08.2021
- (2) Badische Neueste Nachrichten, 19.02.2021, <https://bnn.de/nachrichten/deutschland-und-welt/spektakulaerer-uberfall-auf-geldtransporter-in-berlin> abgerufen am 05.08.2021
- (3) Berliner Morgenpost, 26.05.2021, <https://www.morgenpost.de/berlin/article232378529/Raubueberfall-auf-Bank-in-Gropiusstadt-Zwei-Verletzte.html> abgerufen am 05.08.2021

Bei dem Überfall am 26.05.2021 wurde unmittelbar und direkt ohne vorangegangene Bedrohungshandlung eine Schusswaffe auf den Geldboten abgefeuert und stellt damit ein Novum im Anstieg der Brutalität dar. Es wurde die Vermutung aufgestellt, dass der starke Anstieg von Überfällen aufgrund fehlender Einnahmen aus Prostitution, Drogenhandel und Geldwäsche infolge der Corona-Krise, welche bei der organisierten Kriminalität für Einbußen gesorgt hat, zurückzuführen ist (Berliner Zeitung 19.02.2021). Auch im Bereich der physischen Angriffe auf Geldautomaten konnte ein Anstieg von 2019 zu 2020 in Höhe von 28,2% durch das Bundeskriminalamt (BKA) beziffert werden (Abb. 24). Darunter fallen Delikte:

- des Sprengens von Automaten,
- die sonstigen Öffnungen durch Werkzeug und
- durch Komplettdiebstahl (aus der Wand reißen) (BKA 2021a:5).

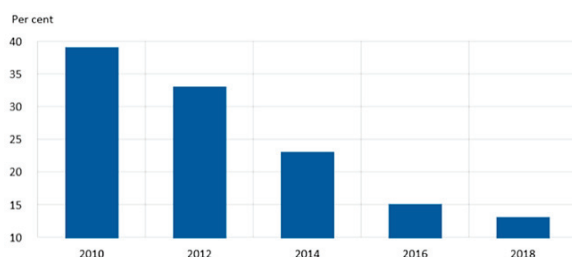
Abb. 24 Zahl der festgestellten Angriffe auf Geldautomaten



Quelle: BKA 2021a:5

In Schweden hingegen wird zunehmend bargeldlos bezahlt und Bargeld wird auch immer seltener als Zahlungsmittel akzeptiert. Bezogen auf physische Geschäfte lagen die Barzahlungen bei 13% im Jahr 2018 und verringerte sich damit um 26% im Vergleich zum Jahr 2010 (Abb. 25) (Sveriges Riksbank 2019:9).

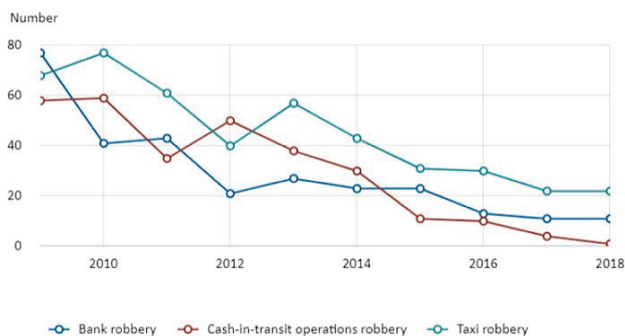
Abb. 25 Percentage who paid for their most recent purchase in cash



Quelle: Sveriges Riksbank 2019:9

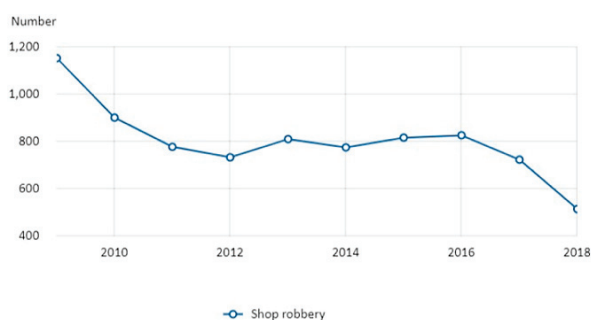
Die Zahl der Überfälle auf Banken, Geldtransporte und Taxen sank seit der verringerten Bargeldverwendung stark in der letzten Dekade (Abb. 26), bei Überfällen auf Geschäfte konnte sogar ein Rückgang von 50% verzeichnet werden (Abb. 27) (Sveriges Riksbank 2019:23 f.).

Abb. 26 Entwicklung der Überfälle auf Banken, Geldtransporte und Taxen in Schweden



Quelle: Sveriges Riksbank 2019:23

Abb. 27 Entwicklung der Überfälle auf Geschäfte in Schweden



Quelle: Sveriges Riksbank 2019:24

Mai stellt fest, dass hier eine Korrelation zwischen der Nutzung von bargeldlosen Zahlungsmitteln und einem Rückgang der Überfallzahlen festzustellen ist. Aus ihrer Sicht besteht demnach ein kausaler Zusammenhang zwischen dem Umlauf von Bargeld und Delikten, welche ausgeführt werden, um Bargeld zu rauben (Mai 2018:135). Auch für Meyer ist die Korrelation der rückläufigen Überfälle mit steigenden Kartenzahlungen eindeutig. Ein unerwünschter Effekt ist aus seiner Sicht der zunehmende Betrug mit Karten (Meyer 2020:131). Abschließend kann hier argu-

mentiert werden, dass ein verringerter Bargeldumlauf bzw. eine völlige Abschaffung des Bargelds die Kriminalität in Bezug auf Raubüberfälle von Geldtransporten, Geschäften, Banken und Taxen verringert werden kann, wenn sich diese auf die Erzielung von Bargeld richten.

5.4.3 Geldwäsche

Nach Nestler ist Geldwäsche „[...] ein Verhalten, das dazu dient Gelder oder Vermögenswerte (insbesondere größere Bargeldbeträge), die aus bestimmten (Katalog-)Straftaten stammen, durch bewusstes Vertuschen ihrer Herkunft in den legalen Wirtschaftskreislauf einzuschleusen.“ (Nestler 2017:349 f.). Gemäß § 261 Absatz 1 Strafgesetzbuch (StGB) liegt Geldwäsche vor, wenn jemand „[...] einen Gegenstand, der aus einer rechtswidrigen Tat herrührt,

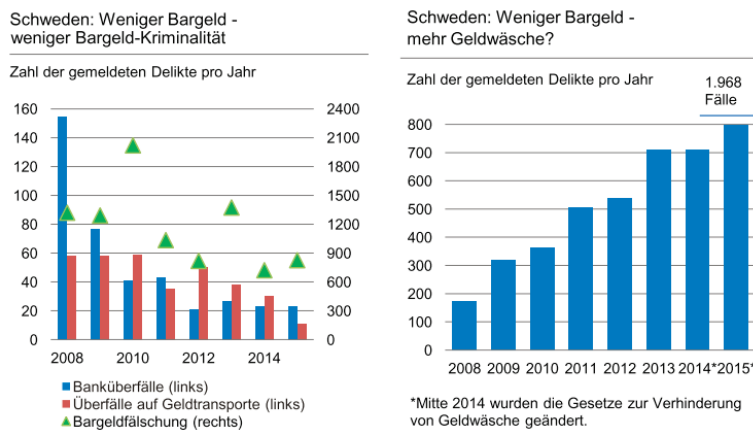
1. verbirgt,
2. in der Absicht, dessen Auffinden, dessen Einziehung oder die Ermittlung von dessen Herkunft zu vereiteln, umtauscht, überträgt oder verbringt,
3. sich oder einem Dritten verschafft oder
4. verwahrt oder für sich oder einen Dritten verwendet, wenn er dessen Herkunft zu dem Zeitpunkt gekannt hat, zu dem er ihn erlangt hat [...]“ (StGB § 261 Geldwäsche, https://www.gesetze-im-internet.de/stgb/_261.html, abgerufen am 05.08.2021)

Barzahlungen stellen aus Sicht des Bundesministeriums für Finanzen ein Risiko für Geldwäsche dar und folgt damit den Empfehlungen von Bussmann in seiner Dunkelfeldstudie, Barzahlungen auf Höchstbeträge zu begrenzen. Dieser Betrag soll sich im Maximum um einen mittleren vierstelligen Bereich bewegen (Bundesministerium der Finanzen (BMF) 2016:13). Geldwäsche stellt ein sogenanntes „Anschlussdelikt“ (Nestler 2017:349) dar, da ihr zuvor eine andere illegale Handlung vorangegangen ist. Daher besteht die strafbare Handlung aus zwei Delikten, die vorangegangene illegale Handlung und die darauffolgende Geldwäsche. Der größte Erfolg wird laut Nestler erreicht, wenn die deliktischen Handlungen in Bezug auf Raum und Zeit auseinanderfallen und ein Zusammenhang schwer herzustellen ist. Aufgrund dessen werden beide illegalen Handlungen oftmals in verschiedenen Staaten durchgeführt. Die Geldwäsche läuft dabei in mehreren Schritten ab. Ziel des Ganzen ist die Umwandlung des Bargeldes, welches durch illegale Aktivitäten erlangt wurde, in Buchgeld. Dies geschieht zumeist in kleinen aufgeteilten Beträgen und nicht selten im Ausland. Oftmals erfolgt hier bereits bei der Einzahlung eine Vermischung mit legalem Bargeld. Nach der Einzahlung erfolgt die Vornahme von verschiedenen Transaktionen in verschiedene Länder, um die Spur des Geldes zu verwischen. Die letzte Stufe ist die Rückführung des Geldes auf das Konto, von dem die Transaktionen vorgenommen wurden. Durch das wiederholte Versenden von Beträgen auf verschiedene Konten und zurück, lässt sich eine Nachverfolgung kaum noch bewerkstelligen und das Geld ist somit gewaschen (Nestler 2017:349 f.). In Deutschland wurde im Jahr 2019 eine Zunahme von annähernd 50% der Geldwäschefälle zum Vorjahr verzeichnet, während bereits im Jahr 2018 eine rückläufige Tendenz festgestellt werden konnte. Deutsche Staatsangehörige waren dabei in der Majorität, an zweiter Position befanden sich italienische Staatsangehörige. Die ansteigende Tendenz wurde vom BKA mit neu eingeleiteten Verfahren und den bereits laufenden Verfahren der vorigen Jahre begründet. Beispielsfälle waren dabei Ermittlungsverfahren wegen Geldwäscheverdachts durch den Handel mit Gold in den Jahren 2017 und 2018 bei gleichzeitig auftretendem Im- und Export von hohen Bargeldmengen. Weiterhin bestand der Verdacht, dass illegale Gelder über ein Netzwerk von in- und ausländischen Firmen gewaschen wurden. Der Geldbetrag belief sich dabei in 36 Fällen auf ca. 45 Millionen Euro durch Drogenhandel in den Niederlanden (BKA 2020a:50 f.). Aufgrund einer Studie im Jahr 2015 durch Bussmann, plante die Bundesregierung zu Beginn des Jahres 2016 die Einführung einer Bargeldobergrenze. Die Studie mit dem Titel „Dunkelfeldstudie über den Umfang der Geldwäsche in Deutschland und über die Geldwäscherisiken in einzelnen Wirtschaftssektoren“ war lediglich ein Teil der Analyse von Risiken im Rahmen der Umsetzung der vierten Geldwäscherichtlinie der EU. Insgesamt wurde bei dieser Studie festgestellt, dass der Umfang der Geldwäsche in Deutschland unterschätzt wird, und Bargeld prädestiniert für Schwarzgeschäfte sei (König 2016:5). Allein in den Jahren 2012/2013 wurden durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) jeweils annähernd 16.000 Verdachtsmeldungen registriert.

Diese stammten zum Großteil aus dem Finanz- bzw. Kreditbereich. Im Gegenzug wurden bei der Studie lediglich 250 Verdachtsfälle per anno aus dem nicht finanziellen Sektor festgestellt. Schätzungen innerhalb der Studie gehen jedoch von einer wesentlich höheren Anzahl von Verdachtsfällen im nicht finanziellen Sektor aus. So sollen die nicht gemeldeten bzw. nicht registrierten Fälle eher bei einer Anzahl von 15.000 - 28.000 liegen und damit einen ähnlichen Umfang wie im Finanzbereich haben. Weiterhin wird geschätzt, dass die Höhe der Verdachtsfälle eine Summe von 20-30 Milliarden Euro im nicht finanziellen Bereich beträgt. Laut Studie wird dieser Betrag jedoch deutlich unterschätzt. Zum einen führt Bussmann an, die zu den Meldungen Verpflichteten unterlägen einer mangelnden Auffassung und besäßen auch nicht die erforderliche Kompetenz, um die Kriterien eines Verdachtsfalles zu erkennen. Somit kommt es aus seiner Sicht schon dadurch zu fehlenden Meldungen. Zum anderen wurden in der Studie aus Gründen der Methodik lediglich ausgesuchte Gruppen des nicht finanziellen Bereiches befragt und damit andere Wirtschaftssektoren nicht betrachtet wie bspw. die Fusion von Unternehmen und Branchen der Dienstleistungen wie das Hotel- und Gaststättengewerbe. Aus diesen Gründen schätzt Bussmann, dass die Dunkelziffer der Geldwäsche weit höher liegen muss und sich damit auch weit über der Schätzung von 50 Milliarden Euro befindet. Er geht davon aus, dass der Betrag der Geldwäsche nahe 100 Milliarden per anno liegen muss, wie bereits in einer Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy (ECOLEF)-Studie im Jahr 2013 geschätzt wurde (Bussmann 2015:16). Eine der genannten Handlungsempfehlungen von Bussmann ist daher die Einführung einer Obergrenze von Barzahlungen. Diese sollte bei ca. 2.000-5.000€ liegen, um den Großteil der Verbrauchsgüter von dieser Regelung auszuschließen. Im gleichen Zuge fordert er präventive Maßnahmen beim Einzahlen höherer Barbeträge auf Ander- und Treuhandkonten (Bussmann 2015:24). Schneider sieht die Studie von Bussmann kritisch. Schon bei der Einschätzung der Entwicklung der Höhe von Geldwäschen macht er deutlich, dass der Begriff einer „starke[n] Zunahme“ (Schneider 2016:5) nicht näher definiert wurde, d.h., es wurden keine definierten Werte angegeben. Weiterhin wird bemängelt, dass ebenso der Ausgangspunkt, also die Basis für eine Annahme fehlt. Die Einschätzung können damit zwar qualitativ getroffen werden, eine quantitative Einschätzung versagt sich jedoch (Schneider 2016:5). Auch die Höhe der Schätzung von 30 Milliarden Euro im nicht finanziellen Sektor wird von Schneider kritisch gesehen. Dafür gäbe es keine begründende Analyse, sondern lediglich eine nicht unterlegte Behauptung. Die schlussendliche Verdopplung von 50 auf 100 Milliarden Euro mit der Berufung auf die ECOLEF-Studie ist nicht nachvollziehbar (Schneider 2016:9). Auch die von Bussmann angegebenen 20 Milliarden Euro im nicht finanziellen Sektor können aus Schneiders Sicht lediglich eine Höchstgrenze darstellen. Die weiteren Berechnungen stellen für Schneider allenfalls "[...] eine wissenschaftliche Spekulation dar". Auch wurde in der Studie von Bussmann nicht angegeben, ob sich die Geldwäsche auf Deutschland oder auf einen anderen EU-Raum bezieht (Schneider 2016:10). Schneider geht aufgrund seiner Berechnungen davon aus, dass die Aufstellungen bzw. Schätzungen von Bussmann wesentlich zu hoch sind. Dies belegen auch bereits andere Studien aus den Vorjahren wie Unger et al. (2013), United Nations Office on Drugs and Crime (UNODC) (2011), Smith (2011) und Schneider (2015). Bei ihren Berechnungen liegt der Betrag weit unter dem von Bussmann berechneten Geldwäschevolumen von 100 Milliarden Euro. Der Tatsache geschuldet, dass Bussmann nicht aufzeigt, ob sich dessen Studie auf die Geldwäsche in Deutschland bezieht, können die Handlungsempfehlungen der Einführung einer Barzahlungsobergrenze oder die komplette Versagung von Barzahlungen in bestimmten Bereichen objektiv nicht befürwortet werden. Auch aus Schneiders Sicht sind die illegalen Handlungen und der Betrug im Finanz- und Steuersektor problematisch geworden, aus denen eine hohe Geldmenge entsteht, welche gewaschen werden muss. Allerdings ist er der Meinung, dass vorrangig die illegalen Handlungen bekämpft werden müssten. Bei seinen Berechnungen kommt Schneider auf ein Volumen von 15-30 Milliarden Euro, wobei hier schon ein hoher Geldanteil von Scheinfirmen aus Europa inhärent ist (Schneider 2016:22). Eine Bargeldbeschränkung oder Bargeldabschaffung hält er nicht für wirkungsvoll, da die organisierte Kriminalität (OK) immer weniger auf Bargeld zurückgreift. Bargeld war besonders in 70er, 80er und partiell in den 90er Jahren von Bedeutung für die OK, als die Bargeldverwendung bei illegalen Handlungen in etwa bei zwei Dritteln aller Handlungen lag. Diese ist jedoch im Zuge der zunehmenden Digitalisierung und der

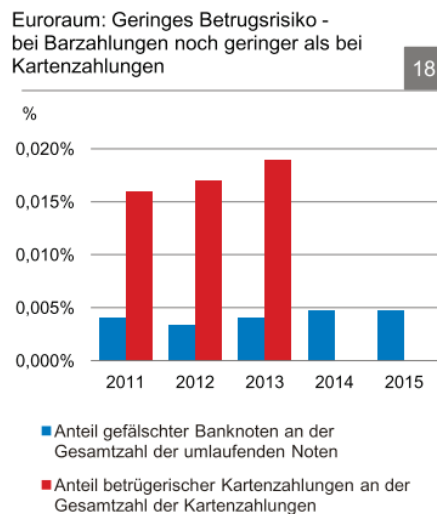
Verwendungsmöglichkeiten unbarer Zahlungsmöglichkeiten immer mehr gesunken. Transaktionen höheren Volumens werden inzwischen oft mit unbaren Zahlungsmöglichkeiten von der OK über Scheinfirmen getätigt, aber auch im Bereich der Transaktionen kleineren Volumens wird verstärkt auf die Zahlung via Bitcoin im Darknet festgestellt (Schneider 2016:23). In Schweden nahmen, wie bereits erwähnt, Barzahlungen stark ab. Erstaunlich ist jedoch, dass sich die Anzahl gemeldeter Fälle der Geldwäsche erhöht hat (Abb. 28). Zusätzlich wurde festgestellt, dass die Betrugsdelikte mit Karten in Europa höher lagen als die mit Bargeld (Abb. 29). Mai schließt daraus, dass Geldwäsche weder eine unmittelbare Korrelation zur Bargeldverfügbarkeit oder Bargeldnutzung hat noch das sie in Interdependenz zu ihr steht. Eine andere Möglichkeit ist, dass die aufgeführten Zahlen der Meldungen nicht die Realität wiedergeben. Zum einen geben die vorhandenen Zahlen keine Auskunft über die Höhe der gewaschenen Gelder aus und zum anderen könnte es auch an gesteigerten Kontrollen von Transaktionen liegen. Ein dritter Grund wäre hier eine Unterschätzung des realen Ausmaßes der Geldwäsche, da Dokumentationen verdächtiger Geldbewegungen fast ausschließlich von Banken und Zahlungsdienstleistern herrühren. In einer Minorität werden verdächtige Beträge aus Handelsgeschäften mit Kunst oder anderen wertvollen Gegenständen gemeldet (Mai 2017:13).

Abb. 28 Schweden Weniger Bargeld mehr Geldwäsche?



Quelle: Mai 2017:13

Abb. 29 Betrugsrisiko Bar- und Kartenzahlungen



Anmerkung: Die aktuellste Zahl für Betrug bei Kartenzahlungen bezieht sich auf das Jahr 2013. Kartenbetrug meint Betrug an der Ladenkasse, am Geldautomaten und online (ohne physischen Einsatz der Karte).

Quelle: Mai 2017:13

In einer Studie der Arbeitsgruppe zur Bekämpfung von Geldwäsche (Financial Action Task Force, FATF) wurde festgestellt, dass Geldwäschen oftmals über Ländergrenzen hinaus funktionieren und die Transporte des Bargelds zunehmen. Damit hebt die FATF die Bedeutung des Bargelds für illegale Aktivitäten hervor. Mai gibt jedoch zu bedenken, dass die Aufdeckung von Geldwäschedelikten eher auf die Aktivitäten mit Bargeld ausgerichtet sein könnten als auf Aktivitäten mit unbaren Zahlungsarten. Gemäß einer Europol-Studie wurden illegale Transporte von Bargeld am häufigsten in Flughafenzonen entdeckt. Mai erklärt sich diese Feststellung durch flächendeckende Kontrollen in den Flughäfen. Mittlerweile werden jedoch Innovativtechniken von der OK verwendet, ohne Bargeld nutzen zu müssen. Als Beispiel führt Mai das „Transaction Laundering“ (Mai 2018:137) bspw. über Online-Shops an, mit welchen sich illegale Aktivitäten als scheinbar legale Aktivitäten darstellen lassen. Hierbei wird z.B. ein Drogenkauf mit unbaren Zahlungsmitteln über eine Scheinfirma wie bspw. eine Online-Buchhandlung abgerechnet. Mai sieht darin eine einfallsreiche „[...] Kombination von Online-Handel, Regulierungslücken und verschiedenen innovativen und traditionellen Zahlungsarten über das Internet“ (Mai 2018:137). Es erschafft damit auch völlig neue und vielfältige Wege, illegales Geld über legale Scheinfirmen in das Zahlungsverkehrssystem zu verbringen. Trotz Versuchen von Behörden und Zahlungsdienstleistern, den Bereich dieser Transaktionen zu überwachen, liegt die Gefahr der Entdeckung weit unter der als bei bisherigen konventionellen Methoden mit Bargeld. Weiterhin ist Bargeld nicht mehr im Wege der digitalen Geldwäsche erforderlich, da die illegalen Beträge im bisher nicht oder schwer reguliertem oder nicht kontrollierbarem Raum Verwendung finden können. So ist es heute problemlos möglich, Güter und Dienstleistungen mit Kryptowährungen erwerben zu können. Eine Umwandlung der illegalen Beträge in eine Fiat Währung ist damit nicht mehr notwendig (Mai 2018:136 f.).

5.4.4 Korruption

Aufgrund seiner Anonymität und damit Nichtverfolgbarkeit ist aus Rogoffs Sicht das Bargeld prädestiniert für Korruption. Ein Verbot von großen Scheinen würde ein Ausweichen auf andere Zahlungsarten wie bspw. Bitcoins oder Gold bewirken, jedoch wären diese wesentlich leichter nachverfolgbar. Zudem sind sie illiquide und unterliegen hohen Kosten bei ihren Transaktionen (Rogoff 2016:99). Der Öffentlichkeit entstehen durch Korruption im öffentlichen Sektor hohe Kosten. Rogoff geht aufgrund Schätzungen davon aus, dass die Höhe der sozialen Kosten selbst anzunehmend größer sind als die Summen, welche bei der Bestechung verwendet werden (Rogoff 2016:95). Die Association of Certified Fraud Examiners (ACFE) untergliedert den Terminus Korruption im Fraud-Tree in vier unterschiedliche Kategorien (Abb. 30). Gemäß Transparency International handelt es sich um Korruption, wenn anvertraute Macht für privaten Nutzen missbraucht wird. Die Bestechung gibt es in verschiedenen Formen. Einerseits durch Zahlung und Entgegennahme von Geldern oder Surrogaten bei der Manipulation von Ausschreibungen oder durch Kick-backs (Anbieten von künftigen Rückzahlungen). Die Rückerlangung der Gelder erfolgt über verdeckte Provisionen (Stirnemann 2018:47).

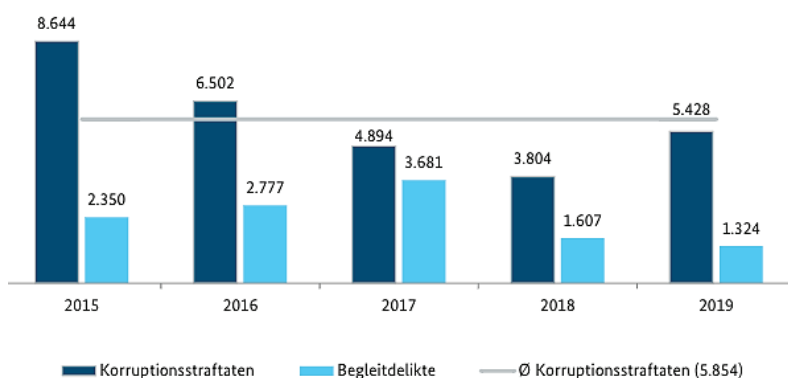
Abb. 30 Bestechung und Korruption



Quelle: Stirnemann 2018:45

In Deutschland wurden im Jahr 2019 5.428 Fälle von Korruption polizeilich erfasst (Abb. 31). Damit ist erstmals seit fünf Jahren ein Anstieg zu verzeichnen. Im Vergleich zum Jahr 2018 wurde ein Anstieg von 42,7% ersichtlich. Trotz dieser hohen Zunahme im Durchschnitt aller Fälle i.H.v. 5.854 innerhalb der letzten Jahre sank die durchschnittliche Anzahl der Fälle von Korruption innerhalb der letzten fünf Jahre. Der Anstieg wird damit begründet, dass in den Bundesländern der Umfang der Korruption unterschiedlich erfasst wird. Bspw. werden in manchen Bundesländern Straftaten der „Bestechung gem. § 334 StGB, besonders schwere Fälle der Bestechlichkeit und Bestechung gem. § 335 StGB“ und „die Bestechung und Bestechlichkeit im Gesundheitswesen gem. §§ 299a, 299b StGB“ erfasst, in anderen wiederum nur in geringerem Umfang (BKA 2020b:5).

Abb. 31 Anzahl der Korruptionsstraftaten 2019 - Fallentwicklung

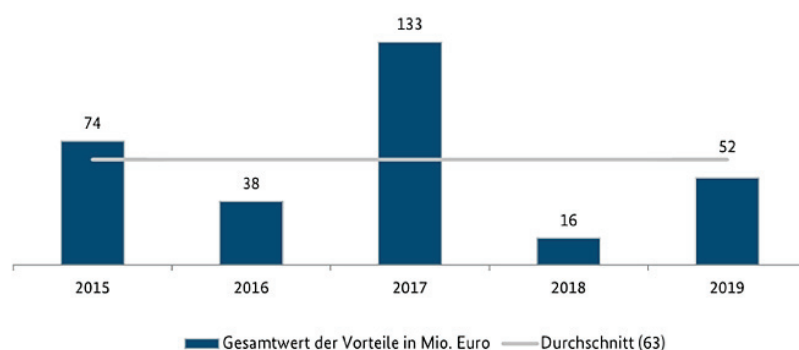


Quelle: BKA 2020b:5

Die Höhe der Vorteilsnahme lag im Jahr 2019 bei 52 Mio. Euro (Abb. 32) und verzeichnet damit einen Anstieg um 225% zum Jahr 2018. Der höhere Wert ergab sich aufgrund des Wertes außergewöhnlich finanziell verschaffter Vorteile in einzelnen Fällen.

Abb. 32 Gesamtwert der Vorteile (in Mio. Euro)

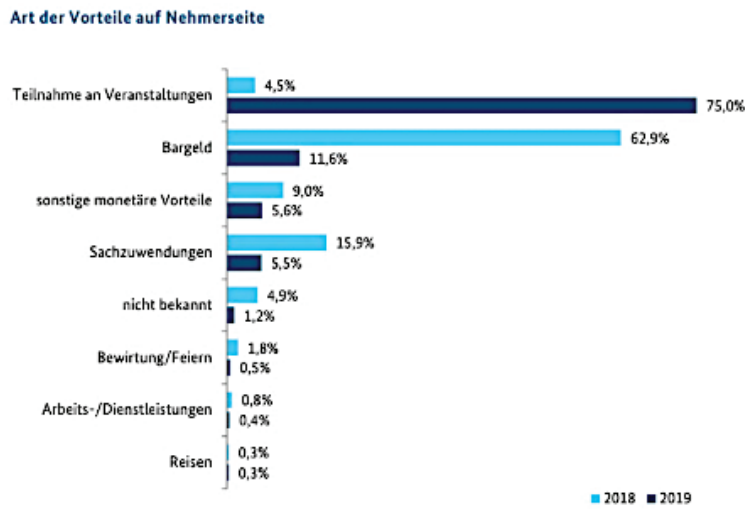
Gesamtwert der Vorteile auf Nehmerseite (in Mio. Euro)



Quelle: BKA (2020b:18)

Drei Viertel aller Korruptionsfälle fielen dabei auf die Vorteilsnahme der Veranstaltungsteilnahme (Abb. 33). Der Anstieg von 4,5% zum Jahr 2018 lag dabei an Verfahren in Hamburg, wo gegen die Vorteilsnahme in Verbindung mit der Vergabe von Örtlichkeiten für Veranstaltungen und der Veranstaltungsgestattung gegen Eintrittskartenübergabe an Kommunalverwaltungsangestellte ermittelt wurde. Weiterhin wurde festgestellt, dass dieser Anstieg zu einer stark rückläufigen Tendenz in der Vorteilsnahme von Bargeld führte. Dabei betrug der Rückgang 51% (2018: 62,9%, 2019: 11,6% - Abb. 33). Trotzdem ist das Bargeld aus Sicht des BKA weiterhin erheblich für die Korruptionsfälle (BKA 2020b:19).

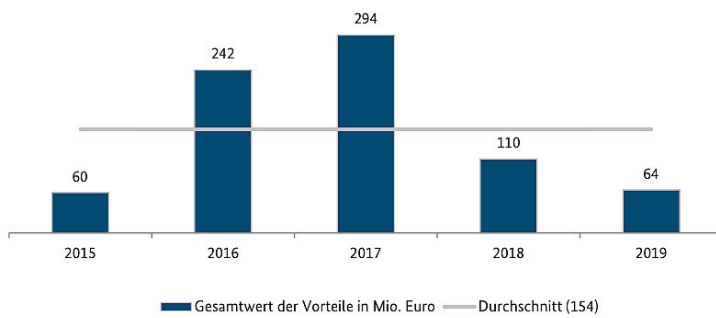
Abb. 33 Art der Vorteile auf Nehmerseite



Quelle: BKA 2020b:19

Auf der Vorteilsgeberseite ist hingegen ein rückläufiger Trend zu beobachten. Hier belief sich die Gesamtsumme auf 64 Mio. Euro und sank damit auf 41,8% (Abb. 34) (BKA 2020b:22).

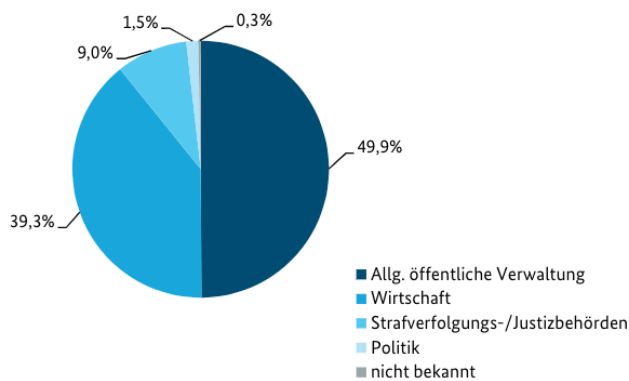
Abb. 34 Gesamtwert der Vorteile auf Geberseite



Quelle: BKA 2020b:22

Die öffentlichen Verwaltungen waren, wie auch den vergangenen Jahren, die häufigsten Vorteilsnehmer. Trotzdem ist auch hier ein Rückgang um 22% im Vergleich zum Vorjahr festzustellen, dagegen stieg die Korruption im Bereich der Wirtschaft um 21,4% an (Abb. 35).

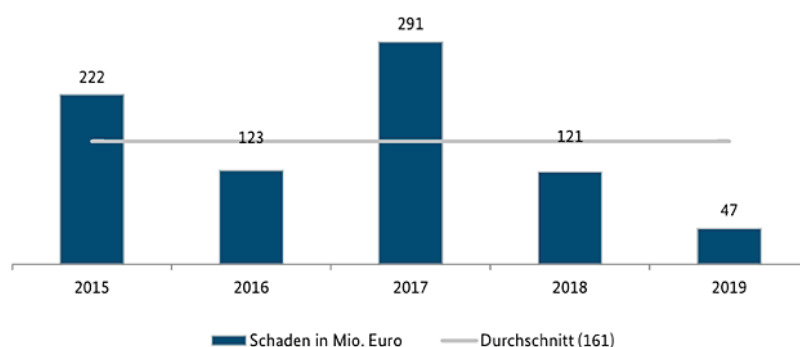
Abb. 35 Zielbereiche der Korruption



Quelle: BKA 2020b:24

Die Gesamtsumme aller Vorteilsnahmen in Geld belief sich im Jahr 2019 auf annähernd 47 Mio. Euro. Sie sank damit um 1,4% im Vergleich zum Vorjahr und lag somit erheblich unter dem Fünf-Jahres-Durchschnitt von 161 Mio. Euro (Abb. 36). Die rückläufige Entwicklung ist dabei auf geringere Schadenssummen zurückzuführen. Im Durchschnitt belief sich die festgestellte Summe auf ca. 41.000 € pro Korruptionsfall, während es im Jahr 2018 ca. 142.000 € waren (BKA 2020b:25).

Abb. 36 Gesamtschaden (in Mio. Euro)

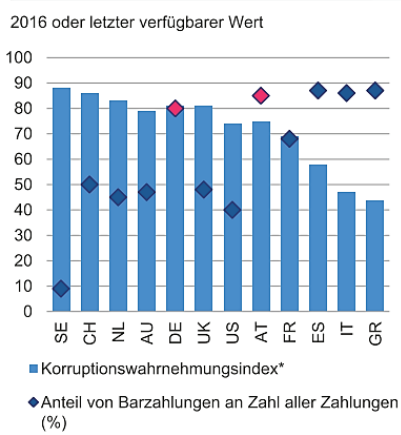


Quelle: BKA 2020b:25

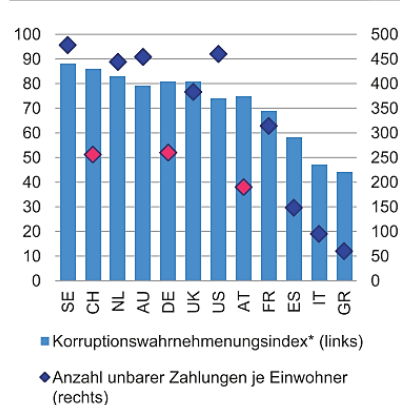
Die dabei ermittelten Summen geben jedoch nicht das tatsächliche Ausmaß des Schadens, hervorgerufen durch Korruption wieder. Daher können auch keine verbindlichen Aussagen diesbezüglich getroffen werden. Beispielsweise sind die monetären Schäden durch erlangte Genehmigungen nur erschwert messbar (BKA 2020b:25). Wie bereits dargelegt, war im Fünf-Jahres-Vergleich ein Anstieg der Korruptionsstraftaten zu verzeichnen. Dieser Anstieg wird jedoch auf umfangreichere Ermittlungstätigkeiten und -verfahren zurückgeführt, welche sich damit auch statistisch signifikant ausgewirkt haben. Das BKA führt weiterhin an, dass die Dunkelziffer weitaus höher liegen kann, da nicht alle Delikte angezeigt werden. Dementsprechend fällt auch die ermittelte Schadenssumme kleiner aus. Darüber hinaus gibt das BKA zu bedenken, dass immaterielle Schäden wie der Verlust in Vertrauen in die staatliche Unbestechlichkeit oder wirtschaftliche Integrität nicht messbar sind (BKA 2020b:28). Auch im Rahmen der ersten nationalen Risikoanalyse kommt das BMF zu dem Ergebnis, dass eine beträchtlich hohe Dunkelziffer von Korruptionsfällen gegeben ist. Die Anzahl der Fälle ist zwar nicht hoch, jedoch sind diese partiell mit Bezug auf das Ausland und mit hohen Summen einhergehend (Bundesministerium der Finanzen 2019:29). Gemessen am Korruptionswahrnehmungsindex (Corruption Perceptions Index, CPI) befindet sich Deutschland auf dem 9. Rang. Mai führt an, dass Korruption nicht mit der Höhe des Bargeldumlaufs korreliert. Während in Ländern wie Deutschland oder Österreich ein hoher Bargeldumlauf vorliegt, belegen diese doch ein recht niedriges wahrgenommenes Korruptionsniveau in den staatlichen Behörden (Abb. 37) (Mai 2018:135). Auch hier ist deutlich zu sehen, dass in Ländern wie Schweden mit einer niedrigen Bargeldnutzung die Korruptionswerte höher liegen können als in Ländern mit hoher Bargeldverwendung.

Abb. 37 Bargeld und Korruption

Häufige Bargeldnutzung nicht identisch mit starker Korruption im öffentlichen Sektor



Nutzung unbarer Zahlungsmittel und Korruption im öffentlichen Sektor 2016



*Der Korruptionswahrnehmungsindex (CPI) misst weltweit das wahrgenommene Korruptionsniveau im öffentlichen Sektor auf einer Skala von 0 (sehr korrupt) bis 100 (sehr sauber).

*Der Korruptionswahrnehmungsindex (CPI) misst weltweit das wahrgenommene Korruptionsniveau im öffentlichen Sektor auf einer Skala von 0 (sehr korrupt) bis 100 (sehr sauber).

Quellen: Transparency International, Payments Council, Verband Elektronischer Zahlungsverkehr, nationale Zentralbanken, Deutsche Bank Research.

Quellen: Transparency International, EZB, BIZ, Deutsche Bank Research

Quelle: Mai 2018:135

Dies gilt auch aus Sicht von König in Bezug auf die Einführung von Bargeldobergrenzen. Trotz der in manchen Ländern vorhandenen Obergrenzen konnte die Kriminalitätsrate nicht reduziert werden (König 2016:6). Beispiele von Bargeldgrenzen in den verschiedenen Ländern sind in Tab. 7 dargestellt:

Tab. 7 Barbezahlungsobergrenzen einzelner Länder der EU

Land	Bargeldbezahlungsobergrenze in € ¹	CPI-Rang 2020 ²
Belgien	3.000	15
Bulgarien	5.110	69
Estland	Bargeld kann ab 50 Geldstücken oder Geldscheinen verweigert werden, egal wie hoch der Wert ist.	17
Finnland	Keine, aber Händler nicht gesetzlich verpflichtet, Bargeldzahlungen immer zu akzeptieren	3
Frankreich	1.000	23
Griechenland	500	59
Italien	2.999,99	52
Kroatien	15.000	63
Polen	15.000	45
Portugal	1.000 Zwischen Verbraucher und Händler	33
Rumänien	2.260 pro Tag	69
Slowakei	5000 unter Händlern 15.000 unter Privatpersonen	35
Spanien	2.500	32
Tschechische Republik	13.000	49
Ungarn	5.000 pro Monat gilt für juristische Personen, Unternehmerverbände und Einzelpersonen, die mehrwertsteuerpflichtig sind	69

Quelle: eigene Darstellung in starker Anlehnung an: ¹ Europäisches Verbraucherschutzzentrum Deutschland 2020. <https://www.evz.de/finanzen-versicherungen/hoechstgrenzen-bargeldzahlung.html>. abgerufen am 21.06.2021, ² Transparency International Deutschland e.V., <https://www.transparency.de/cpi/cpi-2020/cpi-2020-tabellarische-rangliste/>. abgerufen am 06.08.2021

Hier wird ersichtlich, dass keine Korrelation hinsichtlich der Einführung einer Barzahlungsobergrenze und der Höhe der Korruption in den Ländern besteht.

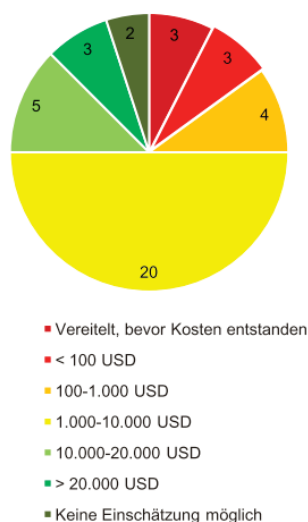
5.4.5 Terrorismusfinanzierung, Drogenhandel und Menschenmuggel

Die Europäische Kommission geht davon aus, dass bei der Terrorismusfinanzierung hauptsächlich Bargeld Verwendung findet. Bei der Bargeldeinführung in die EU ist ab einem Betrag von 10.000 Euro die Person zu kontrollieren, welche den Betrag mit sich führt. Zusätzlich ist die Europäische Kommission darum bemüht, den Anwendungsbereich der entsprechenden EU-Verordnung zu vergrößern, damit Bargeld auch auf dem postalischen Weg erfasst werden kann. Zusätzlich soll dadurch die Möglichkeit gegeben sein, bereits bei weniger hohen Beträgen im Verdachtsfall von illegalen Aktivitäten, Kontrollen durchzuführen. Eine Ausweitung auf teure Güter und Edelmetalle wäre aus ihrer Sicht denkbar. Weiterhin plädiert die Europäische Kommission für eine Barzahlungsobergrenze. Angeführt wird dabei die Begründung, dass Strafverfolgungsbehörden die Bargeldverwendung kritisch in Bezug auf illegale Aktivitäten betrachten. Insbesondere hohe Banknoten stellen aufgrund ihres hohen Wertes aber relativ kleinen Volumens ein Problem dar, da sie leicht transportiert werden könnten (Europäische Kommission, 2016:11). Aber auch auf anderen Wegen wird der Terrorismus finanziert. Beispielsweise kommt es zum Missbrauch von wohltätigen Organisationen und legalen Unternehmen der Wirtschaft. Legal wird die Finanzierung des Terrorismus partiell auch auf dem Wege von Spendenaufrufen vorgenommen. Die FATF stellte in einem Bericht fest, dass sich die Terrororganisation Da'esh vor allem durch illegale Erträge finanziert. Beispiele dafür sind Banküberfälle, Schutzgelderpressung, Raubüberfälle, Erpressungen von Lösegeldern und nicht legale Bargeldtransaktionen (Europäische Kommission, 2016:13 f.). Die Begrenzung anonymer Bargeldtransfers und die weltweiten Ausweitungen der Geldwäschekontrollen bzw. der Erlass ihrer Vorschriften waren nach Rogoff bedeutende Gründe für eine Terrorismusbekämpfung. Insbesondere die Anschläge vom 11. September 2001 sorgten für weltweite Anstrengungen für die Durchsetzung von Geldwäschegesetzen. Besonderes Augenmerk galten hohen Einzahlungen und Überweisungen von Bargeld. Die Europäische Kommission drängte zudem nach den Anschlägen in Paris im November 2015 auf Regulierungsmaßnahmen für digitale Währungen und Prepaid-Karten. Die EZB beschloss im Jahr 2016 die 500 € Banknote nicht mehr nachproduzieren zu wollen, um so eine Finanzierung für den internationalen Terrorismus zu erschweren. Rogoff ist jedoch der Meinung, dass Bargeld in Bezug auf Terrorismus im Vergleich zum Drogenhandel eine eher nachgeordnete Rolle spielt, auch wenn sich Terrororganisationen wie die ISIS mit hohen Bargeldsummen, welche durch Raubüberfälle in den Besatzgebieten erbeutet wurden, teilfinanziert haben. Rogoff vermutet wesentlich höhere Bargeldverwendungen im Bereich anderer Delikte wie bspw. bei der Steuerhinterziehung. Aber auch wenn Bargeld eher eine nachgeordnete Rolle spielt, sieht Rogoff die Bargeldbeschränkung als essenziell für die Terrorismusbekämpfung an (Rogoff 2016:104 f.). Für die internationalen Finanzierungen notwendiger Einnahmen von Terrorgruppen existieren nur unbestimmte Schätzungen. Von der UNODC wurde im Jahr 2003 geschätzt, dass sich die Einnahmen durch den Handel mit Drogen auf einen ungefähren Wert von 322 Mrd. US-Dollar belaufen. Durch Produktfälschungen sollen laut OECD im Jahr 2007 Einnahmen von 250 Mrd. US-Dollar generiert worden sein. Insgesamt macht dies einen Anteil von 50% durch Drogengeschäfte und 39% durch Produktfälschungen an den gesamten Einnahmen der OK aus. Die verbleibenden Prozente gehen auf weitere illegale Geschäfte wie bspw. Menschenmuggel zurück. Es wird vermutet, dass in 80% aller Drogengeschäftsfälle Bargeld verwendet wird. Bei Produktfälschungen soll der Anteil bei 30% liegen. Mai geht davon aus, dass Bargeldumlaufbeschränkungen aufgrund Politikmaßnahmen eine Erhöhung der Transaktionskosten (wie bspw. Beschaffungskosten) für die OK nach sich ziehen würden. Allerdings befürchte Mai, dass lediglich ein Rückgang von 10-20% der OK aufgrund hoher Gewinne durch diese Maßnahmen bewirkt werden würde. Zu bedenken ist außerdem, dass die Schätzungen der Einnahmen aus finanziellen und steuerlichen Straftaten bereits ungefähr 50% höher liegen als die Einnahmen der OK. Weiterhin vermutet Mai, dass dazu kein Bargeld notwendig ist, wie das Beispiel des Panama-Skandals beweist. Die FATF gibt an, dass durch die Nachverfolgung illegaler Bargeldströme eine Terroristenidentifizierung und Anschlagshinderung möglich gemacht wird. Trotz dieser umfangreichen Ermittlungen im finanziellen Sektor ist ein Anstieg des Terrorismus seit dem Jahr 2001 zu verzeichnen. Daher müsse die Frage gestellt werden, ob die Ermittlungen nicht ausreichend bzw. mit Mängeln behaftet waren oder ob eine finanzielle Kontrolle des Terrorismus grundsätzlich schwer zu gewährleisten ist. Eine Analyse von vierzig terroristischen Dschihad-Anschlägen der letzten 20 Jahre in Europa ergab, dass sich die

Terrorgruppen aus eigenen Mitteln finanzierten. Dabei konnten 75% aller Anschläge mit einem finanziellen Volumen mit weniger als 10.000 US Dollar ausgeführt werden (Abb. 38). Diese Beträge fallen auch bei umfangreichen Kontrollen kaum ins Gewicht, selbst wenn diese unbar entrichtet werden (Mai 217:10 f.).

Abb. 38 Kosten von Terroranschlägen

Terroranschläge der letzten 20 Jahre in Europa kosteten zumeist unter 10.000 USD **15**
Zahl der Anschläge nach geschätzten Kosten



Quelle: Mai 2017:11

In Bezug auf Terrorismus bemängelt auch Schneider die Schätzungen über die Höhe der Einnahmen der OK. Unterschieden wird bei Schätzungen/Berechnungen nach direkten und indirekten Methoden (App. 15). Direkte Methoden schätzen das Volumen anhand der ihnen vorliegenden Zahlungsströme, jedoch nehmen diese keine Differenzierung von legalem und illegalem Geld vor, was es beinahe unmöglich macht, ein Dunkelfeld bestimmen zu können. Indirekte Methoden hingegen erfassen lediglich Teile der Finanzierungsmöglichkeiten wie bspw. beim Handel mit Drogen. Andere Finanzierungsbereiche wie bspw. der Handel mit Waffen oder Edelsteinen können zudem mit diesen Methoden nur mit hohen Schwierigkeiten erfasst werden (Schneider 2009:75 f.). Schneider gibt hier wieder zu bedenken, dass die Finanzierungsquellen der OK lediglich partiell erfasst werden und das Bargeld nur einen Teil davon darstellt. Weiterhin nutzt das organisierte Verbrechen, zu dem der Terrorismus zählt, bereits legale Finanzierungsmöglichkeiten wie bspw. Spendenaufrufe. Diese werden nicht unter dem Begriff des „Schwarzgeldes“ (Schneider 2009:81) erfasst und trotzdem für die Finanzierung von Waffen oder Sprengmitteln verwendet (Schneider 2009:81).

5.4.6 Conclusio Kriminalität

Wie dargelegt, ist der Umfang der Verwendung von Bargeld innerhalb des organisierten Verbrechens nur schwer zu ermitteln. Oftmals beruhen diese auch nur auf Schätzungen oder Hochrechnungen. Es liegt hier die Vermutung nahe, dass eine Bargeldbeschränkung die OK partiell beschränken könnte, diese aber keinesfalls die Möglichkeit einer Beseitigung bieten würde. Zudem gibt es vielfältige andere Methoden der Verwahrung oder des Transportes von illegalem Vermögen wie bspw. in Form von Edelmetallen. Diese können aufgrund einer Spurenverwischung kaum erfasst werden. Dazu zählen u.a. auch die Benutzung falscher Identitäten, der Einsatz von Scheinfirmen bei bargeldlosem Zahlungsverkehr im Finanzsektor oder Online-Zahlungen. Die Verwendung von Kryptowährungen stellt eine weitere Möglichkeit dar. Eine Bargeldabschaffung und die Verwendung eines Substitutes e.g. eine digitale Währung mit voll kontrollierbaren und intransparenten Eigenschaften steht jedoch im Widerspruch zum persönlichen Datenschutz der Men-

schen, da ein Schutz nicht mehr gewährleistet wäre. Infolgedessen könnten die Daten missbräuchlich durch staatliche Stellen verwendet werden wie bspw. für Bürgerrechtseinschränkungen. Aber auch ein Missbrauch der Daten durch Unternehmen und die Cyberkriminalität ist hier zu berücksichtigen. Daher gibt es für Mai grundsätzlich nur dann ein Grund für eine Bargeldbegrenzung, wenn fundierte Ergebnisse für das Senken der Kriminalitätsrate in der Verbrechensbekämpfung vorliegen. Weiterhin nimmt Mai an, dass dadurch zwar ein rückwärtiger Trend zu verzeichnen wäre, dieser jedoch nur sehr gering ausfallen würde. Stattdessen sollten die Möglichkeiten der Strafverfolgungen stärker ausgebaut werden wie bspw. die übergreifende Informationsabstimmung oder der Austausch von Informationen innerhalb der Strafverfolgungsbehörden (Mai 2017:11 f.). Schneider schlägt folgende Maßnahmen für die Terrorismusbekämpfung bzw. OK vor:

1. „Bekämpfung der Armut besonders in Ländern mit fundamentalistischen Religionen;
2. Wahrung und Stärkung der demokratischen Grundrechte, der Meinungsfreiheit, der Toleranz sowie der Offenheit;
3. geistige Auseinandersetzung mit dem (insbesondere radikalen) Islamismus;
4. finanzielle Unterstützung der gemäßigten Strömungen;
5. nur Law-and-Order-Maßnahmen beziehungsweise die Todesstrafe wirken nicht, da sie aus den Terroristen Märtyrer machen;
6. menschenrechtskonformer Umgang mit Terroristen und moderate Rhetorik“ (Schneider 2009:83 f.).

Auch Noack und Philipper zweifeln an einer Wirkung in der Beschränkung oder Abschaffung von Barzahlungen. Darüber hinaus sind Noack und Philipper der Meinung, dass die vermutete Erleichterung der Tätigkeiten der Strafverfolgungsbehörden durch Bargeldbeschränkungen oder Bargeldabschaffungen weit überschätzt wird. Weiterhin gehen Noack und Philipper auch konform mit Schneider und Mai in der Zunahme bargeldloser (illegaler) Transaktionen. Noack und Philipper gehen weiter davon aus, dass es insgesamt einen Anstieg der Cyberkriminalität geben wird (Noack/Philipper 2016:13). Meyer bezieht sich ebenso auf die Panama Papers in Bezug auf Bargeldtransaktionen. Wie dieser Fall gezeigt hat, benötigt es mittlerweile keine Bargeldtransaktionen mehr, um bspw. Delikte im Bereich des finanziellen und steuerlichen Betrugs zu begehen (Meyer 2020:132). Insgesamt lässt sich feststellen, dass mit einer Bargeldbeschränkung oder einer kompletten Abschaffung die Kriminalität nicht signifikant sinken würde. Anhand mehrerer Beispiele wurde aufgezeigt, dass im Rahmen der Digitalisierung bereits vielfältige andere Methoden existieren, die von dem organisierten Verbrechen genutzt werden. Bei einer völligen Abschaffung des Bargelds ist zudem ein Erstarren der Cyberkriminalität zu erwarten sowie das Ausweichen auf Substitute des Bargelds (Mai 2017:13). Lediglich in Bezug auf Verbrechen, welche sich ausschließlich auf die Erbeutung von Bargeld richten, würde mit einer Bargeldabschaffung eine Besserung eintreten.

Im folgenden Kapitel wird die These des Ausweichens der Kriminalität in den digitalen Raum eruiert.

Teil 2 - Cybercrime und andere Formen unbarer Kriminalität

6 Cybercrime, Kryptowährungen und andere Begrifflichkeiten

Nachfolgend wird der Begriff des Cybercrimes und die damit oft in Verbindung gebrachten Kryptowährungen näher erläutert.

6.1 Cybercrime

Der Begriff des Cybercrimes wird aufgrund verschiedener Betrachtungen unterschiedlich definiert. Manche Definitionen betrachten ausschließlich Verbrechen mit dem Computer, andere wiederum setzen das Internet als Tatwaffe voraus. Dem BKA zufolge gibt es „Cybercrime im engeren Sinne“ und „Cybercrime im weiteren Sinne“. Cybercrime i.e.S. umfasst dabei die Delikte „[...] die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten“ (BKA 2021b:42), während Cybercrime i.w.S. Delikte umfasst, welche unter der Verwendung von Informationstechnik begangen werden. Als Tatmittel wird das Internet vorausgesetzt (BKA 2021b:42). Nach Huber gibt es drei verschiedene Betrachtungsweisen:

- „Variante 1: Cybercrime im engeren Sinne (Core Cybercrime, Cyberdependent Crime)“ (Huber 2019:3): dazu zählen ausschließlich Delikte, welche ohne Online-Aktivitäten nicht möglich sind wie bspw. Hacken, Viren- und Trojaner (Ransomware) Verbreitung
- „Variante 2: Cybercrime im weiteren Sinn (Non-cyberspecific Cybercrime bzw. Cyberenabled Crime)“ (Huber 2019:3) - Zusätzlich zu den bereits unter Variante 1 gehörenden Delikten werden auch Delikte gezählt, welche sich offline begehen lassen wie bspw. Geldwäsche, Urheberrechtsverletzungen, Missbrauch von Kreditkarten etc.
- „Variante 3: Verschleierung der Identität“ (Huber 2019:3): darunter zählen Delikte wie das Verbreiten illegaler Inhalte (e.g. rassistisches Gedankengut) mit Hilfe einer falschen Identität in den sozialen Medien (Huber 2019:3).

Darüber hinaus besteht, dem rechtlichen und kulturellen Verständnis des jeweiligen Landes geschuldet, kein Konsens in Bezug auf eine länderübergreifende Definition des Begriffes. Während bspw. in einem Land gilt, dass bereits Cybercrime vorliegt, wenn Delinquent:innen sich mit Hilfe eines Computers per E-Mail zu einer Straftat verabreden, ist es in anderen Ländern völlig belanglos, da hier auf den Zeitpunkt des Begehens der Straftat an sich abgestellt wird (Huber 2019:23). Das bloße sich verabreden via Personal Computer (PC) allein stellt keine Straftat dar. Für eine Definition des Begriffes Cybercrime kommt erschwerend hinzu, dass unterschiedliche Auslegungsweisen aufgrund verschiedener Wissenschaften wie rechtswissenschaftliche, kriminologische, psychologische, ökonomische oder technische Ansichten existieren und daraus schlussfolgernd bis dato kein Konsens in Bezug auf eine einheitliche Definition gefunden werden konnte (Huber 2019:24). In den folgenden Ausführungen wird der Definition des Cybercrimes im weiteren Sinne (Variante 2) nach Huber gefolgt.

6.2 Kryptowährungen und digitales (elektronisches) Geld

Nachfolgend werden die Funktionsweisen und einige technische Details von Kryptowährungen näher erläutert.

6.2.1 Allgemeines

Kryptowährungen sind in ihrer Funktion vergleichbar mit Bargeld, da beide über ein dezentrales Peer-to-Peer (P2P) Netzwerk verifiziert werden können (P2P beschreibt im PC-Bereich ein Netz gleichgestellter Computer). Beim Bargeld wird dies durch direkte Übergabe bewirkt, während es bei Kryptowährungen durch sogenannte Distributed-Ledger-Technologien ermöglicht wird. Beiden ist also eine Dezentralität inne, d.h. eine zentrale Stelle für eine Verifizierung ist im Gegensatz zu der Verwendung zum Buch- bzw. Giralgeld nicht notwendig. Bei Buch- bzw. Giralgeld wird die Verifizierung durch den Finanzsektor vollzogen. Im Gegensatz zum Bargeld können Kryptowährungen jedoch nicht physisch gehandelt werden (Wohlmann 2020:305). Das Wort Währung

ist aus dem mittelhochdeutschen Wort „werunge“ (Wohlmann 2020:307), zu deutsch „Gewährleistung“ (Wohlmann 2020:307), abgeleitet und bedeutet, dass für die Werthaltigkeit des Tauschmittels eine Art Gewährleistung übernommen wird. Da bei Kryptowährungen aufgrund fehlender zentraler Verifizierung aber eben gerade keine Gewährleistung übernommen wird, stellt es im Grunde keine Währung dar, denn sie unterliegt lediglich privat geschaffenen Regeln. Gleichwohl können sie auch nicht dem Geldbegriff zugeordnet werden, da sie infolge enormer Kursschwankungen nicht als Wertaufbewahrungsmittel geeignet sind (Wohlmann 2020:307 f.). Laut BaFin zählen virtuelle Währungen gem. § 1 XI 1 Nr. 10 Kreditwesengesetz (KWG) zu den Finanzinstrumenten (BaFin 2020). Die Bedeutung von Kryptowährungen als staatlich anerkannte Währung könnte sich jedoch zukünftig ändern, denn trotz der Bedenken der starken Kursschwankungen, wurde erstmals im Jahr 2021 die Kryptowährung Bitcoin als staatlich anerkannte Währung in El Salvador eingeführt (Mansholt 2021a). Der Begriff Kryptowährung wird in den folgenden Ausführungen weiterverwendet, da er sich unter dieser Bezeichnung in der Öffentlichkeit etabliert hat.

6.2.2 Distributed-Ledger-Technologies und Blockchain

Kryptowährungen und andere Formen elektronischen Gelds haben das Problem einer unendlichen Duplikationsmöglichkeit inne, bekannt unter dem Begriff des „Double-Spendings“ (Wohlmann 2020:309). So könnte beispielsweise ein Betrag nach erfolgter Überweisung nicht vom Zahlungskonto gelöscht werden, obwohl dieser bereits auf dem Empfängerkonto eingegangen ist. Der Betrag würde somit dupliziert werden. Dieser Vorgang könnte theoretisch zudem beliebig oft wiederholt werden. Wie bereits beschrieben, unterliegt bspw. Giralgeld einer zentralen „Clearingstelle“ (Wohlmann 2020:309), diese würde im beschriebenen Fall den Betrag vom Konto des Sendenden löschen und damit die Korrektheit des Vorgangs bestätigen. Bei elektronischem Giralgeld wird dies üblicherweise durch eine zentrale Stelle wie bspw. einer Bank übernommen. Diese Stelle verwaltet und überwacht quasi das Hauptbuch aller Transaktionen. Im Gegensatz dazu existiert bei Kryptowährungen, welche auf die Distributed-Ledger-Technologien (DLT) basieren, kein zentrales Hauptbuch, in dem alle Transaktionen verzeichnet sind, sondern etliche Kopien nach Anzahl der Miner. Der sogenannte Miner stellt einen User oder auch Knoten im Blockchain-Netzwerk dar, welcher die Eintragung von Transaktionen in seiner Kopie des Hauptbuchs vornimmt. Allerdings wird damit noch nicht die Korrektheit der Transaktion bestätigt, denn alle verbleibenden Miner müssen ebenso die Richtigkeit dieser Transaktion in ihrer Kopie des Hauptbuches bestätigen. Erst dann kann die Transaktion auch verbucht werden. Somit entfällt hier eine zentralisierte Verifizierungsstelle, welches den bedeutendsten Unterschied zum Geld darstellt (Wohlmann 2020:309 ff.). Die bekannteste DLT ist die Blockchain-Technologie und die darauf beruhende Kryptowährung Bitcoin. Hier werden die einzelnen Transaktionen in Blöcken gesammelt, mit anderen linear aufgereiht und zusammengefügt. Dadurch entsteht die Blockkette - die Blockchain. Der gesamte Vorgang wird auch als Mining bezeichnet. Für die Sicherheit des gesamten Vorgangs sorgen die in den Blöcken enthaltenen „Hashwerte“ (Hornetsecurity o.D.), die wie Prüfziffern fungieren. Darüber hinaus enthält dieser Hashwert sowohl Daten der aktuellen als auch der vorherigen Transaktion und schützt damit insbesondere vor post festum versuchten Manipulationen, denn dann würden die Hashwerte nicht mehr übereinstimmen und den gesamten Vorgang an sich ungültig machen (App. 16) (Hornetsecurity o.D.). Zudem ist die Datenbank (Hauptbuch) völlig transparent, da jegliche Transaktionen von der Öffentlichkeit eingesehen werden können. Don und Alex Tapscott beschrieben im Jahr 2016 die Blockchain als ein „[...] unbestechliches digitales Hauptbuch von wirtschaftlichen Transaktionen, das so programmiert werden kann, dass es nicht nur finanzielle Transaktionen, sondern praktisch alles von Wert erfasst“ (Schiller 2019). Die ursprüngliche Idee des Bitcoins wurde von dem Pseudonym Satoshi Nakamoto entwickelt. Wer sich dahinter verbirgt, konnte bis dato nicht geklärt werden. In einem Whitepaper beschrieb Nakamoto als Ziel für die Entwicklung der Kryptowährung Bitcoin, das Online-Zahlungen zwischen Nutzern erfolgen können, ohne den Umweg über ein Finanzinstitut nutzen zu müssen (Nakamoto 2008:1). Insbesondere Finanzinstituten spricht Nakamoto das Vertrauen ab, da sie selbst in der Vergangenheit riskante Investitionen mit den ihnen anvertrauten Werten durchführten und Menschen dadurch weltweit in ihrer Existenz bedroht wurden wie bspw. während der

Immobilienkrise im Jahr 2008 in den USA. Weiterhin spricht Nakamoto sein Misstrauen gegenüber Finanzinstituten im Umgang mit Daten aus und wirft ihnen darüber hinaus Finanzbetrug vor. Die Entwicklung des Bitcoins sollte aufgrund dessen und einer vom Finanzsektor unabhängigen Kryptowährung diesen Dingen Vorschub leisten (Schiller 2019). Weitere bekannte Kryptowährungen sind Ethereum, Bitcoin Cash, Ripple, Dash, Litecoin und Monero, welche ebenso auf der Blockchain-Technologie beruhen. Die derzeit einzige Ausnahme bildet IOTA, welche zwar auch auf der Distributed-Ledger-Technologie basiert, jedoch keine Blockchain verwendet. Der Anspruch der Entwickler ist es, die Geschwindigkeit der Transaktionen zu verbessern, welche mit zunehmender Netzwerkgröße wächst. Zudem gibt es keine Transaktionskosten. Beachtung in Bezug auf das Cybercrime ist vor allem Monero geschuldet, denn diese ist im Gegensatz zu vielen anderen Kryptowährungen vollkommen anonym. Es sind dabei weder die Transaktionen noch die dazugehörigen Wallets nachvollziehbar. Weiterhin wird nicht öffentlich ersichtlich, wer über welches Volumen an Monero verfügt. Als weiterer Vorteil ist die Verwendung von gewöhnlichen Prozessoren zu nennen, so dass das Minen von jeder Person durchgeführt werden kann. Andere Kryptowährungen hingegen benötigen leistungsstarke und kostenintensive Computertechnik, um das Minen zu ermöglichen (Jasch/Companisto 2017). Kryptowährungen werden in pseudonym und anonym unterschieden (Abb. 39). Pseudonyme Währungen wie bspw. Bitcoin können aufgrund ihrer Einsehbarkeit in der Blockchain leichter nachverfolgt werden. Anonyme Kryptowährungen, oder auch Privacy Coins, sind mitunter völlig anonym, um die Privatsphäre zu erhalten. Der wichtigste Vertreter ist Monero mit einem geschätzten Marktvolumen von 4,6 Mrd. \$ (Waidmann 2021).

Abb. 39 Comparison of anonymous Cryptos

	PRIVATE	FUNGIBLE	DECENTRALIZED
MONERO	✓	✓	✓
bitcoin	✗	✗	✓
CASH	?	?	✗
DASH	✗	✗	✗
VERGE	✗	✗	✓

Quelle: masterthecrypto (o.D.). Guide on Privacy Coins: Comparison of anonymous Cryptocurrencies. <https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/>. abgerufen am 08.12.2021

Weiterhin wird bei Kryptowährungen unterschieden in konvertierbar (CVC - convertible virtual currency) und nicht konvertierbar. Laut Definition der FATF handelt es sich bei CVC im Gegensatz zu nicht konvertierbaren Kryptowährungen um Währungen, welche zum einen über Gegenwerte in realen Währungen verfügen und zum anderen auch jederzeit in diese getauscht werden können (FATF 2014:4).

6.2.3 Vor- und Nachteile von Kryptowährungen

In Tab. 8 werden die Vor- und Nachteile von Kryptowährungen dargestellt:

Tab. 8 Vor- und Nachteile von Kryptowährungen

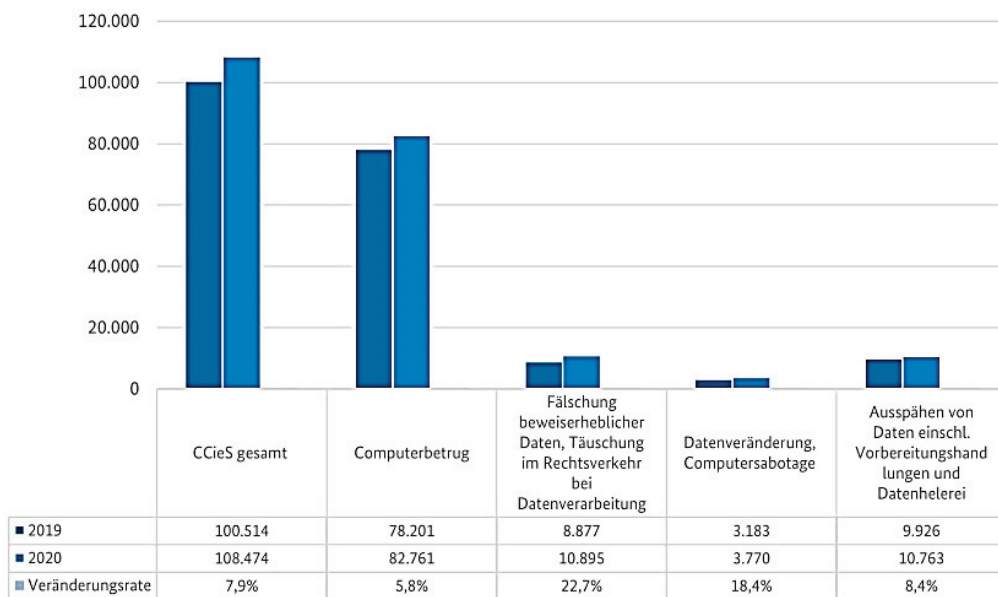
Vorteile	Nachteile
Transaktionen ohne Finanzinstitute, dadurch schneller und nicht so kostenintensiv	kein offizielles Zahlungsmittel - Akzeptanz je nach Bekanntheit der jeweiligen Währung
jeder kann teilhaben - Vor.: Internetzugang	Vor.: Internetzugang
relativ manipulations- fälschungssicher	stark volatil - hohe Wert- und Kursschwankungen
Geldpolitik einflusslos	hohe Anonymität – prädestiniert für Illegalität
kaum Geldschöpfung möglich	starke Computertechnik erfordert und hoher Stromverbrauch
Transaktionen anonym zwischen den teilnehmenden Computern (Coinwissen o.D.)	
hohe Liquidität (schnell in Bargeld umwandelbar)	keine Regulation (keine Rechtsansprüche)
Herkunft und Zielort bekannt	Transaktionen unwiderruflich, bei Diebstahl nicht mehr auffindbar (Burch 2021)

Quelle: eigene Darstellung in enger Anlehnung an Coinwissen o.D. und Burch 2021

6.3 Die Entwicklung der Cyberkriminalität

Die Digitalisierung schreitet zunehmend voran und somit auch die Anzahl an Geräten, welche mit dem Internet verbunden sind. Mit ihnen steigt auch die Potenzialität von Cyberangriffen und Cyberkriminalität. Die Formen der Cyberkriminalität sind dabei zahlreich und unterliegen aufgrund unterschiedlicher Kontexte verschiedenen Klassifikationen. Aufgrund der steigenden Potenzialität der Angriffe nimmt auch die Gefährdung von Unternehmen (insbesondere die der kritischen Infrastruktur), staatlichen Einrichtungen aber auch von privaten Personen zu. Mit der Entwicklung von neuen Sicherungsmöglichkeiten entstehen annähernd zeitgleich Methoden durch Cyberkriminelle, diese zu umgehen oder zu durchdringen. Infolgedessen entstehen Schäden in Millionenhöhe für die Betroffenen durch Diebstahl von Daten oder anderen Delikten (Horten/Gräber 2020:234). Die Cyberkriminalität nahm in den letzten Jahren rasant zu. Meist steht vor allen Delikten der digitale Identitätsdiebstahl, d.h. das Entwenden digitaler personenbezogener Daten. Das BKA führt dabei Phishing- und Spam-Mails, schädliche Software wie Keylogger (aufnehmen von Tastaturanschlägen), nicht gewollte Datenlecks oder bewusst herbeigeführte Dateneinbrüche als häufigste Ursachen an. Spam-Mails sind insbesondere darauf ausgerichtet, durch das Folgen von Weblinks oder des Herunterladens von angehängten Dateien eine Systemkompromittierung herbeizuführen, um so an die gewünschten Daten zu gelangen. Im Jahr 2019 war hier bereits ein 2,8-facher Zuwachs zum Jahr 2018 zu verzeichnen. Und oftmals bekommen die betroffenen Personen den Angriff nicht mit. Eine Form der Spam-Mails ist die Mal-Spam, in ihr ist bereits die Malware enthalten (BKA 2020c:7 ff.). Malware ist Software, welche schädliche Aktionen im betroffenen System ausführen, wie bspw. Datendiebstahl, Datenmanipulation, Datenvernichtung, Übernahme von Computerleistung für das Minen von Kryptowährungen, Fernsteuern von IT-Systemen oder Datenverschlüsselungen. Der Eintritt erfolgt, wie bereits beschrieben, meist über die Mailzugänge. In 2019 wurde die Zahl der identifizierten Malware-Familien bereits auf über eine Milliarde, mit einem täglichen Zuwachs von in etwa 312.000 Varianten, geschätzt (BKA 2020c:12 f.). Im Jahr 2020 waren es bereits 1,15 Mrd. Varianten mit einem täglichen Zuwachs von 314.000 Varianten (BKA 2021b:19). 2019 und 2020 verglichen ergeben dabei die folgenden Zuwächse der einzelnen Delikte, ausgedrückt in der Veränderungsrate in Abb. 40.

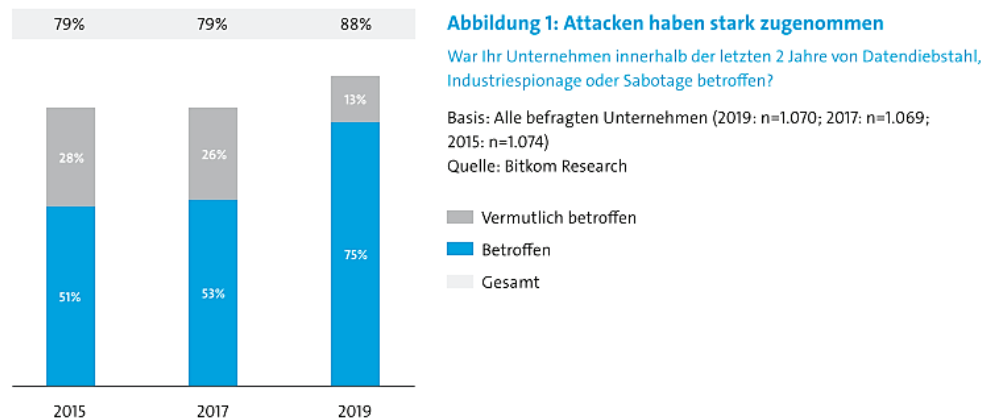
Abb. 40 Fallaufkommen von Straftaten der CCieS 2019 und 2020



Quelle: BKA 2021b:11

Im Jahr 2019 waren bereits drei von vier Unternehmen in Deutschland von Straftaten betroffen. Dazu zählen das Stehlen von Daten, Spionage oder Unternehmenssabotage. In den Vorjahren war lediglich jedes zweite Unternehmen Opfer eines Angriffs (Abb. 41) (Bitkom 2020b:7).

Abb. 41 3 von 4 Unternehmen sind Opfer geworden

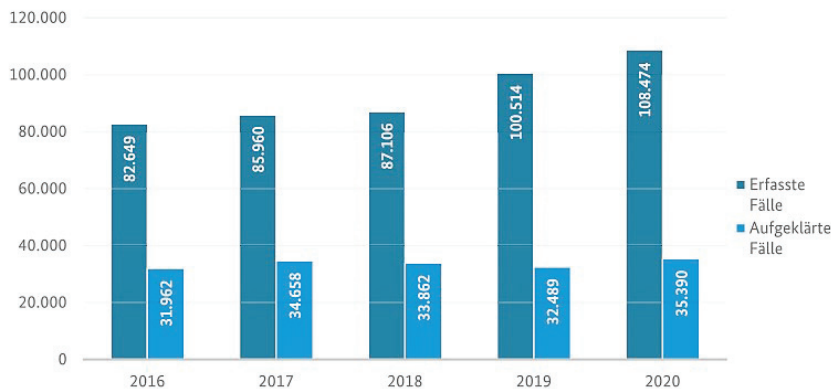


Quelle: Bitkom 2020b:7

Ein Zuwachs um 7,9% mit 108.000 Delikte wurde im Vergleich zum Vorjahr im Jahr 2020 verzeichnet. Als Erklärung führt das BKA die stetig steigende Digitalisierung sämtlicher Lebensbereiche, die wachsende Professionalisierung der Täter:innen bzw. Tätergruppen sowie die gesunkenen Einstiegsvoraussetzungen durch „Cybercrime-as-a-Service“ an (BKA 2021b:9 f.). Cybercrime-as-a-Service bedeutet, dass durch professionellen Service entweder Hilfe für kriminelle Taten bereitgestellt wird oder diese selbst durch Professionelle im Auftrag durchgeführt werden. Diese Leistungen werden überwiegend im Deep Web bzw. Darknet angeboten. Der Unterschied zwischen dem Deep Web oder auch Invisible Web und dem Darknet ist, dass Internetseiten im Deep Web mit gängigen Internetbrowsern erreichbar sind, diese jedoch nicht indiziert oder lediglich im Zugang beschränkt sind. Internetseiten im Darknet sind nur mit speziellen Browsern e.g. dem Tor-Browser erreichbar. Das Darknet bietet neben völlig legalen Aktivitäten auch nicht legale Möglichkeiten von Wikis, Foren oder Blogs bis hin zu Marktplätzen auf denen illegale Güter

angeboten werden (BKA 2021b:43). Starken Zuwachs erhielt das Cybercrime und die Nutzung des Internets weiterhin durch die Maßnahmen während der Corona-Lockdowns. Hauptbedrohungen entstanden hier durch Malware- und Phishing Spam sowie durch falsche Webseiten (BKA 2020d:5), welche oftmals auf Unternehmen der kritischen Infrastruktur ausgerichtet waren (BKA 2020d:18). Die Aufklärungsquote der Delikte hingegen nimmt im Verhältnis zu den zunehmenden Delikten ab oder stagniert (Abb. 42) (BKA 2021b:10).

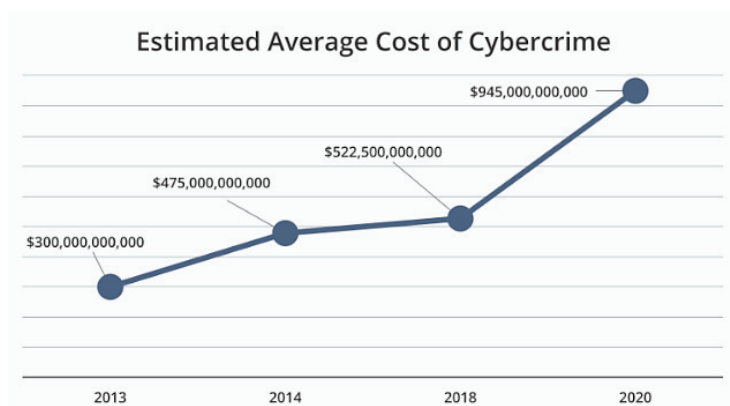
Abb. 42 Relation zwischen erfassten und aufgeklärten Cybercrime-Fällen Deutschland von 2016 bis 2020



Quelle: BKA 2021b:10

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht insgesamt von einer „besorgniserregend[en]“ (BSI 2021:4) Lage in Deutschland durch die sich ständig verändernden, schnell wachsenden und anpassenden Methoden der Angriffe. Dabei nutzen die Delinquent:innen Schwachstellen in Hard- und Software aus (BSI 2021:4), aber zunehmend wird auch auf die Schwachstelle Mensch gesetzt (BSI 2021:10). Die Vernetzung der Kriminellen ist, wie ihre begangenen Straftaten auch, global mit zunehmender Professionalisierung (BKA 2021b:3). Im Jahr 2014 betrugen die Auswirkungen des Cybercrimes laut Schätzungen weltweit bereits 500 Mrd. Dollar, 2018 600 Mrd. Dollar (McAfee/CSIS 2018:1) und im Jahr 2020 eine Billion Dollar, bestehend aus 945 Milliarden Dollar an reinem Verlust und 145 Milliarden Dollar für Sicherungsmaßnahmen (Malekos Smith/Lostri/Lewis 2020:3). An Abb. 43 wird deutlich, wie sprunghaft sich die Kosten des Cybercrimes im Zeitraum 2013 bis 2020 entwickelten.

Abb. 43 The average cost of cybercrime



Quelle: Malekos Smith/Lostri/Lewis 2020:3

Hauptursachen waren Mal- und Spyware in ihren verschiedenen Variationen wie bspw. Würmer, Viren, Trojaner und Ransomware (Malekos Smith/Lostri/Lewis 2020:24). Begünstigt wird der Anstieg krimineller Delikte durch den sogenannten Cybercrime-as-a-Service (CCaaS), d.h. das

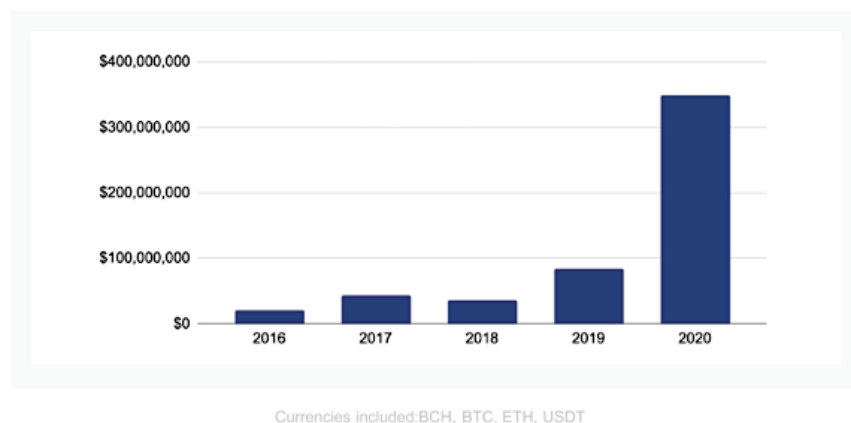
Anbieten cyberkrimineller Straftat als Dienstleistung. Zur Folge hat es, dass sich einzelne Delinquent:innen oder Delinquentengruppen auf einzelne Delikte durch Arbeitsteilung spezialisieren. Stets ist dabei die Gewinnerzielung vordergründig. Dabei beruht CCaaS laut BKA auf neun Säulen (BKA 2021b:12 f.). Diese umfassen die Kontaktaufnahme, das Bereitstellen von entsprechenden Infrastrukturen und Anonymisierungsdienstleistungen, Bereitstellung von Zugangsdaten auf Marktplätzen, Schadsoftwareentwicklung, Verbesserung der Schadsoftwarecodes, Tests der Schadsoftware mit gängigen Antivirentools auf Erkennbarkeit, Verbreitung und Installation der Schadsoftware, Umleiten der inkriminierten Erträge mit Konten oder Abheben von Geldautomaten und die digitale Geldwäsche zur Herkunftsverschleierung (App. 17) (BKA 2021b:46). Angeboten werden diese Arten von Dienstleistung meist im Deep Web oder Darknet (BKA 2021b:13). Nachfolgend werden einzelne Delikte des Cybercrimes näher behandelt. Dabei wird die Kategorie Ransomware aus der Gruppe der Malware näher untersucht, anschließend wird auf den Handel mit illegalen Gütern und Dienstleistungen im Deep Web und Darknet eingegangen.

6.3.1 Ransomware und Hacking

Ransomware zählt zur Gruppe der Malware. Diese verschlüsselt auf infizierten Systemen sämtliche Daten. Dabei ist es irrelevant, ob die Daten lokal oder im Netzwerk gespeichert sind. Zusätzlich kommt es in den meisten Fällen zu einem zeitgleichen Datenabfluss. Die Daten sind nach der Verschlüsselung für die Nutzenden nicht mehr zugänglich. Nach der Verschlüsselung wird ein Lösegeld für die Freigabe der Daten verlangt, oftmals einhergehend mit der Drohung, bei Nichtzahlung die erbeuteten Daten nach einer abgelaufenen Frist zu veröffentlichen (BKA 2021b:44). Der Vorteil dieser „Double Extortion“ (BKA 2021b:22) liegt darin, monetäre Vorteile sowohl durch die Erpressung für die Datenentschlüsselung als auch durch das Veräußern der abgeflossenen Daten zu erlangen (BKA 2021b:22). Die Zahlungen der Lösegelder werden bevorzugt in Kryptowährungen verlangt, meist Bitcoin oder Monero (BSI 2021:12). Das BKA bezeichnete im Jahr 2021 Ransomware als „weiterhin die Bedrohung für öffentliche Einrichtungen und Wirtschaftsunternehmen“ (BKA 2021b:3). Insbesondere Unternehmen der kritischen Infrastruktur, wie Behörden der Regierung oder das Gesundheitswesen, wurden weltweit bereits in 2019 bevorzugtes Ziel von Angriffen. Das BKA vermutete dahinter die bewusste Ausnutzung der Notlage von Einrichtungen der kritischen Infrastruktur während der Corona-Pandemie, um so höhere Lösegeldforderungen zu erlangen (BKA 2020d:18) Die Schäden durch Ransomware gehen dabei in die Millionenhöhe. Im Jahr 2020 war bereits eine Steigerung erpresster Lösegelder um 311% auf eine Summe von 350 Mio. \$ zu verzeichnen (Abb. 44) (Grauer/Updegrave 2021:26).

Abb. 44 Total cryptocurrency value received by ransomware addresses per year - 2016 – 2020

Total cryptocurrency value received by ransomware addresses per year | 2016 - 2020



Quelle: Grauer/Updegrave 2021:26

Schätzungen von Emisoft zeigen dabei deutlich höhere Schadenssummen. Basis der Berechnung waren dabei die Anzahl der registrierten Schadensfälle und eine damit verbundene Hochrechnung

mit durchschnittlich gezahlten Lösegeldforderungen. Die weltweiten Schäden betragen demnach eine Mindestschadenssumme von 18.658.009.233 \$ und einer Schätzung der Höchstsumme von 74.632.036.933 \$ allein für die Zahlung von Lösegeldern im öffentlichen und privaten Bereich (Abb. 45) (Emisoft 2021a).

Abb. 45 Kosten für Lösegeld aufgeschlüsselt nach Ländern inkl. Privatanwender

Aufschlüsselung nach Land - inklusive Privatanwendern

Kosten nur für Lösegeld

Land	Gesamtanzahl der Einsendungen	Mindestkosten (USD)	Zweite Schätzung (USD)
USA	23 661	920 353 010 \$	3 682 228 067 \$
Italien	9 226	346 729 130 \$	1 387 389 097 \$
Spanien	8 475	298 254 459 \$	1 193 709 500 \$
Frankreich	7 824	283 816 080 \$	1 135 795 109 \$
Deutschland	7 138	252 609 210 \$	1 011 001 498 \$
Vereinigtes Königreich	4 788	169 182 845 \$	677 113 461 \$
Kanada	4 257	164 772 274 \$	659 246 267 \$
Australien	2 775	105 978 531 \$	424 034 780 \$
Österreich	1 254	46 643 868 \$	186 645 857 \$
Neuseeland	399	14 230 333 \$	56 951 495 \$
Gesamtkosten (alle Länder)	506 185	18 658 009 233 \$	74 632 036 933 \$

Quelle: Emisoft 2021a

Werden zusätzlich die Ausfallzeiten mitberücksichtigt, verursacht durch die Verschlüsselung und Dauer der Wiederherstellung der Daten, sind die Schadenssummen signifikant höher (Abb. 46) (Emisoft 2021a).

Abb. 46 Gesamtkosten + Lösegeld

Gesamtkosten: Lösegeld + Ausfallzeiten

Land	Gesamtanzahl der Einsendungen	Mindestkosten (USD)	Zweite Schätzung (USD)
USA	15 672	4 893 699 209 \$	19 574 796 838 \$
Frankreich	4 476	1 387 058 087 \$	5 548 232 346 \$
Spanien	4 088	1 272 238 829 \$	5 088 955 314 \$
Italien	3 835	1 198 933 932 \$	4 795 735 727 \$
Deutschland	3 747	1 159 985 450 \$	4 639 941 801 \$
Kanada	3 236	1 011 008 551 \$	4 044 034 203 \$
Vereinigtes Königreich	2 718	838 750 742 \$	3 355 002 968 \$
Australien	2 072	648 093 574 \$	2 592 374 295 \$
Österreich	819	256 822 720 \$	1 027 290 881 \$
Neuseeland	265	82 569 552 \$	330 278 209 \$

Quelle: Emisoft 2021a

Im zweiten Quartal 2021 erreichte die Angriffswelle mit Ransomware u.a. in den USA die kritische Infrastruktur mit hohen Lösegeldforderungen und lösten damit verstärkte Ermittlertätigkeiten aus (Emisoft 2021b). Die schwersten Angriffe waren dabei, geordnet nach Lösegeldsumme in Tab. 9 in den folgenden Branchen:

Tab. 9 Die größten Cyberangriffe 2021

Datum	Unternehmen	Branche	Lösegeldforderung
02.07.2021	Kaseya	IT-Management und Überwachung	70 Mio. \$
21.03.2021	CNA Financial	Versicherung	40 Mio. \$
09.06.2021	JBS	Fleischverarbeitung	11 Mio. \$
07.05.2021	Colonial Pipeline	Kraftstoffversorgung	4,4 Mio. \$
04.05.2021	ExaGrid	Backup-Speicherlösungen	2,6 Mio. \$

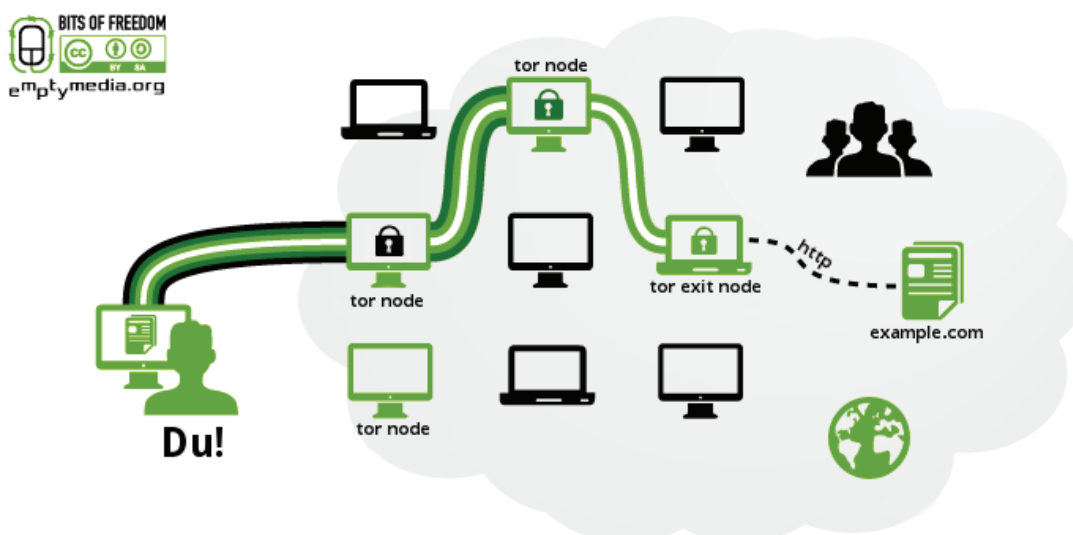
Quelle: eigene Darstellung in enger Anlehnung an Thielmann 2021

Der Angriff auf die Colonial Pipeline bewirkte einen sechstägigen Stillstand in den USA und löste einen Preisanstieg aus, welcher seit sechs Jahren nicht zu verzeichnen war. Aufgrund der Ermittlungsbemühungen und Serverbeschlagnahmungen war die verantwortliche Ransomware-Gruppe gezwungen aufzugeben. Eine weitere Folge weltweit war, dass sich mehrere Ransomware-Gruppen zurückzogen oder sich auf weniger große Ziele für ihre Angriffe einigten. Trotzdem konnte im zweiten Quartal 2021 weiterhin ein Anstieg verzeichnet werden (Emisoft 2021b). Angekündigt wurde zudem, dass künftig Kryptowährungen stärker reguliert werden sollen, um Angreifer:innen die Geschäftsgrundlage zu entziehen (Leisinger, C./NZZ, 14.05.2021). Sophos geht von einem weiteren Anstieg der Verwendung von Kryptowährungen im Jahr 2022 aus, da sich der Erhalt von Zahlungen durch kriminelle Aktivitäten mit ihnen verschleiern lassen. An erster Stelle stehen dabei Ransomware sowie Cyberjacking, da diese direkte Zahlungen der Opfer an die Täter garantieren (SophosLabs/Sophos Managed Threat Response/Sophos Rapid Response 2021:25)

6.3.2 Waffen-, Drogen-, Dokumenten- und Datenhandel, Gewalt- und Mordaufträge im Deep Web und Darknet

Wie bereits geschildert, ist das Darknet ein Teil des DeepWeb, welches nicht durch gewöhnliche Browser erreichbar ist und auf eine hohe Anonymisierung sämtlicher Daten setzt. Aufgrund seiner erschwerten Erreichbarkeit und hohen Anonymisierung wird es u.a. auch als „hidden services“ (Henkel 2020:176) bezeichnet. Erreichbar ist das Darknet mittels des Tor-Internetbrowser, auch „The Onion Router“ (Henkel 2020:176) genannt, welcher offiziell im Internet als Download zur Verfügung steht* (Henkel 2020:175 f.). Bei Standard-Internetbrowsern wird die Erreichbarkeit der Internetseiten durch den jeweiligen Internetprovider realisiert, wodurch gleichzeitig die IP-Adresse des Nutzenden und die Nachverfolgung der besuchten Seiten erfasst wird. Im Tor-Netzwerk hingegen wird diese Verbindung über drei randomisierte Knoten aufgebaut. Jeder Knoten bekommt dabei nur vom anderen Knoten die Herkunft der Verbindung mitgeteilt (Abb. 47). Die Knotenpunkte werden daher auch als eine Art Schale einer Zwiebel angesehen und waren somit namensgebend für den Tor-Browser. Vorteil dieser Praxis ist es, dass keine IP-Adresse einem Nutzenden zugeordnet werden kann und dadurch eine Anonymität gewährleistet wird (Henkel 2020:177).

Abb. 47 Wie das Tor-Netzwerk funktioniert



Quelle: emptymedia.org. 06.01.2015. <https://mtmedia.org/manuals/wie-funktioniert-tor/>. abgerufen am 05.12.2021

Mit dem Tor-Browser können normale Webseiten aufgerufen werden, möglich ist aber zusätzlich das Erreichen von versteckten Webseiten im Darknet. Diese Domains enden auf .onion und sind

* <https://www.torproject.org/download/>

ausschließlich mit diesem Browser erreichbar. Die hidden services garantieren damit, dass weder die Betreiber dieser Seiten noch Standorte der betriebenen Seiten auffindbar sind und somit eine hohe Anonymität garantieren. Henkel bezeichnet Tor deshalb als „digitale Sturmhaube“ (Henkel 2020:178), welche den normalen Nutzenden aber auch Kriminellen als Identitätsschutz dienen kann (Henkel 2020:177 f.). Aber nicht nur im Darknet sind illegale Inhalte auffindbar. Bereits im Jahr 2011 erhielt der Drogenhandel via Internet durch die Eröffnung der Webseite Silk Road eine höhere Bedeutung. Vor 2011 war nur vereinzelt der Drogenhandel im Internet feststellbar. Silk Road war erstmalig eine große Handelsplattform, ähnlich den bekannten Plattformen wie Amazon oder Ebay. Über Silk Road erfolgte sowohl der Handel der Drogen als auch die Bezahlung dieser. Aber nicht nur Drogen waren verfügbar. Das Angebot der Seite enthielt auch verschreibungspflichtige Medikamente, Dokumentfälschungen, Anleitungen zum Hacken, Plagiate bekannter Marken oder Pornografie. Jedoch bestand die Administration der Seite darauf, dass unter keinen Umständen Offerten mit Kinderpornografie angeboten werden durften. Die Sperrung der Seite erfolgte im Oktober 2013 durch das Federal Bureau of Investigation (FBI), jedoch entstanden kurz darauf neue Plattformen (Tzanetakis 2019:478). Eine Listung aktueller Plattformen befindet sich bspw. auf der Internetseite DarknetStats (App. 18) im Clearweb. Diese sind jedoch weitergehend nur über das Tor-Netzwerk abrufbar. Von den Kryptomärkten sind hingegen einzelne Anbieter im Darknet zu unterscheiden, welche sich oftmals auf die Veräußerung bestimmter illegaler Güter spezialisieren und konzentrieren. Verfügbare Links sind bspw. im Clearweb über „The hidden Wiki“ (App. 19, App. 20) erhältlich. Neben dem Waffenhandel (App. 21; App. 22), Dokumentenhandel wie Ausweise oder Staatsbürgerschaften (App. 23; App. 24), Hacker-Services (CCaaS) (App. 25), gehackte Accounts für alle möglichen Seiten wie bspw. PayPal; Ebay; Bank Accounts (App. 26), digitale Geldwäsche (App. 27; App. 28) werden auch in umfangreichem Maße Drogen wie bspw. Cannabis und Kokain angeboten (App. 29, App. 30, App. 31, App. 32). Allerdings ist hier nicht festzustellen, ob es sich bei diesen Seiten oder Anbietern um bewusst ausgelegte Seiten von Strafverfolgungsbehörden handelt. Die bereits beschriebenen Marktplattformen werden als Kryptomärkte bezeichnet, da sie eine Kombination aus „Anonymisierungssoftware und virtuellen Währungen“ (Tzanetakis 2019:478) darstellen. Bevorzugte Bezahlungsmethoden sind hier Bitcoin oder Monero unter Ausnutzung der Dezentralität und erschwerter Nachverfolgbarkeit, da kein direkter Bezug auf die Identitäten der an den Transaktionen Teilnehmenden hergestellt werden kann. Bitcoins unterliegen zwar einer gewissen Nachvollziehbarkeit aufgrund der Speicherung in der Blockchain, jedoch kann die Verbindung zwischen der Identität des Zahlungsempfängers und der erhaltenen Kryptowährung verschleiert werden wie bspw. bei dem Umtausch von Kryptowährungen in Fiat Geld. Die Kombination aus Dezentralität und erschwerter Nachverfolgbarkeit gewährt damit einen „systematischen Drogenhandel im Internet“ (Tzanetakis 2019:479). In einer Studie wurde festgestellt, dass, bezogen auf den Kryptomarkt Silk Road, Drogen im Wert von 15 Mio. \$ im Jahr 2012 umgesetzt wurden. Eine weitere Studie ergab im Jahr 2013, dass der Umsatz bereits auf über 100 Mio. \$ angestiegen war, dieser jedoch nach einer weiteren Steigerung im Jahr 2014 auf gleichbleibendem Niveau stagnierte. Vermutungen legen nahe, dass ca. ein Viertel der dort umgesetzten Drogen später auf realen Märkten auffindbar sind. Es konnte jedoch nicht festgestellt werden, ob die Drogen für den Konsum oder zur Weiterveräußerung bestimmt waren (Tzanetakis 2019:480 f.). Mehrere Studien untersuchten weiterhin den Erfolg der Drogenmärkte im Internet. Zum einen kamen sie zu dem Ergebnis, dass sich mit der Vergrößerung des Marktes im Internet keine erhöhte Sichtbarkeit ergibt. Hier muss demnach keine Abwägung zwischen dem Entdeckungsrisiko und einer Sichtbarkeitsvergrößerung aufgrund steigender Transaktionen vorgenommen werden (Tzanetakis 2019:482 f.). Der ökonomische Ansatz unterteilt in Bezug auf die Abwägung zwischen Entdeckungsrisiko und Sichtbarkeit Drogenmärkte in drei verschiedene Kategorien, offene; semi-offene und geschlossene Märkte (Tab. 10) (Tzanetakis 2019:482).

Tab. 10 Marktformen im Drogenhandel

Marktform	Sichtbarkeit	Entdeckungsrisiko	sozialer Kontakt
offen	hoch - Vertrieb der Drogen in der Öffentlichkeit wie bspw. Parks	hoch	hoch - persönlicher Kontakt zum Verkäufer erforderlich
semi-offen	verringert - Vertrieb in nicht-öffentlichen Einrichtungen wie bspw. Clubs	verringert	kein persönlicher Kontakt notwendig
geschlossen	nochmals verringert - Markt nur zugänglich, wenn Vorhandensein eines besonderen Vertrauensverhältnisses zwischen den Teilnehmenden	verringert - sichere Übergabe der Drogen	persönlicher Kontakt notwendig

Quelle: eigene Darstellung in enger Anlehnung an Tzanetakakis 2019:482 f.

Tzanetakakis ordnet Kryptomärkte in Bezug auf den Drogenhandel in die semi-offenen Märkte ein, da eine erhöhte Sichtbarkeit nicht unbedingt zu einem Entdeckungsrisiko führen muss. Erreicht wird dies durch die Anonymisierung bzw. Verschleierung von Identitäten und Standorten der Teilnehmenden. Für eine strafrechtliche Verfolgung durch Ermittlungsbehörden ist hier also nicht entscheidend, wie viele Teilnehmende ihre Drogen auf dem Markt anbieten. Weiterhin sind weder für den Vertrieb noch für den Erwerb persönliche Beziehungen notwendig (Tzanetakakis 2019:483). Weitere Vorteile von Kryptomärkten sieht Tzanetakakis in der „Reichweite und Verfügbarkeit“ (Tzanetakakis 2019:483) von Kryptomärkten. Einschränkungen in Bezug auf geografische Gegebenheiten materieller Drogenmärkte sind bei Kryptomärkten nicht vorhanden, der Handel kann weltweit stattfinden. Auch die angebotene Vielfalt an Gütern kann im Gegensatz zu materiellen Märkten weit höher sein. Eine Beschränkung der jeweiligen Vielfalt oder Versendungsort unterliegt nur dem jeweiligen Handelnden unter Abwägung der angebotenen Ware oder eines Versendungsrisikos durch etwaige Kontrollen. Diese Vorteile sind aus Sicht Tzanetakakis nicht auf Drogen beschränkt, sondern gelten für alle auf den Kryptomärkten gehandelten illegalen Güter (Tzanetakakis 2019:484). Ein weiterer wichtiger Punkt spielt das Vertrauen auf Kryptomärkten. Auf materiellen Märkten wird Vertrauen durch den persönlichen Kontakt aufgebaut, welcher bei Kryptomärkten nicht vorhanden ist. Gelöst wird es dadurch, dass das persönliche Vertrauen zwischen den Agierenden gegen einen „institutionsbasierendes Vertrauen“ (Tzanetakakis 2019:485) getauscht wird. Dies wird zum einen durch ein Bewertungssystem, basierend auf ein Kundenfeedback, sowie durch die Wahl der Zahlungsmöglichkeiten auf Kryptomärkten erreicht. Kundenfeedbacks können anonymisiert bezüglich der Qualität der Güter, vereinbarte und tatsächlich gelieferte Menge, Dauer der Lieferungen bis hin zur Verpackungsqualität in Bezug auf Verschleierung abgegeben werden und sind mit Hilfe eines Notenratings und Inhalt des Kundenfeedbacks für die Marktteilnehmenden sichtbar. Als Bezahlsysteme haben sich drei Formen, dargestellt in Tab. 11, herausgebildet (Tzanetakakis 2019:485):

Tab. 11 Zahlungsformen auf Kryptomärkten

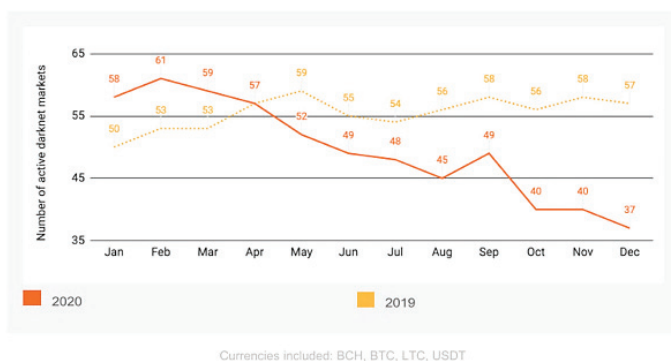
Form	Ablauf	Vorteil	Nachteil
centralised escrow	Treuhandverfahren - Kryptowährung wird vom Treuhandkonto erst nach Erhalt der Ware freigegeben	Besteller erhält die Ware, bei Konflikten Güterverhandlung zwischen Besteller und Handelndem	Treuhänder könnte Zahlungsbetrag einbehalten
finalized early	Zahlungsbetrag wird vor Versand überwiesen	Handelnde erhält Zahlungsbetrag	Bestellende erhält Ware nicht
multi-signature	von mehreren Agierenden Signierung für die Freigabe des Zahlungsbetrags notwendig	Agierende erhalten Zahlungsbetrag und Ware	technisch sehr anspruchsvoll, daher kaum verwendet

Quelle: eigene Darstellung in enger Anlehnung an Tzanetakakis 2019:485

Die Kombination aus Kundenfeedback und Zahlungsmöglichkeit gewährleistet einen Vertrauensaufbau zwischen den Agierenden und setzt somit keine persönliche Kenntnis untereinander voraus.

Ein Anzeichen für das vorhandene Vertrauen könnte bspw. der Fakt sein, dass nach der Schließung der Plattform Silk Road durch Behörden zahlreiche neue Marktplätze entstanden. Die Umsatzzahlen fielen zwar um die Hälfte aufgrund dieser Schließung, jedoch erholten sich die Märkte innerhalb weniger Wochen wieder. Tzanetakis sieht das als ein Indiz für den Aufbau des Vertrauens mit Hilfe von Zahlssystemen und Nutzerbewertungen (Tzanetakis 2019:486). Ein weiterer Grund für diese Art von Beständigkeit der Kryptomärkte sehen Soska und Christin in dem Bestehen der Nachfrage nach den gehandelten Gütern wie bspw. Drogen. Weder eine Schließung solcher Plattform noch ein Verbot der nachgefragten Substanzen haben bisher dauerhaft Wirkung erzielen können. Auch ein Verbot von Netzwerken, welche eine Anonymisierung garantieren, als Ultima Ratio hätte keine Auswirkungen, denn dann würden die Agierenden auf andere Formen des Handels ausweichen. Hier sollte das Augenmerk eher auf die Verhinderung oder Verminderung der Nachfrage durch präventive Maßnahmen gelegt werden (Soska/Christin 2015:47). Laut Bericht von Europol aus dem Jahr 2021 haben die Verwendung des Deep bzw. Dark Web und Kryptowährungen unlängst die OK erreicht. Die Verwendung moderner Technologien bezeichnet Europol dabei als „[...] Hauptmerkmal der schweren und organisierten Kriminalität im Jahr 2021“ (Europol 2021:11). Inzwischen nutzt die OK Verschlüsselungen in der Kommunikation, Social Media, sowie das Internet für den Handel ihrer Güter. Hauptschwerpunkte bilden u.a. Drogen-, Eigentums- und Mehrwertsteuerdelikte sowie Online-Betrugsdelikte und Menschenhandel (Europol 2021:12). In Bezug auf die Kriminalität ist festzustellen, dass jegliche Delikte einen Online-Anteil besitzen, manche Delikte sind vollständig ins Internet verlagert worden. Die OK nutzt Online-Marktplätze für ihre Güter im Darknet und Surface Web, zusätzlich bieten diese anonymisierte Kommunikationskanäle und Bezahlmethoden (Europol 2021:15). Selbst die Beauftragung gewalttätiger Delikte wird auf Online-Märkten im Darknet angeboten. Diese bestehen aus „[...] Drohungen, Einschüchterung, Vandalismus und Überfällen bis hin zu Entführung, Folter, Verstümmelung und Mord“ (Europol 2021:22) und entwickelt sich derzeit zu einem selbständigen Zweig in der OK (Europol 2021:22). Auch im Bereich der Korruption spielen Kryptowährungen aufgrund der zunehmenden Veränderungen in der Verwendung von Technologien zunehmend eine Rolle. Aber nicht nur in der Zahlung von Beträgen in Kryptowährungen an korrumpierte Amtsinhaber liegt hier ein Vorteil in der Verwendung von Technologien. Mit wachsender Digitalisierung gelingt es zunehmend Amtsinhaber dahingehend zu beeinflussen, Einfluss auf Entscheidungsprozesse in digitalisierten Systemen durch manipulative Delikte auszuüben oder an gewünschte Informationen zu erlangen (Europol 2021:26). Verschiedene Ermittlungserfolge belegen das Ausweichen auf Kryptomärkte, die Verwendung von Kryptowährungen und modernster Technik sowie die weltweite Vernetzung des organisierten Verbrechens. Bspw. wurde am 16.06.2020 bei der Verhinderung der Operation „Acquarius“ (Direzione Investigativa Antimafia (DIA) 2020:56) durch italienische Behörden festgestellt, dass für die Kommunikation innerhalb der Tätergruppe sogenannte Kryptophone (Mobiltelefone mit Verschlüsselung) verwendet wurden. Damit war es nur der Tätergruppe möglich untereinander zu kommunizieren. Die Täter stammten dabei aus verschiedenen Regionen Italiens wie bspw. Kalabrien, Florenz oder Sizilien und gehörten zu dem Clan der Morabito-Palmara-Bruzzaniti. Die Kryptophone erlangten sie über einen albanischen Steward und die 505 kg Kokain, auf die sich der Deal bezog, wurden in Spanien beschlagnahmt welches durch ein Schiff aus Brasilien angeliefert wurden. Dabei war das gelieferte Kokain nur ein Teil eines ausgehandelten Deals zwischen den Beteiligten, denn ursprünglich sollten große Mengen regelmäßig geliefert werden und waren für Märkte in den Regionen der Toskana und Emilia-Romagna bestimmt (DIA 2020:56). Ein anderer Fall bestätigt den Drogenhandel mit synthetischen Drogen, welche im Darknet veräußert und mit einem unbaren Bezahl-dienst erworben wurden. Der erzielte Erlös wurde anschließend in Bitcoin umgewandelt (DIA 2020:348). Inzwischen setzen italienische Mafia-Organisationen auf Kryptowährungen wie Bitcoin und Monero und die Nutzung des Deep und Dark Webs, allen voran die stärkste Mafia-Organisation in Italien, die 'Ndrangheta unter Ausnutzung der Anonymität (Klein/OCCRP 2021). Nach einer Analyse ist derzeit ein Abnehmen in der Anzahl der Kryptomärkte feststellbar. Im Dezember 2020 waren lediglich noch 37 von 61 Marktplätzen online (Abb. 48) (Grauer/Updegrave 2021:57).

Abb. 48 Number of active darknet markets - 2019 vs. 2020



Quelle: Grauer/Updegrave 2021:57

Die Ursachen dafür sind vielfältig. Zum einen konkurrieren die Märkte untereinander stark und bekämpfen sich gegenseitig mit Denial-of-Service-Attacks (DoS). Zum anderen kommt hier Betrug in Betracht, bei dem sich die Administratoren die Kryptowährungen aneignen und entweder den Markt für die Erzielung weiterer Einnahmen bestehen lassen oder ihn schließen. Ware wird dabei jedoch nicht ausgeliefert (sogenannte Exit-Scams). Ein weiterer Grund ist die durch Corona-Krise verursachte Unterbrechung der Lieferketten, welche dem Versand der bestellten Güter erhebliche Behinderungen bereitete und Märkte zwang zu schließen. Dokumentiert wurde dies in Beschwerden im Bewertungssystem der Märkte (Grauer/Updegrave 2021:58). Chainalysis sieht hier als Hauptursache die Konsolidierung des Marktes, d.h. ein Schrumpfen der Anzahl der Märkte wie bei Technologieunternehmen. Schon deshalb und durch den Druck von Ermittlungsbehörden wird es zu weiteren Schließungen kommen (Grauer/Updegrave 2021:60). Jedoch könnten sich neue Vertriebsformen wie bspw. Televend zunehmend herausbilden. Televend ist eine Plattform mit über 150.000 Mitgliedern und basiert auf dem Messenger Dienst Telegram. Die Kommunikation zwischen den Beteiligten unterliegt einer hohen Verschlüsselung. Angeboten werden Drogen mit Hilfe automatisierter Chatbots und die Bezahlung erfolgt mit BTC an automatisch erzeugte BTC-Adressen. Für die Vermittlung zwischen den Beteiligten wird eine Provision an Televend ausbezahlt. Televend hat dabei jedoch nie direkten Zugriff auf die an den Veräußernden gezahlten Summen. Selbst Blockchain-Analysen durch die Ermittlungsbehörden führen nicht zum Erfolg, da es keine zentrale Stelle gibt, an der die Zahlungen zusammenlaufen könnten. Das erhöht die Anonymität und Sicherheit der Transaktionen beträchtlich. Chainalysis untersuchte den Verlauf eines Händlers auf dieser Plattform und stellte fest, dass seit dem Betreiben des Accounts über 270.000 \$ durch ca. 500 Transaktionen erzielt wurden. Die nähere Untersuchung dessen Wallet ergab, dass bereits vor dem Teilnehmen an Televend Transaktionen im Wert von 1,4 Mio. \$ stattgefunden haben. Das lässt den Schluss zu, dass der Betreibende vor der Nutzung von Televend bereits auf Kryptomärkten aktiv war und von dort aus zu Televend wechselte. Inzwischen hat sich die Zahl der Veräußernden auf 150 erhöht. Chainalysis nimmt an, dass der Anteil aufgrund der starken Dezentralisierung weiter zunehmen wird, denn die Marktkonkurrenz der Veräußernden und der Druck durch Ermittlungsbehörden sind gering (Grauer/Updegrave 2021:61 f.). Weiterhin wurde festgestellt, dass zunehmend anonyme Kryptowährungen an Bedeutung gewinnen. Insbesondere Monero hat sich dabei auf Darknet-Marktplätzen fest etabliert (Europol 2020:58).

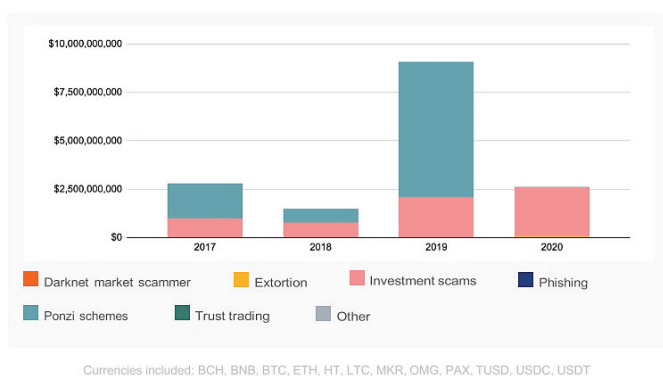
6.3.3 Kriminalität gerichtet auf Kryptowährungen - Hacken und Exit-Scam von Kryptobörsen, Raubüberfälle

Unter Hacken ist ein illegaler Einbruch in Systeme oder die unerlaubte Nutzung dessen zu verstehen (Pawlik 2018:36). In einer Analyse der Dekade der Jahre 2011-2021 kamen Charoenwong und Bernadi unter Annahme, die entwendeten Kryptowährungen unterlägen nicht dem sofortigen Umtausch in Fiat-Währungen und der restriktiven Betrachtung von Vorkommnissen in denen die erbeutete Summe $\geq 1.000.000$ \$ betrug, zu folgendem Ergebnis (Charoenwong/Bernadi 2021:3). Insgesamt wurden in der Dekade 24 Fälle unterteilt in drei Kategorien verzeichnet:

- Eindringen durch Sicherheitslücken (Security Breach)
- Hacken durch die Ausnutzung menschlichen Fehlverhaltens (Human Error) und
- Zuarbeit durch Insider (Agency Problem) (Charoenwong/Bernadi 2021:3).

Der Schaden beläuft sich, abhängig nach der Dauer des Haltens der Kryptowährungen und Nichtumtausch in Fiat-Währungen, berechnet auf Basis des Bitcoin-Kurses mit vom Stand Oktober 2021 auf 85 Milliarden \$. Im Vergleich dazu erzielt das mexikanische Drogenkartell ca. 13 Milliarden \$ per anno. Die größte Anzahl der Kryptohacks wurden durch die Ausnutzung von Sicherheitslücken erreicht (App. 33). Vorausgesetzt, die erbeuteten Kryptowährungen wären sofort in Fiat-Währungen getauscht worden, belief sich die Summe auf 9,8 Milliarden \$. Insgesamt lässt sich somit feststellen, dass der Schaden in Abhängigkeit der Umtauschaffinität der insgesamt 1.264 Mio. gestohlenen BTC zwischen 9,8 und 85,7 Milliarden beträgt (Charoenwong/Bernadi 2021:6). Festzustellen sind weiterhin sowohl die Zunahme der Angriffe in den letzten zehn Jahren als auch die steigende Höhe der erbeuteten Kryptowährungen (Charoenwong/Bernadi 2021:1). Der bisher größte Hack mit einer Beute von 3,6 Milliarden \$ oder 69.000 BTC war der Raub bei der Kryptobörse Africrypt (App. 33, Nr. 23) im Juni 2021 (Charoenwong/Bernadi 2021:1). Anfangs wurde durch die Betreiber behauptet, die Börse wäre gehackt worden, mit dem Verschwinden der beiden Betreiber und 69.000 BTC deutet jedoch alles auf einen Exit-Scam hin (Stede, C./BTC-Echo 2021). In Aussicht auf künftige Diebstähle von Kryptowährungen gehen Charoenwong und Bernadi von einer steigenden Tendenz aufgrund steigender Werte derer aus (Charoenwong/Bernadi 2021:6). Bereits im Jahr 2020 wurde durch Chainalysis ein steigender Trend im Diebstahl von Kryptowährungen beobachtet. Lag die Schadenssumme im Jahr 2019 noch bei 343,7 Mio. \$, steigerte sie sich im Jahr 2020 bereits auf 523,3 Mio. \$. Auch der Trend der steigenden Anzahl von Angriffen wurde identifiziert. Hier lag die Anzahl der Angriffe bei 86 während im Vorjahr lediglich 24 festgestellt werden konnten (Grauer/Updegrave 2021:82). In Bezug auf Betrug (Exit-Scam ausgeschlossen) sind dagegen sinkende Einnahmen zu verzeichnen. Im Jahr 2020 sank die Summe aller erbeuteten Kryptowährungen von 9 auf 2,7 Milliarden \$. Die Anzahl der Opfer stieg jedoch im Gegenzug um 48%. Der Grund für die starke Abnahme im Jahr 2020 war, dass im Jahr 2019 allein 7 Milliarden \$ an Kryptowährungen durch sogenannte Ponzi-Schemata vorwiegend im asiatischen Raum erbeutet werden konnten (Abb. 49) (Grauer/Updegrave 2021:71). Ponzi-Schemata sind Schneeballsysteme, bei denen neue Anleger mit hohen Verzinsungen von Guthaben angelockt werden, welche durch bereits vorhandene Guthaben bestehender Anleger befriedigt werden. Dieses Schneeballsystem wurde nach Charles Ponzi benannt, welcher in den 20er Jahren Betrug in dieser Form betrieb (Herger 2016:148). Die 7 Milliarden \$ konnten allein durch sechs dieser Ponzi-Schemata erbeutet werden. Nach diesem Betrug kam es zu Verhaftungen von 109 Personen durch chinesische Behörden, so das anzunehmen ist, dass zum einen Betrügende davon abgeschreckt und zum anderen Menschen vor dem Anlagebetrug öffentlich gewarnt wurden (Grauer/Updegrave 2021:72) und damit ein Rückgang zu verzeichnen war. Wie in Abb. 49 zu erkennen ist, nahm im Gegenzug der Abnahme von Ponzi-Schemata der Investmentbetrug zu.

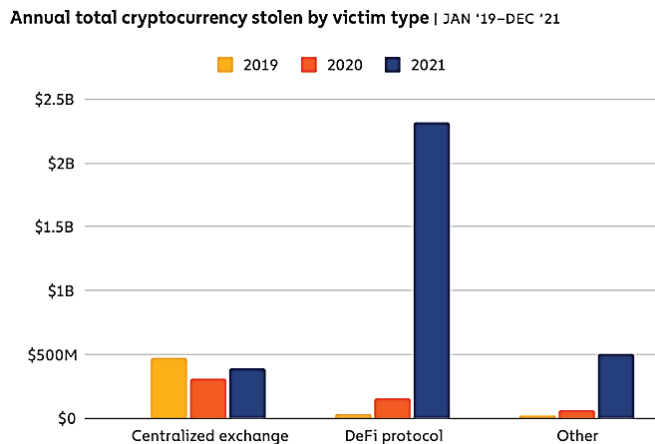
Abb. 49 Total Cryptocurrency value received by scam category



Quelle: Grauer/Updegrave 2021:72

Die Schadenssumme durch Diebstahl von Kryptowährungen belief sich im Jahr 2020 auf annähernd 162 Mio. \$ in Bezug auf Börsen und verzeichnete damit einen Anstieg von 335% im Verhältnis zum Vorjahr. Im Jahr 2021 wurde ein erneuter starker Anstieg um 1.330% verzeichnet (Abb. 50) (Grauer/Kueshner/Updegrave 2022:6).

Abb. 50 Annual total cryptocurrency stolen by victim type - Jan 2019 - Dec 2021



Quelle: Grauer/Kueshner/Updegrave 2022:6

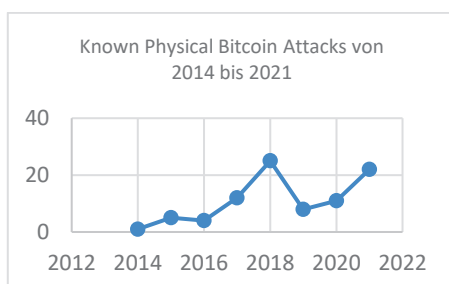
Der Diebstahl von Kryptowährungen ist aber nicht nur im digitalen Bereich festzustellen. Auch im Bereich des analogen Verbrechens sind bereits mehrere Fälle zu verzeichnen. Bei ihnen handelt es sich um physische Angriffe auf Personen, bspw. durch Entführungen, Gewaltandrohungen, Folterungen und Mord, sowie auf Technik wie bspw. Kryptoautomaten, um an die Kryptowährungen zu gelangen. Eine Analyse der bei GitHub verfügbaren Seite „Known Physical Bitcoin Attacks“ führt dabei zu folgenden Ergebnissen. Die Anzahl der Angriffe stieg kontinuierlich bis zum Jahr 2018 an. Nach einem kurzen Abfall im Jahr 2019 ist erneut ein hoher Anstieg zu verzeichnen (Tab. 12, Abb. 51).

Tab. 12 Known Physical Bitcoin Attacks

Jahr	Anz. d. Angriffe
2014	1
2015	5
2016	4
2017	12
2018	25
2019	8
2020	11
2021	22

Quelle: eigene Darstellung in enger Anlehnung an GitHub 2021. abgerufen am 18.12.2021

Abb. 51 Known Physical Bitcoin Attacks 2014-2021



Quelle: eigene Darstellung in enger Anlehnung an GitHub 2021. abgerufen am 18.12.2021

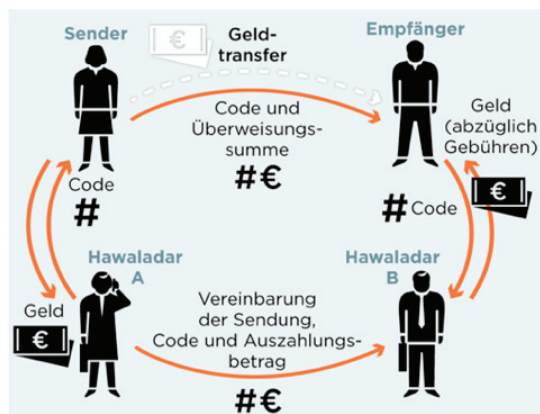
Die bei den Überfällen erbeuteten Summen belaufen sich dabei bei den aufgeführten Fällen auf 10.000 \$ bis 10 Mio. \$ (GitHub 2021). Dabei listet die Webseite jedoch nicht alle weltweiten Fälle auf. Auch in Deutschland wurde bereits in München im Frühjahr 2021 ein Fall des physischen Diebstahls verzeichnet. Dabei wurde durch drei Täter ein entsperartes Smartphone unter Anwendung von Gewalt entrissen. Auf diesem befanden sich in einer Bitcoin-Wallet ca. 2 BTC mit einem umgerechneten Wert von 100.000 € (Bernstein 2021).

6.4 Die Verwendung von Internet und Kryptowährungen durch den internationalen Terrorismus und Extremismus

Rogoff erklärte Kryptowährungen in einem Interview zu einem „Fluch schlimmer als Bargeld“ (Rogoff 2021). Aufgrund ihrer Anonymität und schweren Nachvollziehbarkeit seien sie dazu prädestiniert, Steuern zu hinterziehen und würden dazu dienen, kriminelle und terroristische Delikte zu begehen, so „[...] dass sich Banknoten mit hohem Nennwert dagegen vergleichsweise harmlos ausnehmen“ (Rogoff 2021). Malik zählt in einem Bericht die Risiken der Verwendung des Internets und Kryptowährungen sowie die Benutzung von Verschlüsselungstechnologien durch terroristische Vereinigungen auf. Laut diesem Bericht benutzen Terroristen bereits verstärkt das Darknet aus Gründen der Strafverfolgung für die Planung von Anschlägen sowie verschlüsselte Kommunikationen über entsprechende Messenger wie bspw. Telegram. Weiterhin gibt es zunehmend Anzeichen dafür, dass über das Darknet Rekrutierungen vorgenommen werden. Weiterhin wird das Darknet für Propagandazwecke genutzt. Kryptowährungen werden bei terroristischen Vereinigungen bevorzugt zur Mittelbeschaffung verwendet. Dabei werden sowohl Überweisungen als auch Spendenaufrufe im Darknet unter Ausnutzung dezentralisierter Netzwerke genutzt, um eine Be- oder Verhinderung ihrer Operationen auszuschließen, die ihnen bei zentralen Netzwerken durch Aufsichtsbehörden drohen würde (Malik 2018:IV). Oftmals ist die Korrelation von Darknet und Terrorismus nicht erkennbar vorhanden. Insbesondere nicht-terroristische Delikte wie bspw. Drogenhandel stützen dabei Finanzierungen von terroristischen Vereinigungen. Allerdings nimmt die Offensichtlichkeit der Annäherung weiter zu. Inzwischen ist bestätigt, dass sich Terroristen u.a. mit Hilfe von Prostitution, Organhandel, Waffen- und Antiquitätenverkäufe, Menschenhandel und der Besteuerung von Schmuggelrouten finanzieren. Meist geschieht dies in Konfliktländern wie bspw. im Irak oder in Syrien. Terroristen in Europa hingegen finanzieren sich über Veräußerungen von Bedienungsanleitungen, Waffen oder Waffenteilen, gefälschten Dokumenten und Drogen im Darknet. Oftmals überschneiden sich beide Bereiche der Finanzierung. So können Drogen, welche aus dem Irak geschmuggelt wurden im Darknet in Europa veräußert werden. Gefälschte Dokumente hingegen können Verwendung in der Unterstützung für die Logistik von Terroristen finden, wie auch die im Darknet gehandelten Waffen für Anschläge (Malik 2018:31). Direkt hergestellte Zusammenhänge zwischen dem Erwerb von Schusswaffen aus dem Darknet und terroristischen Anschlägen gibt es nur wenige. Bspw. soll der Anschlag in Paris auf einem Konzert im November 2015 mit Sturmgewehren aus dem Darknet verübt worden sein. Dabei führten die Spuren zu einem Veräußerer aus Stuttgart. Von Seite der Staatsanwaltschaft liegt bis dato die Betätigung vor, dass die Sturmgewehre von einem Veräußerer mit dem Nutzernamen „DW Guns“ aus dem Darknet bezogen wurden. Bis heute liegt jedoch weder ein Dementi noch eine Bestätigung durch deutsche oder französische Behörden vor. Auch bei dem Anschlag in München im Juli 2016 mit rechtsextremistischem Hintergrund wurden die Waffen im Darknet erworben (Malik 2018:34 f.). Eisermann stellt eine zunehmende Gefahr der Finanzierung des Terrorismus unter Verwendung von Kryptowährungen fest. Gründe für die Verwendung derer sieht Eisermann im unkomplizierten Umgang und Vollzug von Transaktionen (Eisermann 2020:24 f.). Malik sieht einen weiteren Grund in der Ähnlichkeit in der Verwendung der Kryptowährungen zu Transfers mit Hilfe des Hawala-Netzwerkes (Malik 2018:37). Hawala-Netzwerke als „alternative Überweisungssysteme“ (Wahlers 2013:96) entwickelten sich ursprünglich in Ost- und Zentralasien sowie im Vorderen Orient. Gründe dafür waren das Nichtvorhandensein von Bankensystemen oder die nicht vorhandene Effizienz dieser (Wahlers 2013:95). Das Versenden und Ausgeben von Geld erfolgt über die Hawaladare. Bezogen auf Abb. 52 würde das Geld vom Versender und unter Übergabe eines Codes bei Hawaladar A eingezahlt. Dieser Code wird

an Hawaladar B übermittelt, welcher dem Empfänger unter Angabe des richtigen Codes den Empfang bestätigt und den Betrag auszahlt (Maisch/Keuchel 2019). Es findet hier also kein realer Geldfluss statt (Wahlers 2013:96).

Abb. 52 Das Hawala-System



Quelle: Maisch/Keuchel 2019. abgerufen am 20.12.2021

Hawala-Systeme werden aufgrund ihrer Funktionsweise in mehreren Ländern als Finanzierungsmöglichkeit für Terrorismus und für die Benutzung von Geldwäsche angesehen (FATF 2013a:10). Festgestellt wurde bspw., dass sowohl Al-Quaida als auch der Islamische Staat (IS) Hawala-Systeme für den Geldtransfer und Gehaltszahlungen verwendeten (Malik 2018:37 f.). Bis dato sind nur wenige Fälle der Verwendung von Kryptowährung als Finanzierung von Terrorismus bekannt (Eisermann 2020:24). Erste Anzeichen gab es im Jahr 2015, als ein Sympathisant des IS Ratschläge für die Verwendung von Finanzierungsmöglichkeiten mit Bitcoin via Twitter an den IS übermittelte. Die erste direkte Verwendung wurde im Jahr 2016 durch einen Spendenaufruf der Ibn Taymiyya Media Center (ITMC) - Medienorganisation des Mujahideen Shura Council (MSC) im Gazastreifen festgestellt. Die Einnahmen beliefen sich jedoch auf lediglich 0,929 BTC, was nach damaligem Kurs lediglich 540 \$ ausmachte. Im Jahr 2017 wurde eine Crowdfunding-Aktion von al-Sadaqh (Terrororganisation aus Syrien) bekannt. Genutzt wurden für den Spendenaufruf soziale Medien wie Twitter und der Messengerdienst Telegram. Wurde anfangs noch um Spenden in Form von BTC gebeten, wurden später auch Monero und Dash akzeptiert. Die Einnahmen beliefen sich dabei auf 0,075 BTC, umgerechnet 803 \$. Am Ende desselben Jahres unterstützte Zoobia Shahnaz, gebürtige Pakistani mit anerkannter US-Staatsbürgerschaft, den IS mit Spenden. Die annähernd 62.000 \$ erlangte sie mit Betrugsdelikten in BTC, welche sie später nach Umtausch in die Fiat Währung \$ an den IS überwies. Der Umtausch sollte dabei die Herkunft der Gelder verschleiern. Im Jahr 2018 wurde durch Malhama Tactical (Terrororganisation aus Syrien) ein Spendenaufruf in BTC veröffentlicht. Der Spendenlink wurde jedoch nicht veröffentlicht. Um diesen zu erhalten, bat die Gruppe um Kontaktaufnahme, um so die Transaktionen an die BTC-Adresse für Ermittlungen zu erschweren. Im Jahr 2019 wurden weitere Spendenaktionen durch die Kassam-Brigaden (Hamas aus Palästina) und dem IS bekannt. Neu war allerdings, dass die Spendenlinks bei jedem Seitenaufruf neu generiert und dadurch Spenden auch an verschiedene Wallets gesendet wurden, um so die Nachverfolgbarkeit zu erschweren. Die Hamas erzielte dadurch nach eigenen Angaben 7.400 \$, bei dem IS hingegen gehen Ermittler von mehreren 10.000 \$ pro Spendenaktion aus. Die größte bisher dokumentierte Verwendung von Kryptowährungen zur Finanzierung von Terror wurde im Jahr 2019 verzeichnet. Bei dem Anschlag in Sri Lanka mit Hilfe von Sprengstoffen am Ostersonntag wurden am Vortag 4.000.000 \$ in BTC an verschiedene Wallets an den IS überwiesen. Nach dem Anschlag fiel der Kontostand wieder auf die ursprünglich vorhandene Höhe von 500.000 \$ (Eisermann 2020:25 ff.). Im Jahr 2019 kommen Schwarz, Manheim und Johnston zu dem Schluss, dass keine der betrachteten Kryptowährungen die finanziellen Anforderungen von terroristischen Organisationen erfüllen können. Trotzdem könnten diese unter besseren Bedingungen für die Mittelbeschaffung wichtig

sein wie bspw. das Fundraising (Schwarz/Manheim/Johnston 2019:35). Trotz alledem wären derzeitige Bedenken, Kryptowährungen könnten für den Terrorismus dienlich sein, übertrieben. Langfristig gesehen könnte sich das jedoch durch Verbesserungen von Technologien ändern (Schwarz/Manheim/Johnston 2019:55). Eisermann kommt im Jahr 2020 hingegen dazu, dass die aufgeführten Beispiele der Finanzierungen nicht die letzten sein werden. Insbesondere die Verfeinerung der Anwendung durch die Terroristen hat gezeigt, dass Kryptowährungen sehr wohl für die Finanzierungen geeignet sind und eine Rückverfolgung aufgrund Verschleierungsaktivitäten kein Hindernis darstellt. Weiterhin können sich auch Kryptowährung als Wertaufbewahrungsmittel in Wallets und zum schnellen Umtausch in Fiat Währungen eignen und damit „[...] neben Bargeld zu einem zweiten Grundpfeiler der Terrorismusfinanzierung werden“ (Eisermann 2020:29). Das International Institute for Counter Terrorism (ICT) bestätigte im Jahr 2021 im Cyber Report Eisermanns Annahme. Beobachtet wurde bei mehreren Finanzierungen durch Kryptowährungen, dass sich die Taktik in Bezug auf die Verwendung von Spendenaufrufen verändert hat. Aufgrund der „Know Your Customer“-Richtlinie (ICT 2021:12), welche Kryptobörsen dazu zwingt, Transfers von und für Terrororganisationen abzulehnen, sind diese auf andere Möglichkeiten ausgewichen. Bspw. wurden private Adressen veröffentlicht, an die gespendet werden konnte. Weiterhin ist das Ausweichen auf die Kryptowährung Monero festgestellt worden (Abb. 53) (ICT 2021:12).

Abb. 53 ISIS schwenkt auf Monero um

whitestream - Blockchain Intelligence · 25. Juni 2020

Now it's official, #ISIS moved to @monero to raise funds from the public.

With the awareness we created worldwide, and thanks to our global collaborations, we were able to push ISIS out of the Bitcoin Blockchain

التحويل على حساب رايكس من الامم المتحدة ورسالة اربعة وسبعين من كلادي بالارد
 من كلادي وسبعين من كلادي
 هو قد تم تحديث طريقة التبرع الى
 تم تحديث طريقة التبرع ، التبع الخطوات بعناية
 آخر قس الله ، هذا التبرع للتوقف فقط لا يجوز التبرع من اموال الزكاة لولا فضل الله لم
 يبر عليكم كما استمر الموقع الى يومنا هذا
 تم تحديث صفحة التبرع الى حصة مزودو الخدمة التي انزلت الامم المتحدة على الموقعين، يعني ان من اراد التبرع لا يجوز ان يبر
 بالتبرع من اموال الزكاة لان الامم المتحدة من حوزان التبرع او حتى التبرع التي ارادتها، حتى ان التبرع بغيره خطية لا يتسلف له التبرع بها بعد
 ان التبرع الغير موافق

أخبار المسلمين
 موقع مستقل يعنى بأخبار المسلمين
 بروايات
 تقارير مسورة
 اخبار المسلمين العامة
 مسيرات
 التاريخ الهجري - يدافن الحداثة
 ارتداد الموقع في مساهمة الامم
 احداث طريقة اخرى لا تقدر على التبرع لغير
 المسلمين

WHAT IS MONERO?
 EXPLAINED SIMPLY AND IN PLAIN ENGLISH

whitestream - Blockchain Intelligence
 @whitestream5

ISIS updated their website on the 21.6.2020, saying that from now on the donation system will move to @monero.
 On the Bitcoin blockchain we can see that at same date, ISIS grouped together some of their latest donations.

Bitcoin address -
 38R62BMQG8WvYy8h6VhCQ8B2oYUkSB2PDK

1:25 nachm. · 25. Juni 2020

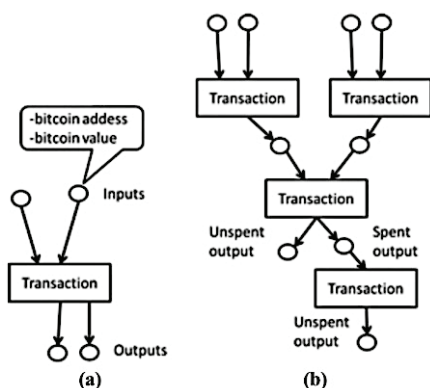
Quelle: Roos, A. be[in]crypto. Terrorfinanzierung: ISIS nutzt Monero statt Bitcoin. 26.06.2020. <https://de.beincrypto.com/terrorfinanzierung-isis-nutzt-monero-statt-bitcoin/>. abgerufen am 28.12.2021

Darüber hinaus konnten Terrororganisationen in denen von ihnen beherrschten Gebieten Wechselnrichtung eröffnen, um die Kryptowährungen in Fiat Währungen zu tauschen und eine Rückverfolgung der Mittel erschweren (ICT 2021:12).

6.5 Digitale Geldwäsche

BTC-Transaktionen bestehen aus verschiedenen vielen Vorgängen. Sie können sich aus mehreren Ein- und Ausgängen zusammensetzen (Abb. 54 (a)), wobei jeder Ein- und Ausgang über seine spezifische Adresse sowie Betrag verfügt. Zudem sind sie miteinander verlinkt, so dass die Transaktionen einer Nachverfolgbarkeit unterliegen (Abb. 54 (b)) (van Wegberg/Oerlemans/van Deventer 2018:423).

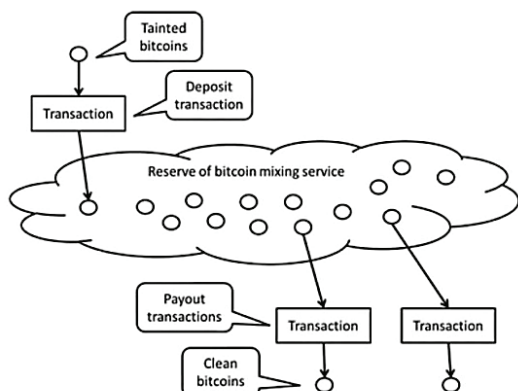
Abb. 54 Transaktionen mit BTC



Quelle: van Wegberg et al. 2018:423

Dieser Fakt hindert Kriminelle daran, die Transaktionen nach dargestelltem Schema durchzuführen, denn inkriminierte BTC wären jederzeit nachvollziehbar. Um die Kette der Nachverfolgbarkeit zu unterbrechen, wurde die Technologie des BTC-Mixens entwickelt. Wie in Abb. 55 dargestellt, weisen Bitcoin-Mixer den Einzahlenden eine neue Einzahladresse zu. Nach Zahlung einer Gebühr oder Provision erfolgt eine Rückauszahlung an die Einzahlenden. Die Auszahlung der Bitcoins erfolgt dabei aus einem Pool des Bitcoin-Mixer Anbieter, welcher zu diesem Zeitpunkt bereits besteht. Zudem werden die Auszahlungen zeitlich nach Zufall verteilt, um so eine adäquate Mischung zu garantieren. Nun besteht kaum noch eine Nachverfolgbarkeit der BTC, denn eine eindeutige Quelle der BTC ist nicht mehr gegeben. Zusätzlich kann der Empfangende die Korrektheit des Mixens auf der Internetseite blockchain.info checken. War der Mischvorgang erfolgreich, ist jede Korrelation von ein- und ausgezahlten BTC nahezu ausgeschlossen. Um die Sicherheit für Dauerkunden zu erhöhen, erhalten diese nach jeder Mischung eine Nummer, die sie bei einem erneuten Mischvorgang angeben. Damit soll verhindert werden, dass an die Dauerkunden BTC ausgezahlt werden, welche sie bei einem vorangegangenen Mischvorgang eingezahlt haben. Somit eignet sich dieses Verfahren für inkriminierte Kryptowährungen aus Cyberdelikten (van Wegberg et al. 2018:423 f.).

Abb. 55 BTC-Mixer Service

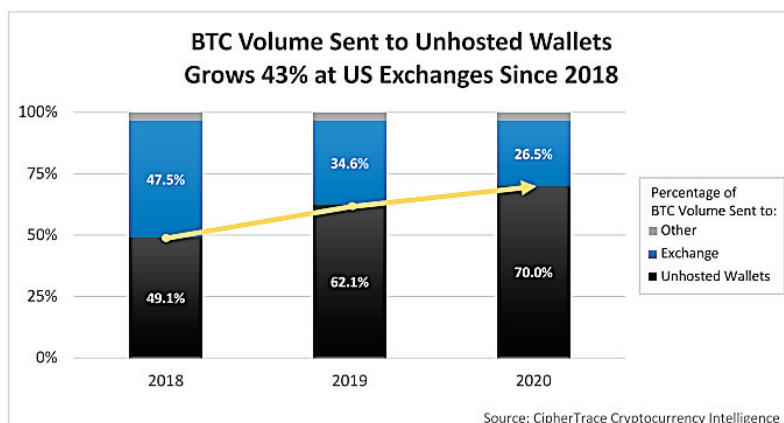


Quelle: van Wegberg et al. 2018:424

Im Jahr 2012 warnte das FBI vor der zunehmenden Verwendung von dezentralisierten Kryptowährungen, schätzte jedoch zu dieser Zeit das Risiko von Geldwäschen als gering ein. Als Einschränkung ihrer Einschätzung ging das FBI jedoch davon aus, dass mit steigender Akzeptanz von Kryptowährungen fest mit einer Zunahme von Geldwäschen von virtuellen Währungen zu rechnen ist (FBI 2012:6 f.). Auch im Jahr 2015 wurde, wie bspw. in England, weiterhin das Risiko von Geldwäschen mit Kryptowährungen als gering eingestuft. Dabei wurden im selben Jahr bereits erste große Fälle der digitalen Geldwäsche bekannt. In den Niederlanden wurden mehrere Personen verhaftet, welche im Verdacht standen, annähernd 22 Mio. \$ mit BTC gewaschen zu haben (Brown 2016:332). Brown ging davon aus, dass Risiken in Bezug auf Geldwäsche durch Ermittlungsbehörden vernachlässigt wurden, obwohl Kryptowährungen bereits in großer Höhe für kriminelle Delikte in Verwendung waren. Als Gründe nennt er das Außerachtlassen der Risiken sowie zu komplexe ermittlungstechnische Tätigkeiten (Brown 2016:336). Bestätigt werden Browns Annahmen durch folgende Fälle. Im Jahr 2021 wurde ein 32-Jähriger wegen Geldwäsche in Los Angeles verhaftet. Dieser betrieb das bis dato größte Portal für Geldwäsche namens Bitcoin-Fog. Bei den Ermittlungen kam zutage, dass Gelder i.H.v. 1,2 Mio. BTC mit einem Marktwert von 53 Mrd. € im Zeitraum von über zehn Jahren gewaschen wurden. Die Gelder stammten dabei überwiegend aus dem Handel mit Drogen sowie Betrugsdelikten. Der Drogenhandel erzielte dabei den Anteil i.H.v. 78 Mio. \$ (Mansholt 2021b). Zuvor wurde im Jahr 2018 Larry H. in Ohio verhaftet, der bereits seit dem Jahr 2006 mit seinem BTC-Mixer 4 Mio. \$ gewaschen hatte, indem er Konten auf Verstorbene eröffnete (Mansholt 2018). Die FATF beschrieb im Jahr 2014 die potenziellen Risiken von Kryptowährungen unter Bezug auf die NPPS-Leitlinien* aus dem Jahr 2013. Vor allem Geldwäsche und Terrorismusfinanzierung stünden dabei aus mehreren Gründen im Focus. Gründe für die Begünstigung dieser Delikte sind mehr Anonymität im Vergleich zu anderen bargeldlosen Transfers, der Handel über das Internet, anonymisierte Finanzierungsmöglichkeiten und Überweisungen und Dezentralisierung. Weiterhin gäbe es keine softwareseitige Lösung für die Identifikation oder Überwachung verdächtiger Transfers. Weitere Probleme werden in den grenzüberschreitenden Reichweiten, Komplexitäten, rasanten technologischen Entwicklungen und problemlosen Lagerungsmöglichkeiten in unterschiedlichen Ländern gesehen. Insbesondere Länder mit schwach ausgeprägten Vorschriften in Bezug auf Geldwäsche und Terrorismusfinanzierung stellen hier ein Problem dar (FATF 2014:9 f.). Das BKA warnte in seinem Bericht im Jahr 2018 vor Delikten mit Kryptowährungen. Diese seien aufgrund fehlender staatlicher Kontrolle nachweislich für das Cybercrime geeignet. Insbesondere stellt es ein adäquates Mittel für Geldwäschen und Terrorismusfinanzierung dar (BKA 2018:32). Die Financial Intelligence Unit (FIU), Sondereinheit des deutschen Zolls, bezog sich in ihrem Bericht für das Jahr 2018 erstmalig auf Kryptowährungen. Hierbei wurde festgestellt, dass ausgesuchte Kryptowährungen geschaffen wurden, um mit ihrer Unterstützung illegale Handlungen vornehmen zu können. Dazu zählen insbesondere der Drogen- und Waffenhandel, Kinderpornographie, Geldwäsche und die Finanzierung des Terrorismus. Auch würden die Täter die volatile Eigenschaft von Kryptowährungen in Kauf nehmen, um den Vorteil einer schnellen Transferierung höherer Summen zu nutzen. Aufgrund dessen sind diese prädestiniert für Geldwäschen. Im Jahr 2018 wurden bei der FIU 570 Meldungen auf Verdacht illegaler Handlungen mit Kryptowerten gemeldet. (FIU 2018:35 f.). Die Zahl der Verdachtsmeldungen erhöhte sich im Jahr 2019 auf 760. Festgestellt wurde, dass die Geldwäsche als Anschlussdelikte von Betrugsdelikten fungierte. Hauptsächlich erfolgte dies über Marktplattformen im Ausland (FIU 2019:46 f.). Kongruent dazu waren die Feststellungen von Houben und Snyers im Report an das Europäische Parlament. Hier wird von einer zunehmenden Nutzung von Kryptowährungen für Terrorismusfinanzierung, Steuerhinterziehung und Geldwäsche unter Ausnutzung der Anonymität berichtet (Europäisches Parlament/Houben/Snyers 2018:6). Da diese Delikte jedoch grenzübergreifend ausgeführt werden, wäre ein Vorgehen auf nationaler Ebene nicht anzuraten, sondern müsse international erfolgen (Europäisches Parlament/Houben/Snyers 2018:83). In der Europäischen Union wurden aufgrund der genannten Risiken Kryptowährungen und E-Wallets in die Richtlinie zur Verhinderung der

* NPPS – „New payment products and services“ – neue Zahlungsprodukte und -dienstleistungen. FATF 2013b:2

Abb. 57 BTC Volume sent to unhosted Wallets



Quelle: CipherTrace 2021a:16

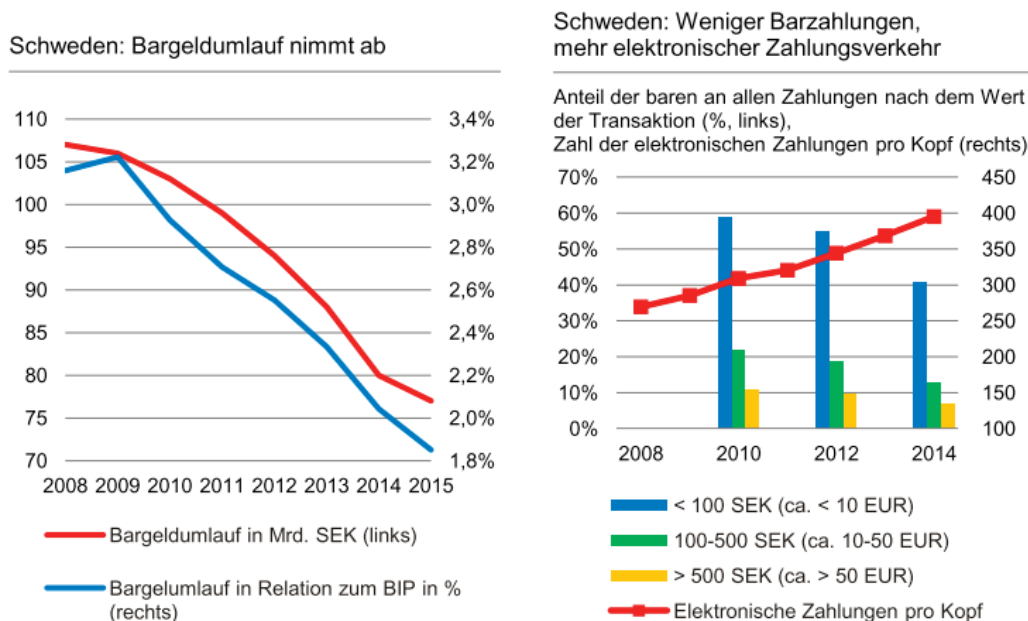
Weiterhin wurde festgestellt, dass mehr als ein Drittel aller grenzüberschreitenden Transaktionen (84% aller Transaktionen) an Börsen (Exchanger) mit gering ausgeprägten KYC gesandt wurde. Insgesamt macht das einen Anteil von 36% aus. Die Eingänge in die USA waren i.H.v. 74% grenzüberschreitend, davon 50% aus Börsen mit schwach ausgeprägten KYC. Es ist davon auszugehen, dass weder über die übermittelten Transfers noch über die Eingänge Aufzeichnungen bei den Börsen erfolgen, welche eine schwach ausgeprägte KYC besitzen, was die Strafverfolgung erheblich behindert (CipherTrace 2021a:20). Schwächen in Bezug auf die Regulierung von Kryptowährungen und Geldwäsche sind ebenso in der fünften Geldwäscherichtlinie der EU (AMLD5) zu finden, welche erstmals Kryptowährungen miterfasst. Angefangen bei ungenauen Definitionen, veralteten Begriffen bis hin zu unberücksichtigten Agierenden und Dienstleistungen, so dass sie zum Zeitpunkt der Verabschiedung überholt hätte werden müssen. Bspw. enthält die AMLD5 die Regelung, dass virtuelle Währungen die Akzeptanz eines Tauschmittels erfahren müssen, bezieht sich jedoch nicht näher auf den Begriff des Tauschmittels, so dass selbst Knöpfe oder Steine in Frage kämen. Die Gefahr einer weiten Auslegung dieser Definition besteht darin, dass dabei eine Legitimation geschaffen wird, um „alle Transaktionen mit privaten Gütern zu überwachen“ (Haffke et al. 2020:11 zitiert nach Svensson 2021:9). Unsicherheit in Bezug auf virtuelle Währungen besteht ebenso bei den erwähnten Tauschdiensten (Kryptobörsen). Erfasst wird nur der Tausch von Fiat-Geld in virtuelle Währungen und vice versa, jedoch nicht der Tausch von Kryptowährung zu Kryptowährung (Svensson 2021:11).

6.6 Conclusio Cybercrime

Terrorismus und OK sind aus Sicht von Europol eine der größten Herausforderungen mit Delikten wie der Drogenhandel. Das angestrebte Ziel, die Anhäufung von Reichtum unter Verwendung aller zur Verfügung stehenden Mittel, ist dabei unverändert. Das Motiv der Gewinnanhäufung ist dabei das treibende Mittel aller kriminellen Delikte unter ständiger Bestrebung der Ausnutzung von Schwachstellen in Gesetzen, Wirtschaft und Gesellschaft. Hingegen haben sich jedoch strukturelle Veränderungen, Veränderungen in der Vorgehensweise und Veränderungen der Agierenden selbst ergeben, was aus Sicht von Europol „die Vielseitigkeit und Flexibilität der Kriminalität verdeutlicht“ (Europol 2021:14). Trotz der Bekämpfung der Kriminalität unterliegt sie einem stetigen Wandel aufgrund hoher Flexibilität und konnte sich dadurch einer dauerhaften Störung durch Ermittlungsbehörden entziehen. Die OK des 21. Jahrhunderts ist hervorragend vernetzt, verfügt über Fachkräfte auf den Gebieten des Rechts, aus dem Finanzbereich und dem Logistiksektor. Die Zerschlagung einzelner kleiner Netzwerke hat nur marginal Einfluss auf die Kriminalität (Europol 2021:14). Die OK verfügt über Widerstandsfähigkeit, Vielseitigkeit und unterliegt einer ständigen Anpassung, um adäquat auf Veränderungen reagieren, ihren Gewinn maximieren und Risiken vermindern zu können. Dazu nutzt sie jede erdenkliche neue Chance einer Strafverfolgung zu entgehen. Die Corona-Krise hatte insbesondere Einfluss auf die Entwicklung

der Cyberkriminalität, der Produktfälschung und den Handel mit Falsifikaten oder minderwertigen Produkten sowie diverse Betrugsdelikte. Erwartet werden zudem langfristige Folgen der Krise und daraus resultierend die steigende Zahl der Schwachstellen, welche durch die Kriminalität genutzt werden. Dazu werden, wie bereits dargestellt, neue Technologien verwendet zur Weiterentwicklung ihrer technischen Fähigkeiten. Die Pandemie machte die Dynamik der Cyberkriminalität ersichtlich. Cyberdelikte, wie der Einsatz von Ransomware, Hackerangriffe oder Betrugsdelikte, unterlagen einer signifikanten Zunahme. Die Opfer sind sowohl im Unternehmensbereich als auch in staatlichen Einrichtungen und Privatpersonen zu finden (Europol 2020:94 f.). Die Digitalisierung durchströmt sämtliche Bereiche des Handels, des Privatlebens, der Gesellschaft und der Wirtschaft und schreitet auch weiterhin stetig voran. Daher ist auch eine Anpassung der Kriminalität an die Digitalisierung nicht überraschend. Annähernd jedes kriminelle Delikt besitzt heute eine Online-Komponente. Kriminelle Aktivitäten haben sich mindestens partiell in die digitale Welt verlagert. Für den illegitimen Handel wird das Surface, Deep und Dark Web benutzt, um Waren oder Dienstleistungen online vertreiben zu können. Die ubiquitäre Verfügbarkeit des Internets und der ubiquitäre Zugang zu diesem forcierten die Entwicklung diversifizierter illegaler Plattformen. Die Verwendung verschlüsselter Technologien und Social-Media-Plattformen erhöhte die Angebotsvielfalt, das Kundenvolumen sowie die Kundenbreite. Um die Strafverfolgung zu erschweren, werden Sicherheitsmaßnahmen e.g. die Verwendung von VPNs oder andere Anonymisierungsdienste wie der Tor-Browser ergriffen. Unterschieden wird selbst nach angebotener Ware oder Dienstleistung bezüglich des gewählten Vertriebsortes e.g. spezialisierte Webshops, Marktplattformen, Foren, Social-Media-Kanäle oder einer starken Verschlüsselung unterliegende Nachrichtendienste. Diese werden zudem für Reklame oder Marketingmaßnahmen für ihre Güter oder Dienstleistung verwendet. Wie dargestellt, werden Dienstleistungen im Bereich des Hackens oder Ransomware als CCaaS dargeboten, um dafür einen Anteil an kriminellen Handlungen zu erzielen. Informationen über Kreditkarten und Bankkonten werden veräußert sowie ausführliche Anleitungen vielfältiger Deliktsarten e.g. die Herstellung von Drogen, Schusswaffen oder Sprengsätzen oder andere Anleitungen für Internetdelikte (Europol 2021:26). Betrugsdelikte wie Phishing, Hacken und Malware haben sich an die digitale Entwicklung angepasst, um an Daten von Bankkonten oder Onlinebanking zu gelangen. Weiterhin werden modernste Technologien verwendet, selbst wenn diese mit Authentifizierungsmethoden geschützt werden, um erwähnte Daten erlangen zu können. Europol fasst die Entwicklung der Digitalisierung und die damit korrelierende Internetkriminalität zusammen: „Der Übergang zur bargeldlosen Wirtschaft schafft starke Anreize für Zahlungsbetrüger. Cyberkriminelle versuchen, Online-Zahlungen, Internet- und Mobile-Banking, Online-Zahlungsanfragen, kontaktlose Zahlungen (sowohl mit als auch ohne Karte) und mobile Anwendungen zu kompromittieren. Die zunehmende Nutzung mobiler Geräte für Finanztransaktionen und Authentifizierungsprozesse hat sie zu einem Ziel für Cyberkriminelle gemacht. Durch die Verwendung von Deepfakes wird es viel schwieriger, Betrug zu erkennen und zu bekämpfen. Deepfakes imitieren scheinbar echte Foto-, Video- und Audioaufnahmen von Personen. Betrüger haben die Stimmenimitation bereits als Teil von CEO-Betrugsplänen eingesetzt und werden diese Technologie wahrscheinlich noch stärker für ihre kriminellen Aktivitäten nutzen.“ (Europol 2021:62, übersetzt ins Deutsche). Das belegen auch Auswertungen innerhalb Schwedens, dem Vorzeigeland der bargeldlosen Zahlen in Europa. Der Bargeldumlauf sowie die Zahlung mit Bargeld sind in Schweden seit Jahren stetig gesunken. Die Zahlungen via unbaren Zahlungsmöglichkeiten hingegen verzeichneten einen stetigen Zuwachs (Abb. 58) (Mai 2017:13).

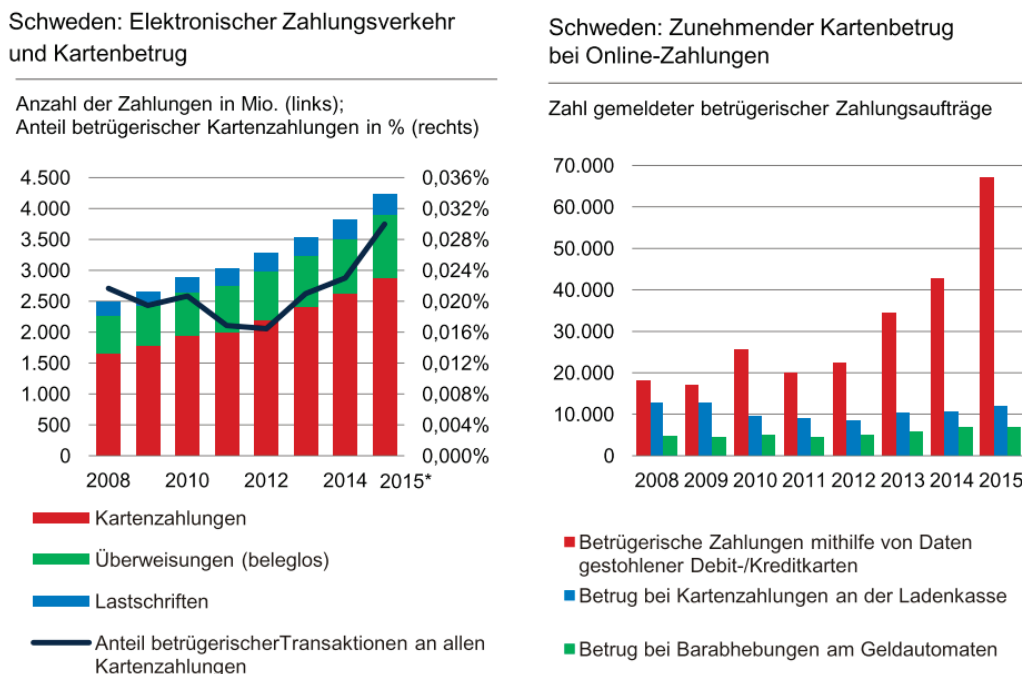
Abb. 58 Abnehmende Barzahlungen und zunehmender elektronischer Zahlungsverkehr in Schweden



Quelle: Mai 2017:13

Mit dem Rückgang der Bargeldzahlungen in den Jahren 2012-2015 wurde gleichzeitig ein starker Anstieg der Betrugsdelikte mit Karten registriert. Dieser lag sogar höher als die Zahlungen mit Karte selbst (Abb. 59) (Mai 2017:13).

Abb. 59 Schweden: Elektronischer Zahlungsverkehr und Kartenbetrug/Zunehmender Kartenbetrug bei Online-Zahlungen



Quelle: Mai 2017:14

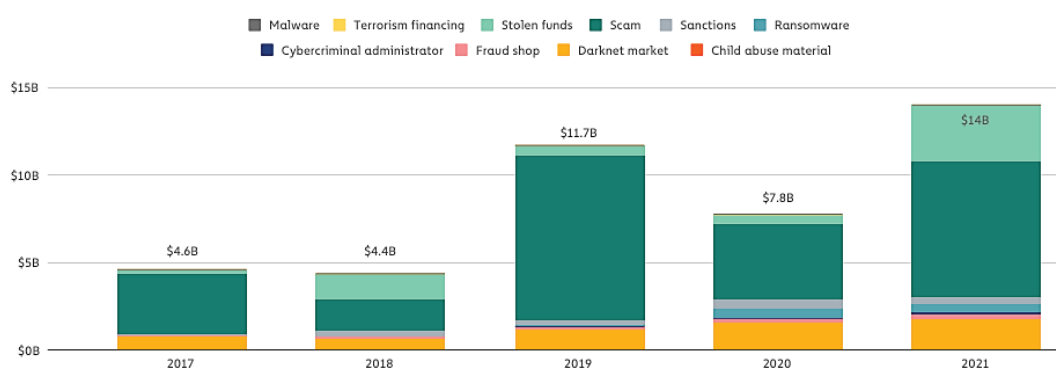
Eriksson gibt zu bedenken, dass die Zahlen der Statistik in Bezug auf Kartenbetrug in Schweden nicht der Realität entsprechen. Diese liegen weit höher, da die Majorität der Betrugsdelikte nicht von der polizeilichen Statistik erfasst werden. Grund dafür ist, dass Banken die Anzeige der Betrugsdelikte verhindern, indem sie den Kunden die Schäden aus den Delikten ersetzen und von

einer Meldung an die Polizei absehen. Oftmals haben die Kunden nicht einmal Kenntnis von den Betrugsdelikten, da verdächtige Transaktionen bereits vor Kenntnisnahme der Kunden durch die Banken selbst behoben werden. So wird das wahre Ausmaß der Betrugsdelikte verschleiert und der Schein einer Sicherheit gewahrt, welcher so nicht existent ist. Aufgrund des hohen Umsatzes und hoher Gewinne durch Kartenzahlungen sind sie bereit, die Schäden aus Betrugsdelikten in Kauf zu nehmen (Eriksson 2021:11 f.).

Innovationen sind immer mit Chancen und Risiken verbunden, davon sind Kryptowährungen nicht ausgeschlossen. Wie sich anhand der Ausführungen zeigt, werden diese zunehmend für illegitime Aktivitäten verwendet. Dazu zählen Korruption, Betrugsdelikte, Diebstahl an Kryptobörsen, Missbrauch der Märkte, Ransomware- und Hackerangriffe, Geldwäsche und Finanzierung des Terrorismus oder Extremismus, Steuervermeidung und Steuerhinterziehung. Regulierungen von Kryptowährungen sind bis dato schwach ausgebaut, um die umfänglichen Risiken überhaupt erfassen zu können. Daher könnte sich der Segen der Kryptowährungen schnell zu einem Fluch wandeln (Katarzyna 2019:12 f.). Auch im Jahr 2021 wurde eine steigende Tendenz im Bereich des Cybercrimes verzeichnet. Chainalysis spricht im aktuellen Bericht von einem Allzeithoch in Bezug auf kryptowährungsbasierte Kriminalität (Abb. 60) (Grauer/Kueshner/Updegrave 2022:3).

Abb. 60 Total cryptocurrency value received by illicit addresses 2017-2021

Total cryptocurrency value received by illicit addresses | 2017-2021



Quelle: Grauer/Kueshner/Updegrave 2022:3

Der fortschreitenden Digitalisierung geschuldet nehmen digitale personenbezogene Daten stetig zu. Anzumerken ist, dass diese sich zumeist unter Zugriff von privaten Firmen befinden. Der starke Anstieg der Datenmenge könnte weiterhin zu Überlastungen und Überforderungen von Regierungen führen, was zu einer Gefahr für den Schutz, die Verwaltung oder die effiziente Nutzung von Daten führen könnte. Auch künftig werden Cyberkriminelle zunehmend Unternehmen und staatliche Einrichtungen der kritischen Infrastruktur angreifen, um gezielt Schäden zu verursachen und um an Daten zu gelangen (Europol 2021:92). In Bezug auf die Gefahr des Verlustes der Kontrolle des Staates formuliert Europol: „Die Staaten laufen Gefahr, die Kontrolle über viele Bereiche des Finanzwesens und der Wirtschaft an die Privatunternehmen abzutreten, die den digitalen Raum beherrschen. Führende Technologieunternehmen werden ihre Monopolstellung ausbauen und dabei auf finanzielle Ressourcen und überlegene technische Kapazitäten zurückgreifen. Das Monopol auf Daten im Besitz von Dritten wird weiterhin ein zunehmendes Risiko der Manipulation und der kriminellen Nutzung von persönlichen Informationen mit sich bringen. Der Schutz der Privatsphäre und die ethische Nutzung von Daten sind zentrale Themen, mit denen sich Strafverfolgungsbehörden, Gesetzgeber und politische Entscheidungsträger befassen müssen.“ (Europol 2021:92).

In den folgenden Kapiteln wird die Kriminalität innerhalb des Finanzwesens anhand ausgewählter Beispiele und die Behauptung Europol, Unternehmen könnten mit fortschreitender Digitalisierung ihre Monopolstellung ausbauen, untersucht.

7 Andere Formen unbarer Kriminalität - Kriminalität im Finanzwesen

Trotz umfangreicher Regelungen wie bspw. das Geldwäschegesetz und Transparenzregister sind Erkenntnisse über den Umfang von Geldwäsche und Steuerhinterziehung im Finanzbereich kaum vorhanden. Die vorgeschriebenen Dokumentationen, Meldepflichten, Compliance-Vorschriften und der automatisierte Austausch von Informationen für Banken und den Finanzsektor konnten bis dato nichts an großen Geldwäschefällen ändern. Insbesondere die Geldwäsche via Briefkastenfirmen und nicht legaler Transaktionen über Konten sind in der Vergangenheit mehrfach aufgedeckt worden und stellen dabei mit Abstand das höchste Risiko für Geldwäsche und Steuerhinterziehung dar. Die Größe der Banken ist dabei unerheblich. Geld wird meist über anonyme Konten und Kunden durch Tochterfirmen im Ausland gewaschen und verschoben. Ein Hauptgrund dafür ist die Profitabilität dieser Geschäfte für Banken und Finanzsektor (Transparency International Deutschland 2021: Zusammenfassung). Mehrere Datenveröffentlichungen zeigen dabei die Vorgehensweise von Banken, dem Finanzsektor und Firmengeflechten, wie Geld transferiert, gewaschen und für Steuerhinterziehung missbraucht wird. Im Folgenden werden aufgedeckte Fälle und deren Auswirkungen näher dargestellt.

7.1 Steuervermeidung, Steuerhinterziehung und Geldwäsche

7.1.1 Begrifflichkeiten

Steuervermeidung ist laut internationalem Steuerrecht eine legale Möglichkeit Steuern zu sparen. Dabei werden steuerliche Unterschiede in der Höhe der zu zahlenden Steuern zwischen verschiedenen Ländern ausgenutzt. Ein anderer Begriff dafür ist die Steueroptimierung. Dem gegenüber steht das Delikt der Steuerhinterziehung (s. Abschnitt 5.4.1). Offshore-Zentren hingegen sind Finanzmärkte, welche nur schwachen Regulierungen unterliegen (Böhm 2012:12). Als Steueroasen oder Steuerparadiese werden Länder bezeichnet, welche entweder keine oder nur sehr niedrigen Steuern erheben. Dies bezieht sich zudem meist auf ausländisches Kapital (Böhm 2012:13). Laut Schweigert Consulting sind Offshore-Konten Konten, welche sich nicht in dem Land befinden in welchem sich der Wohnsitz des Eröffnenden befindet (Schweigert 2021a). § 7 BGB definiert dabei den Begriff des Wohnsitzes als den Ort, an dem sich Jemand „ständig niederlässt“. § 8 AO versteht darunter: „Einen Wohnsitz hat jemand dort, wo er eine Wohnung unter Umständen innehat, die darauf schließen lassen, dass er die Wohnung beibehalten und benutzen wird.“. Dabei sind Offshore-Konten grundsätzlich nicht illegal und stellen nur Konten im Ausland dar. Vorteile eines Offshore-Kontos sind nach Schweigert dabei bspw.:

- „anderen Personen ist das Konto nicht bekannt (z.B. auch ehemalige Ehepartner, aktuelle Freundin oder Geschäftspartner)
- Schutz vor Währungskrisen und Entwertung des Geldes
- Schutz vor möglichen staatlichen Eingriffen (z.B. Enteignung)
- Ersparnis von Negativzinsen
- Geld auf dem Offshore Konten kommt bei Rechtsstreitigkeiten nicht auf den Tisch
- vereinfachter Zugang zu internationalen Finanzmärkten
- ggf. weitere Vorteile (z.B. geringere Gebühren, Reputation etc.) im Land, wo das Auslandskonto eröffnet wurde“ (Schweigert 2021a).

Ein weiterer Vorteil dieser Konten ist, dass diese nicht dem automatisierten Informationsaustausch unterliegen und durch die Verfügbarkeit von IBAN und BIC als reguläre Konten, wie bspw. für Überweisungen, verwendet werden können. Diese gibt es sowohl für Privatpersonen als auch für Firmen (Schweigert 2021a). Offshore-Firmen sind Firmen, welche ihren Sitz außerhalb des Heimatlandes haben. Oftmals wird diese als International Business Company (IBC) geführt. Vorteile sind laut Schweigert:

- „Steuern sparen
- Anonymität sicherstellen
- geringer Verwaltungsaufwand
- einfachere Buchführung
- verschiedene Gesellschaftsformen möglich

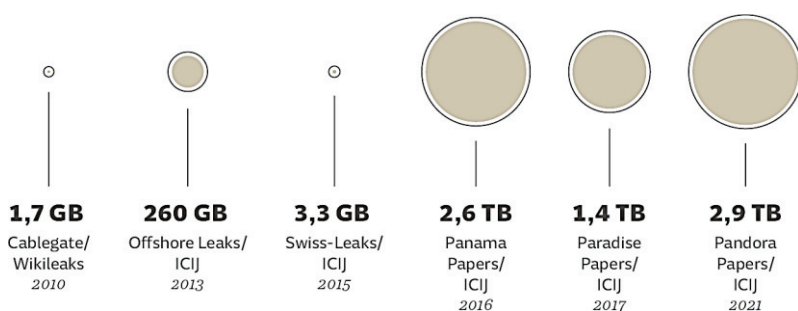
- recht niedrige Kosten für die Gründung der Offshore Firma
- schnelle Gründung der Gesellschaft (meist < 2 Wochen)“ (Schweigert 2021b).

Länder bieten Unternehmen u.a. mit günstigen Gründungskonditionen, geringeren oder keinen Steuern oder anderweitigen Vorteilen an, ihren Hauptsitz in ihre Region zu verlegen. Offshore-Firmen werden als normale Unternehmensform geführt, d.h. jegliche Geschäftstätigkeiten sind mit ihnen möglich. Weiterhin können diese aber auch in Form einer Beteiligung an anderen Gesellschaften Verwendung finden. Bspw. ist es möglich, sich an einer deutschen GmbH zu beteiligen, um die Gewinne dieser an die Offshore-Firma weiterzugeben, damit sie nicht unter die deutsche Steuerpflicht fallen. In Bezug auf die Legalität solcher Offshore-Firmen ist diese gegeben, solange mit dieser Gesellschaft legale Tätigkeiten verübt werden (Schweigert 2021b).

7.1.2 Offshore-Leaks und FinCen Files

Der größte Datenleak in Bezug auf Offshore-Aktivitäten von Privatpersonen, Politikern und Firmen stellen in jüngster Zeit die Pandora-Papers dar. Dabei wurden insgesamt 2,9 Terrabyte (TB) (Abb. 61) an Daten veröffentlicht, welche diese Aktivitäten offenlegen.

Abb. 61 Die Größe des Leaks – Umfang der Pandora-Papers im Vergleich zu andern Leaks



Quelle: Balbierer/Baumann/Bovensiepen et al./ICIJ 2021. abgerufen am 02.01.2022

Weltweit waren mehr als 600 Journalist:innen aus 117 Ländern an der Auswertung des Datenleaks beteiligt. Insgesamt wurden vierzehn Offshore-Dienstleister dabei identifiziert, welche u.a. Dienstleistungen wie die Eröffnung von Briefkastenunternehmen, Gründungen von Trusts und Stiftungen in Steueroasen für Privatpersonen und Firmen anboten und durchführten. Steueroasen waren zum Großteil die Britischen Jungferninseln, die Seychellen, Hongkong, Belize, Panama und South Dakota. Nutznießer der Dienstleistungen waren sowohl Personen aus der Politik, Musik- und Schauspielbranche als auch kleinere Unternehmen. Die Anzahl der Personen aus der Politik belief sich dabei auf über 330 aus 90 verschiedenen Ländern und Gebieten. Diese benutzten unterschiedliche, teils anonymisierte Konstellationen für die Vermögensverwaltung, Kauf von Immobilien und den Besitz von Unternehmen und anderer Vermögenswerte. Bekannt wurde auch, dass Banken an diesen Geschäften beteiligt waren. Teilweise kannten sie nicht einmal die Kunden, trotz gesetzlicher Verpflichtung diese kennen zu müssen. Der Unterschied zu den Panama-Papers aus dem Jahr 2016, welche ähnliche Daten in Bezug auf Offshore-Aktivitäten von Amtsinhaber:innen, Politiker:innen und anderen enthielten, ist, dass bei den Panama-Papers lediglich Daten einer Anwaltskanzlei namens Mossack-Fonseca enthalten waren. Bei den Pandora-Papers waren es bereits vierzehn Anbieter von Offshore-Dienstleistungen. Ähnlich liegt der Sachverhalt bei den Paradise-Papers aus dem Jahr 2017 mit nur zwei Anbietern, der Kanzlei Appleby und Asiatic Trust. Viele Kunden und Unternehmen der Panama-Papers wurden m.H.v. den Trust-Firmen Trident-Trust und Alcotgal in Panama registriert. In Bezug auf Alcotgal betrifft das in etwa die Hälfte aller Politiker:innen und Beamte:innen aus den Panama-Papers. Gründer der Firma Alcotgal waren u.a. Politiker:innen, bspw. der Botschafter Panamas in den Vereinigten Staaten. Trotz des umfangreichen Leaks der Daten, ist der überwiegende Teil der Offshore Dienstleister nicht enthalten (Díaz-Struck/Reuter/Armendariz et al./International Consortium of Investigative Journalists (ICIJ 2021)). Der jährliche Schaden aufgrund von Steuerumgehungen und Steuerhinterziehungen in Steueroasen wird in Deutschland auf 5,7 Mrd. € geschätzt. Diese setzen sich aus 1,6

Mrd. € durch deutsche multinationale Großunternehmen und 4,1 Mrd. durch kleinere multinationale Firmen oder Tochterfirmen von multinationalen Firmen im Ausland zusammen (Fuest/Hugger/Neumeier 2021:38) Weltweit geht die OECD von einem Schaden von 11,3 Mrd. aus. (Balbierer/Baumann/Bovensiepen et al./ICIJ 2021). Eine weit höhere Schätzung des Tax Justice Network beläuft sich auf 483 Mrd. Dollar weltweit (Tab. 13) (Global Alliance For Tax Justice/Tax Justice Network 2021:8).

Tab. 13 Schäden durch Steuerumgehung und Steuerhinterziehung in Steueroasen

Institution/Land	Schaden
Ifo-Institut/Deutschland	5.700.000.000 € ¹
OECD/weltweit	11.300.000.000 \$ ¹
Tax Justice Network/weltweit	483.000.000.000 \$ ²

Quelle: eigene Darstellung in enger Anlehnung an

¹ Balbierer/Baumann/Bovensiepen et al./ICIJ 2021, ² Global Alliance for Tax Justice/Tax Justice Network (2021:8)

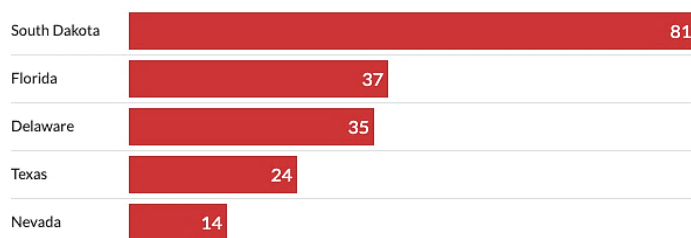
Der Anteil von 171 Mrd. der 483 Mrd. \$ entfällt dabei auf Offshore-Aktivitäten von Privatpersonen, der überwiegende Teil i.H.v. 312 Mrd. \$ entsteht durch die Verschiebung von Gewinnen multinationaler Unternehmen (Global Alliance For Tax Justice/Tax Justice Network 2021:8). Begünstigte sind aber auch zumeist Politiker:innen, welche vorgeben gegen Offshore-Netzwerke vorzugehen (Balbierer/Baumann/Bovensiepen et al. 2021). Die Medienwirksamkeit auf die Skandale der verschiedenen Offshore-Leaks in den vergangenen Jahren ließ stetig nach. Wurde der Skandal der Panama-Papers noch medial ausgeschlachtet, fanden die Pandora-Papers weder umfassend in den Medien noch in der Politik wie bspw. in der Aktuellen Stunde des Bundestages, einberufen durch die Regierung, größere Aufmerksamkeit. Schäuble veröffentlichte nach den Panama-Papers einen 10-Punkte-Plan für den Kampf gegen Steueroasen, jedoch scheitert es zum größten Teil an der Umsetzung. Von der EU wurde im Jahr 2017 als Folge des Offshore-Leaks eine Liste „nicht kooperativer Länder und Gebiete“ (Rat der Europäischen Union o.D.) in Bezug auf Steueroasen, auch „Schwarze Liste“ (Genzmer/Kogel 2021) genannt, veröffentlicht (Genzmer/Kogel 2021). Derzeit enthält diese Liste neun Steueroasen: Amerikanisch-Samoa, Fidschi, Guam, Palau, Panama, Samoa, Trinidad und Tobago, die Amerikanischen Jungferninseln und Vanuatu. Grund für die Aufnahme dieser Gebiete ist der fehlende oder unzureichende automatische „Austausch finanzieller Informationen“ (Rat der Europäischen Union 2021:5 f.). Der automatische Austausch dieser Informationen wurde im Jahr 2014 im Common Reporting Standard (CRS) vom OECD-Rat verabschiedet. Darin verpflichteten sich die teilnehmenden Staaten untereinander, Informationen über bspw. Kontoinformationen auszutauschen (OECD o.D.). Weiterhin wurde das Transparenzregister im Jahr 2017 eingeführt. Dieses soll die „[...] wirtschaftlich Berechtigten von im Geldwäschegesetz (GwG) näher bezeichneten Gesellschaften und Vereinigungen (sog. transparenzpflichtige Rechtseinheiten)“ (Bundesanzeiger o.D.) erfassen. Das sind bspw. gemäß § 21 GwG „Juristische Personen des Privatrechts (z.B. GmbH, AG) und eingetragene Personengesellschaften (z.B. KG, GmbH & Co. KG)“ (Bundesanzeiger o.D.) und gemäß § 22 GwG u.a. Trusts und „Nichtrechtsfähige Stiftungen, wenn der Stiftungszweck aus Sicht des Stifters eigennützig ist“ (Bundesanzeiger o.D.). Das Transparenzregister ist allerdings bis dato wie die schwarze Liste der Steueroasen lückenhaft (Genzmer/Kogel 2021). Auf der schwarzen Liste der EU ist festzustellen, dass lediglich 2% aller Vermögensverschiebungen weltweit durch die auf der Liste genannten Länder erfasst werden. Weder wird ein EU-Land aufgeführt (Genzmer/Kogel 2021), noch finden sich Länder wie die Schweiz oder die USA auf der Liste wieder, da sie als „too big to be listed“ (Langerock 2019:3) gelten. Auch im Jahr 2021 sind kaum Veränderungen in der Liste festzustellen. Lediglich zwei von insgesamt dreizehn Ländern mit einem Steuersatz i.H.v. 0% Körperschaftssteuer finden sich auf der Liste wieder. Länder mit einem signifikant niedrigen Steuersatz von weniger als 12,5 % Körperschaftssteuer sind nicht enthalten. Keines der vom Tax Justice Network ermittelten 20 Länder als signifikantes Steuerparadies sind auf der EU-Liste verzeichnet (Oxfam 2021:1 f.). Die USA sind, wie bereits erwähnt, nicht auf der Liste enthalten, obwohl sie seit längerer Zeit als Offshore-Oase gilt. Bereits im Jahr 1966 wurde vom Außenministerium die USA als „wahrscheinlich das zweitwichtigste Zentrum für Fluchtgelder in der Welt“ (Michel 2017:6) bezeichnet. Einerseits liegt es an der hohen Geheimhaltungsstufe

durch den Bank Secrecy Act (BSA). Weiterhin nimmt die USA nicht am CRS teil und ist aufgrund dessen nicht verpflichtet, Finanzinformationen mit anderen Ländern auszutauschen (Michel 2017:6). Laut dem Tax Justice Network belegt die USA Rang zwei auf dem Financial Secrecy Index* nach den Cayman Islands (Tax Justice Network 2020a). Neben dem Angebot der Geheimhaltung und Steuererleichterung für nicht im Land Ansässige auf Bundesebene und auf Ebene einzelner Bundesstaaten werden anonyme Briefkastenfirmen geduldet. In Bezug auf ausländische Steueroasen unternahm die USA große Anstrengungen, betrachtete jedoch nicht den inländischen Finanzmarkt. Das CRS-Abkommen wurde zunächst begrüßt, später aber abgelehnt. Derzeit werden von der USA, teils unter Drohungen, Informationen gemäß dem CRS von anderen Ländern abgefordert, übermitteln jedoch keine Informationen an andere Länder. Inzwischen besitzen die USA den höchsten Anteil am Offshore-Markt in der Welt (Tax Justice Network 2020b:1). Das Offshore Vermögen wurde im Jahr 2017 auf 800 Mrd. \$ geschätzt. Der geschaffene Foreign Account Tax Compliance Act (FATCA), welcher ausländischen Kreditinstitute dazu verpflichtet, Transaktionen von amerikanischen Kunden außerhalb der USA zu melden, ähnelt dabei stark dem CRS. U.a. schlossen sich diesem Regelwerk Bahrain und Vanuatu an. Trotz der Nähe zum CRS sind keine Zusammenhänge zwischen den Regulierungen erkennbar, ins besonders auf den Austausch von Finanzinformationen. Das eigens geschaffene Regelwerk FACTA hatte zur Folge, dass signifikante Vermögensverschiebungen von europäischen Kreditanstalten in die USA erfolgten (Michel 2017:6). Bezugnehmend auf die Pandora-Papers waren auch hier die meisten Kunden unter der Verwaltung von Trident-Trust mit Sitz in Sioux Falls, South Dakota. Weitere Trust-Dienstleister stammen aus den Bundesstaaten Florida, Delaware, Texas und Nevada (Abb. 62) (Fitzgibbon/Cenziper/Georges/ICIJ 2021).

Abb. 62 Which US states have the most trusts in the Pandora Papers?

Which US states have the most trusts in the Pandora Papers?

The investigation shows how U.S. trusts have become a go-to vehicle for financial secrecy.



Quelle: Fitzgibbon/Cenziper/Georges/ ICIJ 2021

Innerhalb einer knappen Dekade ist das Trust-Vermögen von 57,3 Mrd. \$ auf 355,2 Mrd. \$ im Jahr 2020 in South Dakota gestiegen. Grund dafür ist ein lückenhaftes Finanzsystem. Ein Anwalt aus South Dakota, spezialisiert auf das Treuhandrecht, gab in Bezug auf die Trusts folgendes Statement: „Man kann sich South Dakota und seine Treuhandbranche ansehen, aber wenn man sich wirklich mit CRS befassen will, sollte man sich die Menge an ausländischem Geld ansehen, die in US-Banken fließt, nicht nur in Treuhandgesellschaften. Die USA haben auf sehr hoher Ebene beschlossen, dass sie erheblich davon profitieren, nicht Mitglied von CRS zu sein. Das ist ein viel größeres Problem als das der Trusts, und ich glaube nicht, dass sich daran etwas ändern wird, wirklich nicht.“ (Bullough 2019). Die Beteiligung der Banken an Vermögensverschiebungen, Geldwäsche und Unterstützung von Terrorismus, Drogenhandel und Korruption von Regierungen wurde in den FinCen Files offengelegt. Ausgewertet wurden dabei geheime Dokumente der US-Regierung. In den Dokumenten wurde offenbar, dass fünf weltweit tätige Banken trotz

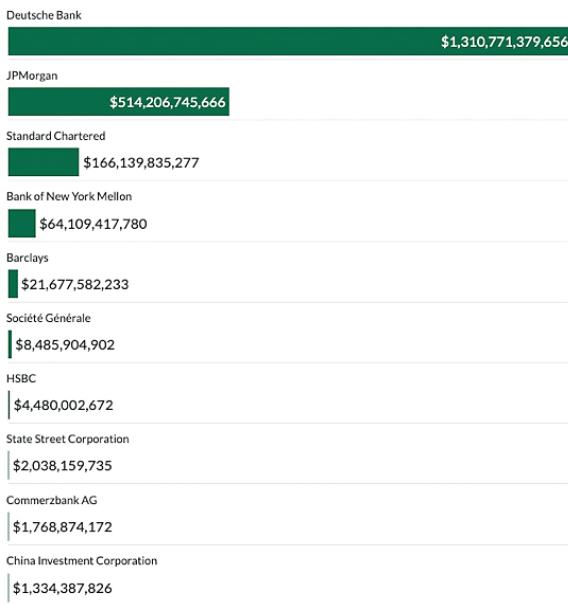
* „Der Financial Secrecy Index (FSI) ist die weltweit umfassendste Bewertung der Geheimhaltung von Finanzzentren und der Auswirkungen dieser Geheimhaltung auf die globalen Finanzströme.“ Tax Justice Network o.D. . <https://fsi.taxjustice.no/index/top>. abgerufen am 05.01.2022

bereits vorher erfolgten Strafsanktionen durch die US-Regierung hohe Summen für Kriminelle bewegten, weil sie daraus Profit schlugen. Dies betraf die Banken JPMorgan, die HSBC, die Standard Chartered Bank, die Deutsche Bank (DB) und die New York Mellon Bank. Insgesamt sollen im Zeitraum von 1999 bis 2017 Gelder i.H.v. zwei Billionen \$ bewegt worden sein, welche als geldwäscheverdächtig eingestuft wurden oder dem Verdacht anderer krimineller Aktivitäten unterstanden. Die größte Summe bildeten die Anteile der Deutschen Bank mit 1.311 Mrd. und JPMorgan mit 514 Mrd. am Gesamtvolumina (Abb. 63) (ICIJ 2020).

Abb. 63 Top 10 banks by reported amount in FinCen Files

Top 10 banks by reported amount in FinCEN Files

Total amount disclosed by banks in suspicious activity reports found in the FinCEN Files.



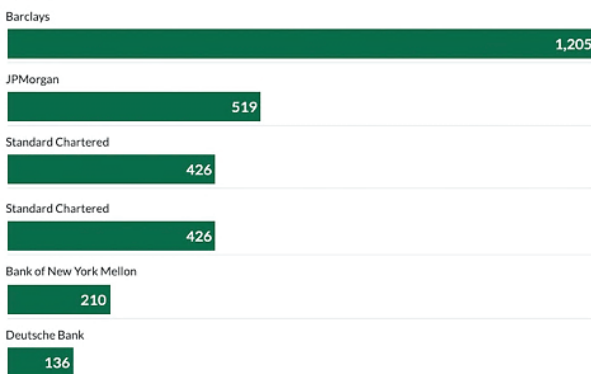
Quelle: ICIJ 2020

Dabei bilden die FinCen Files und die Sachverhalte mit ihren zugehörigen Summen weniger als 0,02% aller Verdachtsmeldungen i.H.v. 12 Mio. von Banken und Finanzinstituten ab. Die 0,02% Verdachtsmeldungen selbst wurden zudem mit hoher Verzögerung abgegeben. Barclays bspw. benötigte dafür 1.205 und die DB 136 Tage (Abb. 64) (ICIJ 2020).

Abb. 64 How long it takes banks to file a suspicious activity report

How long it takes banks to file a suspicious activity report

The median number of days it took the top five banks by transactions amount in FinCEN Files to file a report from the time transactions took place and the time it was reported to FinCEN.



Source: FinCEN Files data

Quelle: ICIJ 2020

Die Geldwäsche korrelierte dabei mit diversen Delikten. Im Jahr 2012 unterzeichnete die HSBC eine Erklärung, Bargeld i.H.v. 881 Mio. \$ für ein Drogenkartell aus Lateinamerika gewaschen zu haben. Die Strafzahlung dafür belief sich auf 1,9 Mrd. \$. Weiterhin erklärte sich die HSBC dazu bereit, innerhalb eines Zeitraums von fünf Jahren die Geldwäsche signifikant zu bekämpfen. Dafür wurde ihr im Gegenzug die Strafverfolgungseinstellung versprochen. Aus den FinCen Files geht jedoch hervor, dass innerhalb dieses Zeitraums Gelder von Russen und aus einem Ponzi-System gewaschen wurden. Im Dezember 2017 wurde der HSBC durch die Regierung zugestanden, öffentlich eine Erklärung abzugeben, dass sie den Forderungen aus den Verpflichtungen nachgekommen sei. Infolgedessen wurde, wie versprochen, die Strafverfolgung eingestellt. 2005 wurde bekannt, dass die Arab Bank mit Sitz in Jordanien mit einem Bombenattentat in Jerusalem im Jahr 2003 in Verbindung stand. Grund dafür waren Geldverschiebungen und Unterstützung von Terrorismus. Die Arab Bank wurde daraufhin in den USA in Geldgeschäften aufgrund Geldwäsche beschränkt. Jedoch ging diese daraufhin mit der Standard Chartered eine geschäftliche Beziehung ein, welche ihr wieder den Zugang zum Bankensystem in der USA verschaffte. Weiterhin wurde im Jahr 2012 festgestellt, dass die Standard Chartered mit der iranischen Regierung in Verbindung stand und Gelder i.H.v. 250 Mrd. \$ transferierte. Dafür erhielt sie im Gegenzug „Hunderte von Millionen Dollar an Gebühren“ (ICIJ 2020). Die Standard Chartered wurde daraufhin mit einer Strafe von 670 Mio. \$ belegt und musste eine Vereinbarung wie die HSBC unterzeichnen. Trotz dieser Vereinbarung wurden auch hier Gelder i.H.v. 24 Mio. \$ im Zeitraum 09/2013-09/2014 für die Arab Bank transferiert. Die Arab Bank wurde im Jahr 2014 im Zusammenhang mit dem Bombenattentat in Jerusalem für haftbar erklärt. Trotzdem bewegte die Standard Chartered weitere Millionen für die Arab Bank bis Ende 2016. Auffällig daran waren die Stichwörter bei Überweisungen wie „Wohltätigkeitsorganisationen“, „Spenden“, „Unterstützung“ oder „Geschenke“ (ICIJ 2020), welche oftmals mit kriminellen Aktivitäten korrelieren. Im Jahr 2016 wurde das Urteil der Haftbarkeit gegen die Arab Bank aufgehoben, da es zu Formfehlern seitens des Richters gekommen war. Die Arab Bank zahlte den Opfern des Bombenanschlags freiwillig eine nicht bekannt gewordene Summe und verkündete, dass sie Terrorismus nicht unterstützt. Dabei gab sie an, dass zu jener Zeit nicht über die technologischen Mittel verfügt hätte, um die Geldwäsche zu verhindern. 2018 wurde die Beschränkung aus 2005 seitens der US-Behörden beendet. JPMorgan wurde beschuldigt in Verbindung mit der iranischen Regierung zu stehen, wusch Gelder in Bezug auf Betrug, Diebstählen und anderen Delikten. Die DB transferierte im Zeitraum von 2003-2017 11 Mrd. \$ für einen russischen Oligarchen und verschob mit Hilfe der Standard Chartered 677 Mio. \$ für ein Bauunternehmen aus Lateinamerika. Dieses Geld korreliert mit dem bis dato größten Bestechungsskandal im Ausland. Allein 560 Mio. \$ wurden dabei durch die DB verschoben. Bis dato hat die DB als einzige der fünf genannten Banken keine Unterlassungserklärung in Bezug auf Geldwäsche unterzeichnet. Es wurde weiterhin bekannt, dass Mitarbeiter Kunden aus dem Iran und anderen Krisengebieten berieten, Überweisungen mit bestimmten Stichwörtern zu versehen. Die Mitarbeiter wurden von einem Führungsmitarbeiter dazu instruiert, damit die US-Behörden nicht aufmerksam werden. 2015 wurde die Vorgehensweise entdeckt und festgestellt, dass zwischen 1999 und 2006 annähernd 11 Mrd. \$ für US sanktionierte Staaten wie Syrien oder den Iran verschoben wurden. Die Strafzahlung belief sich auf 258 Mio. \$. Die fortwährenden Tätigkeiten der Banken mit Geldwäsche, Vermögensverschiebung und Offshore-Geschäfte werden aus Profitgründen durchgeführt. Sie bekommen für diese Delikte hohe Gebühren und Prämien bezahlt. JPMorgan hat bspw. über eine halbe Mrd. \$ an Erlösen an der Beteiligung an einem Ponzi-System erzielt. Weitere 4,13 Mrd. \$ wurden an Einnahmen aus der Plünderung ukrainischer Staatskassen erzielt. Darüber hinaus wird vermutet, dass Banken nur einen geringen Anteil an Delikten offenlegen und hohe Strafsanktionen bei Entdeckung in Kauf nehmen in Aussicht auf hohe Prämien und Erlöse aus Gebühren (ICIJ 2020).

7.2 Steuererschleichung, Steuerbetrug und Lobbyismus

7.2.1 Wirecard

Wirecard war ein in Bayern ansässiger Payment-Service-Provider (PSP). PSPs fassen Informationen aus Kreditkartenzahlungen, welche online erfolgen, zusammen und übermitteln sie als Datensätze für die Abbuchung an die Banken. Zusätzlich besaß Wirecard eine Banklizenz. Dies ermöglichte nicht nur die Funktion eines PSP, sondern ebenso die Transferierung des Geldes aus Onlinezahlungen. Bezeichnet wird dies als Acquirer. Der Acquirer hat die Funktion inne, den Zahlungsbetrag vom Kreditinstitut des Zahlenden anzufordern und nach Abzug seiner Gebühr dem Händler zukommen zu lassen (Bergermann/Ter Haseborg 2021:100). Gegründet wurde Wirecard ursprünglich unter dem Namen Wire Card im Jahr 1999 (Bergermann/Ter Haseborg 2021:26) und wollte sich hauptsächlich auf Zahlungen im Bereich der Pornoindustrie und Online-Glücksspiel bzw. Online-Wetten spezialisieren (Bergermann/Ter Haseborg 2021:37). Den größten Markt dafür bot die USA. Als Präsident Bush im Jahr 2006 den „Unlawful Internet Gambling Enforcement Act“ (UIGEA) unterzeichnete, fielen allein 12 Mrd. \$ Umsatz auf die Online-Gaming-Industrie. Mit der Verabschiedung dieses Acts sollte der Finanzbranche die Abwicklung von Zahlungen aus Online-Glücksspielen untersagt werden, um gegen illegale Glücksspielportale vorzugehen (Bergermann/Ter Haseborg 2021:60). Im Jahr 2010 wurde Strafanzeige gegen Wirecard wegen Geldwäsche und Betrugs unter Vorlage belastenden Materials bei der Staatsanwaltschaft München gestellt. Die Geldwäsche soll dabei im Zusammenhang mit verbotenen Transaktionen im Glücksspielbereich in den USA gestanden haben (Steinmann 2020a). Verschleiert wurden diese über falsche Internetshops oder anderen Unternehmen, welche unter Mithilfe von Personen, bspw. aus UK, zu diesem Zweck gegründet wurden (Bergermann/Ter Haseborg 2021:66 f.). Insidern zufolge hatte Wirecard bereits seit 2008 ein solches System in Verwendung. Im Jahr 2012 wurde das Verfahren wegen fehlendem Tatnachweis eingestellt. Weitere Anzeigen wegen Geldwäsche und Betrugs erfolgten im Jahr 2016 u.a. durch Kreditinstitute. Zusätzlich wurde im Internet ein Report von Zatarra Research & Investigations veröffentlicht, welche bis dato völlig unbekannt war. Darin war umfassend beschrieben und nachgewiesen, dass Wirecard an Geldwäsche und Betrug in Korrelation zu Online-Glücksspielen beteiligt ist. Wirecard wies die Vorwürfe als unwahr zurück. Die BaFin untersuchte daraufhin den Vorwurf der Marktmanipulation den Wirecard gegen Investoren erhob und leitete eine Strafanzeige bei der Staatsanwaltschaft in München ein. Das betraf u.a. auch die Verfasser des Zatarra Reports. Der Vorwurf der BaFin lautete hier, dass gezielt die Aktien der Wirecard AG mit einem Kursabfall manipuliert werden sollten, um damit Gewinn zu erzielen. Den Autoren des Reports konnte jedoch keine Marktmanipulation nachgewiesen werden. Spätere Untersuchungen der Ermittlungsakten belegen, dass sich bei der Ermittlung eher auf die Wirecard-Kritiker und die Autoren des Berichts konzentriert wurde als auf die Berichtsinhalte selbst, d.h., die Vorwürfe und Belege für Geldwäsche und Betrug. Bereits im Jahr 2011 war nach selbem Muster eine Anzeige wegen unerlaubten Transfers in Bezug auf Online-Casinos der Schutzgemeinschaft der Kapitalanleger e.V. (SdK) verfahren worden. Die Wirecard AG wehrte sich daraufhin mit dem Argument der Marktmanipulation, weil mehrere Beteiligte von SdK auf das Fallen des Aktienkurses gewettet hatten. Auch ein anonymes Hinweis eines Whistleblowers bezüglich Manipulation von Aktien und Bestechung von Wirtschaftsprüfern blieb erfolglos. Auch im Jahr 2019 leitete die Staatsanwaltschaft in München auf Anzeige der BaFin Verfahren gegen Journalist:innen nach mehreren Berichten in der Financial Times und gegen Investoren wegen des Verdachts der Marktmanipulation ein. Bezüglich des Zatarra-Reports aus dem Jahr 2016 erfolgte eine Durchsichtung der Geschäftsräume bei der Wirecard bereits in 2015, da mehrere Behörden den Bericht schon vor der Veröffentlichung zugestellt wurde (Steinmann 2020a). Dieser ging u.a. an das FBI, den United States Secret Service, Visa, Mastercard oder das Criminal Bureau of India (Earl/Perring 2016:5). Erkenntnisse aus der Durchsichtung wurden bis dato nicht veröffentlicht (Steinmann 2020a). Im Jahr 2019 erhob Merkel während ihres China Besuchs im September 2019 auf Empfehlung zu Guttenbergs, welcher Berater von Wirecard in den Jahren 2016-2020 war, Fürsprache für die Übernahme des PSP AllScore in China durch Wirecard. Laut späterer Aussage der Bundesregierung „[...] hatte sie keine Kenntnis von möglichen schwerwiegenden Unregelmäßigkeiten bei Wirecard“ (Bundesregierung zitiert nach

Bergermann/Ter Haseborg 2021:196). Weitere Beteiligte aus der Politik auf Empfehlung zu Guttenbergs sind später der deutsche Botschafter in Peking und der chinesische Botschafter in Deutschland mit unbekanntem Gesprächsinhalt. Weiterhin waren Fritsche - ehemaliger Beauftragter für Nachrichtendienste der deutschen Regierung, Kindler - Präsident der Landespolizei in Bayern für den Zugang zu Söder, Carstensen - ehemaliger Ministerpräsident Schleswig-Holsteins als Zugang zu Herrmann als bayrischer Innenminister sowie von Beust - ehemaliger Bürgermeister Hamburgs beteiligt an der Fürsprache von Wirecard. Die geplante Übernahme von AllScore wurde noch im Jahr 2019 von Wirecard verkündet. Weiterhin wurde die Übernahme der Deutschen Bank seitens Wirecard geplant (Bergermann/Ter Haseborg 2021:195 ff.). Bereits am Jahresanfang 2019 berichtete die Financial Times mehrfach über Fälschungen von Verträgen und Geldwäsche in Singapur, dem Geschäftsbereich der Wirecard im asiatischen Raum (App. 34). Im Auftrag der BaFin wurde daraufhin eine Ermittlung im Februar eingeleitet, welche durch eine Person bewältigt werden sollte. Einige Zeit später wurde die KPMG Wirtschaftsberatungsgesellschaft zur Untersuchung hinzugezogen. Aufgedeckt wurden Unregelmäßigkeiten, Scheinfirmen und Konten wie bspw. in Asien auf denen ein positiver Saldo von ca. 1,9 Mrd. € befinden sollte. Die Wirtschaftsprüfer fanden zum damaligen Zeitpunkt weder ein Beleg für die Existenz der Konten noch für die 1,9 Mrd. € und verweigerten aufgrund dessen die Testierung des Jahresabschlusses. Im Juni 2020 meldete Wirecard infolge Illiquidität und Überschuldung Insolvenz an. Im Juli wurden mehrere Beteiligte verhaftet unter dem Vorwurf der Untreue, Bilanz- und Marktmanipulation. Der entstandene Schaden beläuft sich für die Gläubiger der Wirecard AG auf über 12,4 Mrd. € (Siller/Schrag/Althammer et al. 2021). Weiterhin ergab die Untersuchung des causa Wirecard eines später einberufenen Untersuchungsausschusses, dass Mitarbeiter der BaFin, zum damaligen Zeitpunkt unter Führung von Bundesfinanzminister Olaf Scholz, an Aktiengeschäften der Wirecard beteiligt waren und Wetten auf fallende Kurse im Zeitraum der Insolvenz abschlossen. Insgesamt gab es 265 Fälle, von denen 106 auf Juni 2020 des Bekanntwerdens der Bilanzmanipulation und der öffentlichen Vermutung der Nichtexistenz des Bankguthabens i.H.v. 1,9 Mrd. € entfielen. Bei einer vorherigen Anfrage im Oktober 2020 an das Finanzministerium wurden lediglich 196 Fälle gemeldet. Die Differenz erklärte das BaFin auf nochmalige Nachfrage durch verspätete Meldungen von BaFin Mitarbeitern. Zwei beteiligte Mitarbeiter an Aktiengeschäften waren dabei aus der Abteilung für die Überwachung des Marktes und Insiderhandverfolgung. Im Umfeld der BaFin sind solche Aktiengeschäfte der Mitarbeiter ohne Verzug zu melden. Zusätzlich unterliegen die Mitarbeiter dem Insiderhandelsverbot und haben erhöhte Verschwiegenheitspflichten. Trotzdem wurde ein Fall einer Beteiligung eines Mitarbeiterangehörigen identifiziert (Steinmann 2020c). Ein Sonderbericht der BaFin vom Februar 2021, welcher sich mit diesen Fällen auseinandersetzte, kam zum Ergebnis, dass lediglich in einem Fall die Verwendung von Insiderinformationen nicht ausgeschlossen werden könne. Für alle anderen Fälle lägen keine Belege dieser Informationen vor (BaFin 2021:2). Jakubeit geht hier von einem kompletten Versagen deutscher Behörden aus. Als Grund sieht er Voreingenommenheit gegenüber Beschuldigungen deutscher Unternehmen wie Wirecard aus dem Ausland und aus dem Anspruch des Schutzes deutscher Unternehmen (Jakubeit 2021:1). Insbesondere die BaFin habe durch ihr Versagen verdeutlicht, dass der Schutz von Wirecard höher gewichtet wurde als die Untersuchung der vorgebrachten Vorwürfe. So ging sie mehrfach von einer versuchten Marktmanipulation der Kritiker aus. Zusätzlich ist sie damit auch verantwortlich für den hohen Schaden der Anleger, die aufgrund dessen auf die Korrektheit der Vorgänge vertrauten (Jakubeit 2021:34). Scholz, ehemaliger Finanzminister, wies sämtliche Schuld von sich. Während der Befragung durch den Untersuchungsausschuss musste er jedoch trotz Beteuerung, er würde dienstliche und private Emails stets strikt trennen, eingestehen, dass E-Mails in Bezug auf Wirecard von seinem privaten Mailkonto gesendet und empfangen wurden. Allerdings gäbe es nur die zwei Mails, die ihm der Untersuchungsausschuss zum Beweis der privaten Kommunikation vorlegte (Tagesspiegel 2021).

7.2.2 Cum-Ex

Der Unterschied zwischen Cum-Ex und Cum-Cum Geschäften besteht in der steuerlichen Last bzw. Rückerstattung von Steuern bei Aktiengeschäften. Diese werden also aus rein steuerlichen Zwecken durchgeführt. Ziel dieser Geschäfte ist es, sich die Kapitalertragssteuer auf Dividenden (Gewinnausschüttungen) für Aktien aus dem Inland entweder sich anrechnen oder erstatten zu lassen. Die Kapitalertragssteuer ist eine sogenannte Quellensteuer, d.h. die Steuer wird dort einbehalten, wo sie entsteht, an der Quelle. Diese ist im Voraus zu leisten und soll damit die Steuereinnahmen schützen. Da eine doppelte Besteuerung vom Gesetzgeber ausgeschlossen werden soll, lässt sich die Kapitalertragssteuer auf die Einkommenssteuer oder Körperschaftssteuer entweder anrechnen oder erstatten. Bei natürlichen Personen entsteht die Besteuerung mit der abzuführenden Kapitalertragssteuer bei der Gesellschaft, welche die Ausschüttung vornimmt. Von dieser Besteuerung soll eine teilweise Entlastung mit den Vorschriften der Doppelbesteuerung erreicht werden. Juristische Personen hingegen werden fast vollständig oder vollständig entlastet (Nickel 2021:4), da Ausschüttungen für juristische Personen lt. Körperschaftsteuergesetz (KStG) steuerfrei sind. In der Vergangenheit kam es zu mehrfachem Missbrauch von Cum-Ex-Geschäften mit nachfolgendem Muster (App. 35): Bei Cum-Ex-Geschäften handelt es sich um Aktiengeschäfte um den Dividendenstichtag herum, welcher ebenso der Termin für die Hauptversammlung ist, bei denen alle Aktionäre über die Höhe der auszuschüttenden Dividende abstimmen. Am Dividendenstichtag erfolgt die Ausschüttung, und zwar einen Tag nach der Hauptversammlung. Bei der Ausschüttung behält die ausschüttende Aktiengesellschaft die Steuer i.H.v. 25% ein und führt sie an das Finanzamt (FA) ab, 75% werden als Nettodividende an die Investoren ausgeschüttet (Nettodividende + Steuer = Bruttodividende). Diese Steuer müssen von natürlichen Personen getragen und können im Rahmen der Einkommenssteuer geltend gemacht werden aufgrund der bereits erwähnten Doppelbesteuerungsregelung. Eine Rückerstattung durch das FA ist jedoch nicht möglich. Hingegen können sich juristische Personen wie Banken die Kapitalertragssteuer i.H.v. 25% vom FA rückerstatten lassen, da bei Dividenden keine Körperschaftssteuer (Einkommenssteuer bei Unternehmen) fällig wird. Die Dividende wird überwiegend vom ausschüttenden Unternehmen jährlich ausbezahlt. Für den Erwerber verliert die Aktie damit deutlich an Wert, denn sie besitzt nur noch den ursprünglichen Wert abzüglich der noch nicht ausgeschütteten Dividende. Er könnte sie demnach nur unter Wert weiterverkaufen. Entscheidend ist hierbei die Rolle des Händlers, bei Cum-Ex-Geschäften oftmals ein sogenannter Leerkäufer. Leerkäufer bedeutet, dass der Verkäufer der Aktien (meist Personen aus Finanzinstituten) zum Zeitpunkt der Veräußerung die Aktien nicht hält, sondern noch vom Eigentümer gehalten werden. Mit Leerverkäufen wird sehr oft auf fallende Aktienpreise gesetzt, um damit Gewinn zu erzielen. Geht der Leerkäufer einer Aktie von deren zukünftig fallenden Preis aus, kann er zu diesem Zeitpunkt die Aktie für bspw. 90 € verkaufen, auch wenn er sie nicht hält. Gleichzeitig hofft er, dass die Aktie tatsächlich im Preis verfällt, bspw. auf 80 €, um sie dann bei dem Eigentümer zu diesem Preis zu bekommen und an den Erwerber zu liefern. Die Differenz von 10 € ist sein Gewinn (Budras 2016). Wie bereits erwähnt, wird die Nettodividende i.H.v. 75% ausbezahlt, die einbehaltenen 25% können sich juristische Personen nach Vorlage einer Kapitalertragssteuerbescheinigung (von seiner Depotbank ausgestellt), vom FA rückerstatten lassen. Investoren, zumeist juristische Personen, machten davon regelmäßig Gebrauch. Der Leerverkäufer muss nun die Aktien liefern, welche jetzt bereits im Wert gesunken sind und daher vergünstigt erworben werden können (App. 36). Ein Problem besteht allerdings bei der Lieferung der Aktien, denn sein Erwerber wollte die Aktien nur mit Dividendenanspruch erwerben (= cum dividend). Erworben hat der Leerverkäufer jedoch nur Aktien ohne Dividendenanspruch (= ex dividend). Also vereinbart er mit dem Erwerber (= Aktienfond) eine Ausgleichszahlung für den entfallenen Dividendenanspruch. Insgesamt erhält der Aktienfond dann einen Betrag, den er bei einer Ausschüttung von der Aktiengesellschaft erhalten hätte, also abzüglich der einbehaltenen Steuer. Die Ausgleichszahlung war bis zum Jahr 2006 steuerfrei, und trotzdem konnte der Erwerber (Aktienfond) mit einer Steuerbescheinigung eine Rückerstattung beim FA geltend machen. Der Leerverkäufer hat an dem Cum-Ex-Geschäft einen hohen Gewinn erzielt. Dieser errechnet sich aus dem Verkaufspreis abzüglich des Lieferpreises und der Ausgleichszahlung. Oftmals sind diese Geschäfte in der Vergangenheit in Absprache mit dem Aktienfonds und Investoren vorgenommen worden und der Gewinn wurde unter den Beteiligten aufgeteilt (Budras 2016). Zusätzlich kam es zu aufgrund Verschleierungen durch

mehrfach durchgeführte Verschiebungen ganzer Pakete von Aktien dazu, dass die zu erstattende Steuer mehrfach beantragt und auch mehrfach erstattet wurde. Im Jahr 2007 beschloss der Bundestag eine Gesetzesänderung in Bezug auf die Ausgleichszahlungen. Diese unterlag ab da an ebenso der Kapitalertragssteuernpflicht. Findige Leerkäufer fanden aber alsbald eine Gesetzeslücke, indem sie auf Depotbanken im Ausland zurückgriffen, da sich die Regelung nur auf Depotbanken im Inland bezog (Budras 2016). Im Juli 2021 bestätigte der Bundesgerichtshof (BGH) ein Urteil des Landgerichtes in Bonn im Jahr 2019, dass es sich bei Cum-Ex-Geschäften um Steuerhinterziehung handelt und dass keinesfalls Gesetzeslücken vorlägen. In dem Prozess vor dem Landgericht wurden zwei britische Aktienhändler der Steuerhinterziehung für Cum-Ex-Deals zwischen 2011 und 2017 schuldig gesprochen und zur Zahlung von Geldstrafen verurteilt. Die beteiligte Warburg-Bank aus Hamburg wurde zur Rückzahlung der Steuerforderung i.H.v. 176 Mio. € verurteilt (Hempel 2021). Dabei gab es bereits vor dem Urteil des Landgerichtes Anzeichen für die Unrechtmäßigkeit dieser Deals. Im Jahr 2012 verlor die Finanzfirma Rajon in einem Prozess gegen das FA Wiesbaden, welches eine Steuerrückzahlung von 113 Mio. € verlangte, eine Klage gegen den Steuerbescheid. Weiterhin gab es Ermittlungen gegen die am Deal beteiligte Hypo-Vereinsbank. Am 24.05.2013 gab die Bundesregierung im Rahmen der Beantwortung einer kleinen Anfrage des Parlamentes bekannt, dass zum einen weder ein Anspruch auf die Rückerstattung bestünde noch, dass diese Geschäfte legal seien. In den Folgejahren gab es weitere Klageabweisungen und mehrere Razzien bei beteiligten Banken wie die DB, Dekabank oder Commerzbank und Finanzunternehmen. Im Jahr 2018 gab es weitere Razzien bei der Warburg Bank und dem Finanzunternehmen BlackRock zu dessen Vorstand Friedrich Merz gehört. Weitere Ermittlungen ergaben den Umfang der Cum-Ex-Deals mit beteiligten Banken weltweit (Iwersen/Votsmeier/Bender 2019). Correctiv schätzt den weltweiten Schaden der Cum-Ex-Deals auf mehr als 150 Mrd. €. Dabei teilt sich die Schadensumme geordnet nach Höhe wie folgt auf (Tab. 14) (Correctiv 2021).

Tab. 14 Schadenhöhe der Cum-Ex-Deals in verschiedenen Ländern

Land	Schadenhöhe in Mrd. €
Deutschland	36,0
Frankreich	33,4
Niederlande	27,0
Spanien	18,9
Italien	13,3
Belgien	7,5
USA	4,9
Schweiz	4,8
Luxemburg	2,2
Dänemark	1,7
Österreich	1,2

Quelle: eigene Darstellung in enger Anlehnung an Correctiv 2021

Beteiligte waren u.a. die Commerzbank, die DB, die Hypovereinsbank, die M. M. Warburg, J. Safra Sarasin (Schweizer Privatbank) und die Merrill Lynch (Investmentbank in den USA). Aber auch Politiker waren daran beteiligt (Correctiv 2021). Wolfgang Kubicki, welcher im Jahr 2017 als aussichtsreichster Bewerber für den Posten des Bundesfinanzministers galt, vertrat einen der Hauptangeklagten Hanno Berger in den Cum-Ex-Skandalen (Rohrbeck/Salewski/Schröm 2017). Das Mandat legte er erst im Jahr 2020 nieder (Correctiv 2021). Paradox daran ist, dass Kubicki sowohl Anwalt des Hauptangeklagten war als auch Leiter der Bundestagsitzung zur Auswertung der Cumex Files (Fend 2018). Ein weiterer Beteiligter aus der Politik war Olaf Scholz. Dieser war in der Zeit von 2011-2018 Hamburgs Bürgermeister. Das BMF wies die Hamburger Finanzbehörde im Jahr 2016 an, die Steuern von der Hamburger Warburg Bank zurückzufordern (Correctiv 2021). Dabei drohte bereits die Verjährung eines Teilbetrags i.H.v. 43 Mio. €. Bekannt wurde, dass nach der Forderung Treffen zwischen dem Inhaber der Warburg Bank, Christian Olearius, und Scholz stattfanden, an die sich Scholz nicht mehr erinnern konnte. Diese konnten jedoch aufgrund Tagebucheintragungen Olearius belegt werden. Die restlichen 47 Mio. € des Ge-

samtbetrages verjährten in 2016 (Salewski/Schröm/Strunz 2020). Bei diesen Treffen soll laut Tagebuchaufzeichnung versucht worden sein, Einfluss auf die Finanzbehörden zu nehmen, welches Olaf Scholz vor dem späteren Untersuchungsausschuss abstritt und behauptete, dass er sich nicht an die Inhalte der Gespräche erinnere. Weiterhin wurde Kontakt zu Kahrs, dem haushaltspolitischen Sprecher der SPD und Pawelczyk, welcher einen hohen Einfluss in Hamburgs SPD hat, aufgenommen. Belegt ist, dass Kahrs Kontakt zum BMF und der BaFin hatte und das im Jahr 2017 die Hamburger SPD eine Spende i.H.v. 13.000 € von Olearius erhielt. Eine Korrelation zwischen der Rückforderung und dem dargestellten Kontakt zwischen den Personen sowie zur Spende an die SPD konnte nie nachgewiesen werden. Wie bereits beschrieben, verurteilte das Landgericht Bonn die Warburg Bank zur Rückzahlung der erstatteten Steuern in voller Höhe. Die Verjährung des Teilbetrages wurde rückgängig gemacht (Daubenberger/Salewski/Schröm 2021). Olaf Scholz wurde im Jahr 2018 Bundesfinanzminister und war in dieser Zeit im vorab behandelten Wirecard-Skandal beteiligt.

7.3 Conclusio

Der Finanzsektor hat hochkomplexe Konstrukte erschaffen zur Umgehung von Gesetzen oder Ausnutzung von Gesetzeslücken. Dazu bedingen sie sich Beraterfirmen, welche oftmals ebenso Regierungen bei der Gestaltung von Gesetzen bedienen. Ausgerichtet ist es auf die Steuervermeidung für Unternehmen oder Steuerhinterziehung im Aktienhandel. Darüber hinaus nutzen sie ihre hochkomplexe Struktur, um die Herkunft der Gelder oder das Vermögen ihrer Kund:innen zu verschleiern. Statt eines Einsatzes von Kreativität für eine Wohlstandsmehrung bewirken diese Aktivitäten Wohlstandsminderungen für die Gesellschaft. Die Schäden durch Cum-Cum oder Cum-Ex-Geschäfte belaufen sich weltweit auf Milliarden, was zugleich aufgrund der erhobenen Gebühren durch den Finanzsektor ein lohnendes Geschäft darstellt. In Bezug auf Steuerhinterziehung wurde die Beteiligung von Banken in Verbindung mit den Offshore-Leaks der Paradise, Pandora und Panama Papers sowie zu einzelnen Agierenden, wie die Anwaltskanzlei Mossack-Fonseca nachgewiesen. In den Panama Papers wurde nachgewiesen, dass 15 Banken aus Deutschland beteiligt waren. Die Strafen für illegale Geschäfte beliefen sich dabei in Millionenhöhe (Peters/Senn 2021:22), was die Einnahmen durch solche Geschäfte trotz dessen nicht weniger attraktiv machte. Beteiligt waren weiterhin Wirtschaftsprüfungsgesellschaften wie die PwC, KPMG, Deloitte und EY um bei der „Steuroptimierung“ (Peters/Senn 2021:22) behilflich zu sein. Dabei sind weder Steuervermeidung noch Vermögensverschiebungen von vornherein illegal. Schäden verursachen sie jedoch trotzdem jährlich in Milliardenhöhe für die Volkswirtschaften. Laut einer Studie aus dem Jahr 2018 werden annähernd 40% aller Gewinne durch weltweit tätige Konzerne in Steueroasen verschoben. Im Jahr 2015 betrug die Verschiebung von Vermögen in verschiedene Steueroasen wie Singapur oder Irland mehr als 540 Mrd. \$. Dadurch entstehen große Schäden allein schon durch die verminderten Steuereinnahmen. Die Schäden für die Volkswirtschaften dürften sich dabei noch weit höher belaufen. Wie die FinCen-Files zeigten, waren Banken aus Europa mit Transaktionen in großem Maße an Geldwäsche und damit an Korruption, Menschenhandel, Drogenhandel, Terrorismus- und Extremismusfinanzierung beteiligt. Bis dato mangelt es an der Kontrolle für adäquate Gegenmaßnahmen (Peters/Senn 2021:22). Und gerade in Bezug auf Geldwäsche wird deutlich, wie sehr Strafverfolgungsbehörden auf die Mitarbeit von Banken angewiesen sind (Svensson 2021:10). Hetzer ist der Meinung, dass aufgrund der Tatsache dass der Finanzsektor mit seinen kriminellen Aktivitäten die OK überholt hat, sie auch der OK zugordnet werden sollte. Dies ist aber bis dato aufgrund falschen Verständnisses der Begriffsdefinition oder Begriffsauslegung der OK nicht erfolgt. Denn schließlich fallen unter die OK nur Gewalt-, Prostitutions- oder Drogendelikte (Hetzer 2014:15). So auch Brorhilker, zuständige Staatsanwältin im Cum-Ex Skandal, welche die Machenschaften der Beteiligten in eine „neue Form der Organisierten Kriminalität“ einordnet (Bognanni/Mascolo 2021).

Wie dargestellt, findet sich Kriminalität unabhängig des gewählten Mittels wie Bargeld, digitalen Währungen und Giralgeld sowohl in der materiellen als auch in der digitalen Welt wieder. Eruiert werden soll im folgenden Kapitel, wer die Digitalisierung des Bargeldes bzw. dessen Abschaffung trotz dessen forciert und welche Gründe dafür bestehen.

8 Exempel der Bargeldabschaffung und der gläserne Mensch

8.1 Die Better-Than-Cash-Alliance, „The war on cash“ und die „Finanzielle Inklusion“

Der „Krieg gegen das Bargeld“ (Häring 2018:24) wurde durch die Mitglieder der Better than Cash Alliance (BTCA) Visa und MasterCard geprägt. Vertreter von MasterCard sprachen auf einer Konferenz im Jahr 2005 davon, gegen das Bargeld „in den Krieg zu ziehen“ (Häring 2018:24). Visa hingegen gab an „den Krieg gegen das Bargeld“ (Häring 2018:24) gewinnen zu wollen. Später heißt es dazu im European Card Review: „Obwohl Banken und Regierungen der Wunsch eint, Bargeld aus dem System zu entfernen, überlassen die Regierungen den anderen die Initiative, weil sie sich sorgen, dass der Krieg gegen das Bargeld in der Öffentlichkeit nicht gut ankommt.“ (Häring 2018:24). Den Krieg gegen das Bargeld aus rein wirtschaftlichem Interesse vertrat MasterCard bis zum Jahr 2010. So äußerte sich Banga, einer der Köpfe MasterCards während eines Interviews im Forbes: „Die Gewinne, so das Unternehmen, werden aus dem Wachstum von Karten und anderen elektronischen Zahlungsmitteln kommen, die ein Produkt dessen sind, was MasterCard-Chef Ajay Banga Ajay Banga (sic!) einen ‚Krieg gegen das Bargeld‘ (Banga 2010 zitiert nach Gutierrez 2010) nennt.“ (Gutierrez 2010). Später wurde der Slogan des Krieges gegen das Bargeld gegen den humanitären Begriff der finanziellen Inklusion getauscht und von der BTCA verwendet. Finanzielle Inklusion bedeutet aus Sicht der BTCA: „Digitales Bezahlen hat sich zu einem wichtigen Werkzeug zur Förderung der finanziellen Inklusion entwickelt, weil es die Kosten von Finanzdiensten für die Armen senkt und die Sicherheit und Bequemlichkeit der Nutzung von Spar-, Zahlungs-, verkehrs- und Versicherungsprodukten erhöht.“ (BTCA zitiert nach Häring 2018:28) und als „als essenziell für die Bekämpfung der Armut und das Erzielen von inklusivem Wachstum“ (Häring 2018:29). Welche Auswirkungen die proklamierte finanzielle Inklusion hat, konnte am Beispiel Indiens verfolgt werden, wo die Entwertung der 500 und 1.000 Rupien Scheine quasi über Nacht erfolgte. Am 08.11.2016 erklärte Ministerpräsident Narendra Modi morgens in einer Fernsehansprache, dass die genannten Denominationen ab Mitternacht keine Gültigkeit mehr hätten. Schätzungen zufolge betraf dies 85% des im Umlauf befindlichen Bargelds. Vorwarnungen einer Demonetisierung hatte es zuvor nicht gegeben. Annähernd 97% aller Zahlungen im Land wurden bis zu diesem Zeitpunkt mit Bargeld durchgeführt und ein Anteil von 94% aller Händler verfügte nicht einmal über die Technik, um bargeldlos zu zahlen zu ermöglichen. Zudem war weder die Mobilfunknetz- noch die Internetabdeckung im Land dafür vorhanden. Allenfalls waren die Voraussetzungen nur rudimentär gegeben. Die ungültigen Denominationen konnten gegen 2.000 Rupien Scheine bei den Banken gewechselt werden. Jedoch gab es weder Automaten, die diese aufgrund ihrer Übergröße annahmen, noch konnten diese in Geschäften getauscht werden, da aufgrund der Knappheit kein Bargeld zur Verfügung stand. Die Bargeldknappheit wurde zudem durch streng limitierte Ausgaben von Bargeld durch die Banken stark forciert. Betroffen waren insbesondere Wanderarbeiter, die bis dato über kein Konto bei der Bank verfügten. Diejenigen, den ein solches Konto zur Verfügung stand, brauchten Tage für den Umtausch des Geldes aufgrund des großen Andrangs bei den Banken. Die Auswirkungen auf kleine Handelsgewerbe waren verheerend. So konnten sie weder Bargeld annehmen oder umtauschen noch waren sie technisch für bargeldlos zahlen ausgerüstet, so dass viele von ihnen ihre Existenz verloren. Ausgewichen wurde bevorzugt auf größere Einkaufszentren, welche als Einzige über die technischen Voraussetzungen des bargeldlos Zahlens verfügten. Durch die fehlende Möglichkeit Löhne auszubezahlen, verloren viele Menschen ihre Arbeitstätigkeit und Arbeitgebende waren nicht mehr in der Lage ihre Produkte oder Dienstleistungen zu veräußern (Häring 2018:75 ff.). Teilweise starben Menschen während des Anstehens oder begingen Suizid aus Verzweiflung ob der Bargeldabschaffung und Existenzberaubung (Häring 2018:78). Im Jahr 2017 waren viele Probleme der Versorgung mit Bargeld noch nicht gelöst. Es kam zu Protesten durch Händler:innen, welche gewaltsam eingedämmt wurden. Händler:innen erhielten oftmals nur Münzen während ihrer Geschäftstätigkeit, jedoch wurden diese nicht mehr von Banken angenommen mit der Begründung, sie seien mit dem Volumen überfordert und dafür nicht ausgelegt. Von Regierungsseite wurden diese Probleme gezielt ignoriert, da eine bargeldlose Gesellschaft durchgesetzt werden sollte. Mit Beginn der Durchsetzung der Bargeldabschaffung wurden die Bekämpfung des Terrorismus, der Schattenwirtschaft und Drogenhandel als Grund für die Maßnahmen angegeben. Prognostiziert wurde, dass ca. ein Drittel des Bargeldes nicht eingezahlt werden

würde, da es inkriminiert sei. Im Herbst 2017 gab jedoch die Notenbank bekannt, dass 99% aller Noten eingezahlt wurden. Im Laufe des Jahres 2016 wurde die Maxime der bargeldabschaffenden Maßnahmen verändert. Vorgeschoben wurden die finanzielle Inklusion für Bedürftige sowie Modernisierungsmaßnahmen innerhalb des Finanzsystems. Ein Teil des Bargelds, welcher tatsächlich Schwarzgeld darstellte, wurde m.H.v. korrumpierten Beamten gewaschen oder durch Andere eingezahlt, welche nicht die Besitzer waren (Häring 2018:80). Auf der Internetseite der BTCA wird in Bezug auf Arme und Frauen propagiert: „Die Umstellung dieser Zahlungen von Bargeld auf Digitaltechnik hat das Potenzial, das Leben von Menschen mit geringem Einkommen, insbesondere von Frauen, zu verbessern.“ (BTCA – „Why digital payments“ o.D.). Vor allem kam jedoch von den Frauen in Indien Proteste gegen die Bargeldabschaffung, da nun ihre finanzielle Situation und Ersparnisse durch Kontenführung vor ihren Männern offengelegt wurden, welche das Geld vertranken oder anderweitig ausgaben. Offensichtlich wurde mit der Abschaffung des Bargelds genau das Gegenteil erreicht, von dem was proklamiert wurde (Häring 2018:81). Die Verbindung zwischen der Bargeldabschaffung Indiens und der BTCA wurde bereits im Jahr 2015 geschaffen. Bei einem Staatsbesuch Obamas trat das Land Indien der BTCA unter dem Schlagwort einer Sicherheitspartnerschaft offiziell bei. Gleichzeitig verpflichtete sich die indische Regierung, eine biometrische Datenbank mit zugehöriger Identifikationsnummer für jeden Einwohner Indiens zu schaffen. Ein Mitglied der BTCA, die United States Agency for International Development (USAID) gründete eine enge Zusammenarbeit mit dem indischen Ministerium für Finanzen, die „Partnerschaft für inklusives bargeldloses Bezahlen“ (Häring 2018:84). Weitere Mitglieder dieser Partnerschaft waren Unternehmen wie MasterCard, Visa sowie Unternehmen aus der Finanzbranche, Telekommunikation und IT. Indien wurde in einer Veröffentlichung des USAID im Jahr 2017 als besonderer Erfolg und als Exempel einer erfolgreichen Bargeldabschaffung ausgeführt (Häring 2018:84). Vorab wurde im Jahr 2016 eine Studie von Google und der Boston Consulting Group veröffentlicht, mit der inhärenten Schlussfolgerung, dass der Markt Indiens einen „500-Milliarden-Dollar-Goldtopf“ (Häring 2018:84 f.) für die Finanzbranche darstelle. Verbindungen zur geplanten Bargeldabschaffung in Indien wurden jedoch abgestritten. Lenkungsausschuss der Studie waren in Vertretung Visa, Vodafone und PayTM, Partner des USAID und indischem Ministerium für Finanzen. Inhalt der Studie war die Gewinnerzielung durch den indischen Finanzmarkt für amerikanische Finanzdienstleister. Schlagwörter wie finanzielle Inklusion wurden nicht erwähnt (Häring 2018:85). Im Jahr 2018 kaufte sich Walmart eine Beteiligung i.H.v. 77% am indischen Online-Handelsunternehmen Flipkart ein, welches zu diesem Zeitpunkt 40% aller Marktanteile des Onlinehandels beherrschte. Der Rest der Anteile an Flipkart wurden u.a. unter Microsoft und dem chinesischen Internetunternehmen Tencent aufgeteilt. Das sicherte eine über 50%ige Beteiligung der USA am indischen Onlinehandel (Häring 2018:82). Bhaskar Chakravorti, Dekan für Global Business an der Fletcher School der Tufts University, gab eine Zusammenfassung der Ergebnisse der Demonetisierung im Harvard Business Review. Dabei bezog sich Chakravorti u.a. auf eine Schätzung des Central Statistics Office (CSO,) indisches Zentralamt für Statistik, welche eine 7%ige Steigerung des Wirtschaftswachstums infolge der Demonetisierung ergab und daraus schlussfolgerte, dass die Demonetisierung keine negativen Auswirkungen auf die Wirtschaft hatte (Chakravorti 2017). Eine im Jahr 2016 veröffentlichte Studie der amerikanischen Beratungsfirma McKinsey und dessen Kooperationspartner Gates-Stiftung, kam bei ihrer Schätzung auf eine Erhöhung des Wirtschaftswachstums in Indien um 10% durch die Demonetisierung. Leiter der Studie war Mor, Aufseher der Notenbank Indiens und Direktor der Bill & Melinda Gates Stiftung Indiens (Häring 2018:86). Chakravorti stellte erhebliche Schwächen bei der Schätzung der CSO fest. Zum einen widerspräche die Studie zahlreichen Berichten über Schließungen von Unternehmen und Fabriken sowie großen Projektverschiebungen. Weiterhin wurden bei den Schätzungen Vergangenheitswerte herangezogen und der Bereich der Schattenwirtschaft nicht berücksichtigt, da dieser nicht durch staatliche Stellen erfasst wird. Schätzungen zufolge beläuft sich dieser auf 45% der Landesproduktion Indiens in dem 94% der Arbeitnehmer beschäftigt sind. Die produzierenden Gewerbe wurden zudem nur in Form von Aktienunternehmen erfasst. Unternehmen aus dem informellen Sektor wurden aus genanntem Grund nicht erfasst. Diese jedoch waren unmittelbar und überwiegend von der Demonetisierung betroffen. Eine Analyse zusätzlicher Daten des letzten Quartals 2016 ergab, dass mehrere Bereiche, e.g. Steuereinnahmen oder Produktionen im Schienengüterverkehr, Produktion von

Nutzfahrzeugen einer Verlangsamung im Wachstum unterlagen. Die Bruttoinlandsproduktwachstumsprognose wurde daraufhin von 7% auf 6,4% vermindert. Große Konzerne wie Nestle oder Unilever meldeten signifikante Gewinn- und Umsatzrückgänge. Allein bei Unilever wurde ein Absatzrückgang von 4% verzeichnet. Traktoren wurden im Vergleich zum vorherigen Quartal zu 10%, Pkw zu 14,9% und Motorroller zu 22% weniger abgesetzt. Bei den Motorrollern war das der niedrigste Wert seit dem Jahr 1997. Gewinner der Demonetisierung waren die Finanzunternehmen, welche die mobilen Wallets anboten. PayTM bspw. verzeichnete einen Anstieg des Verkehrsaufkommens um 435% und 170 Mio. neue Nutzende. Die Transaktionswerte stiegen um 250%. Trotz dieser Fakten gelang es der amtierenden Regierungspartei bei den Wahlen im März 2017 einen großen Sieg zu erzielen. Chakravorti begründet das überraschende Wahlergebnis: „Während wir das Zeitalter von Big Data feiern, ist es vielleicht die ‚große Erzählung‘, die die fundiertesten Entscheidungen herbeiführt: Das haben wir in Großbritannien, in den USA und jetzt in Indien erlebt. Wenn die Menschen das Gefühl haben, dass man für sie kämpft, scheinen selbst die konkretesten Beweise, seien es Daten oder Geschichte, immer weniger Einfluss zu haben.“ (Chakravorti 2017) bezüglich der anfänglichen Behauptung der Regierung, die Demonetisierung würde die Schattenwirtschaft und Korruption bekämpfen (Chakravorti 2017).

Bereits im Jahr 2015 wurde auf einem Treffen der G20 empfohlen: „Die US-Regierung sollte die G20-Regierungen auffordern, sich zu den Zielen der Better than Cash Alliance zu verpflichten - und bei der Erreichung dieser Ziele Fortschritte zu machen -, um den Bemühungen um die Digitalisierung des staatlichen Zahlungsverkehrs Impulse zu verleihen, einschließlich Sozialtransfers. Fortschritte bei den G2P-Zahlungen bilden das Gerüst, auf dem weitere Finanzdienstleistungen aufgebaut werden können.“ (President’s Global Development Council 2015:3). Dabei wurde bereits im Jahr 2010 ersichtlich, worauf die finanzielle Inklusion im Grunde abzielt. So heißt es im Bericht der G20 Financial Inclusion Experts Group: „Eine Milliarde Menschen mit Mobiltelefonen haben nicht einmal ein einfaches Bankkonto. Unter sinkenden Kosten der Informations- und Kommunikationstechnologie, ist die Zeit reif für den Einsatz von Technologie zur Bekämpfung der finanziellen Ausgrenzung. Die technologische Innovation verändert die Kosten und Zugang Gleichung, so dass es für Finanzdienstleister, oft in Partnerschaft, wirtschaftlich tragfähig macht, arme Menschen mit einer breiteren Palette von Produkten und Dienstleistungen zu erreichen.“ (G20 Financial Inclusion Experts Group 2010: V). Mit Finanzdienstleistungen sind bspw. Mikrokredite oder Mikrofinanzierungen benannt. Auf Seite sechs des Berichtes heißt hingegen: „Es gibt eine Fülle von Forschungsergebnissen und Daten zur ‚Mikrofinanzierung‘ (G20 Financial Inclusion Experts Group 2010:6). Diese Daten zeigen, dass Mikrofinanzkunden oft marktübliche Preise für Finanzdienstleistungen zahlen und zuverlässige Kunden sind. Diese marktüblichen Preise können die höheren Transaktionskosten von Kleinkrediten abdecken und enthalten oft erhebliche Risikoprämien. Die Mehrheit der Mikrofinanzanbieter, die eine große Anzahl von Kunden haben, sind profitabel (d.h. finanziell nachhaltig) und werden von sozialen und kommerziellen Investoren und nicht durch Geberzuschüsse finanziert.“ (G20 Financial Inclusion Experts Group 2010:6). Beschlossen von den G20 wurde weiterhin, dass die Consultative Group to Assist the Poor sich der Aufgabe finanzieller Inklusion annehmen solle. Mitglieder dieser Gruppe sind MasterCard, Visa und die Citibank. In Kooperation mit der Allianz für Finanzielle Inklusion (AFI), bestehend aus Banken und Zentralbanken etlicher Länder und der Weltbank wurde die Globale Partnerschaft für finanzielle Inklusion (GPFI) gegründet. Für die Umsetzung der beschlossenen finanziellen Inklusion sicherte sich die GPFI u.a. die Partnerschaften mit der Allianz für Finanzielle Inklusion, der Weltbank-Gruppe und später mit der BTCA, welche 2012 gegründet wurde (Häring 2018:104 f.). Mader fasst die Errungenschaften finanzieller Inklusion und Mikrofinanzierung zusammen. Seit über dreißig Jahren fehle jeglicher Beweis dafür, dass Mikrofinanz die Armut lindern können. Unter dem Schlagwort der finanziellen Inklusion wurde ein neuer Markt definiert, den der Armen. Zusätzlich wurde damit die Bargeldabschaffung offiziell eingeleitet, welche privaten Zahlungsdienstleistern zugutekommt. Profitabel wirkt es sich zudem für die Finanzbranche und Regierungen aus, da sich neben monetärem Profit umfangreiche Daten gewinnen lassen und neue Formen sozialer Kontrolle entstehen (Mader 2017:27). Im Jahr 2017 veröffentlichte der Internationale Währungsfonds (IWF) eine Stellungnahme zu makroökonomischen Folgen einer Bargeldabschaffung. Betont wurde dabei, dass es sich bei den Ausführungen weder um eine Befürwortung der Abschaffung des Bargelds noch um die Ablehnung dessen

handle (Kireyev 2017:4, Nr. 3), sondern lediglich die Vor- und Nachteile einer Abschaffung aufführt. In Punkt 11 wird angeführt, welche Schritte zur Bargeldbeschränkung in verschiedenen Ländern unternommen wurden wie bspw. des Nichtannehmens von Bargeld durch 900 von annähernd 1.600 schwedischen Banken, der gezielte Abbau von Geldautomaten in ländlichen Gebieten Schwedens oder die gesetzliche Berechtigung von Händlern für die Ablehnung von Bargeld (Kireyev 2017:6). Über den ersten von öffentlicher Seite geschaffenen Anreiz für eine geringere Bargeldverwendung spricht Kireyev über eine Möglichkeit des Vorschreibens bargeldloser Zahlungen durch Behörden (Kireyev 2017:13). Aus Sicht von Kireyev besitzt Bargeld lediglich eine nützliche Funktion, als Frühwarnindex für finanzielle Krisen, wenn aufgrund von Vertrauensverlust die Nachfrage nach Bargeld steigt, wie bspw. bei Bank-Runs. Allerdings sei auch dies zweifelhaft, da auf Substitute wie Gold o.a. Rohstoffe infolge einer Bargeldabschaffung zurückgegriffen werden könnte (Kireyev 2017:15). Finanzielle Inklusion sieht Kireyev als Vorteil der Abschaffung des Bargelds. Weiterhin würde dies die Einlagen bei den Banken erhöhen, wenn jeder Mensch über ein Konto verfügen muss. Gleichzeitig warnt Kireyev vor sozialen Auswirkungen wie die Änderungen von Verfassungen, da die Benutzung des Bargelds verfassungsrechtlich gesichert ist. Weiterhin könnte es als Eingriff in Grundrechte wie bspw. das Recht auf Vertrags- und Eigentumsfreiheit angesehen werden und damit sozialen Unfrieden schaffen (Kireyev 2017:22). Am Schluss der Abhandlung kommt Kireyev zu der Auffassung, dass Regierungen das Bargeld abschaffen können, schon allein aus Sicht des Wirtschaftswachstums. Allerdings müsse dies langfristig und in mehreren Schritten angegangen werden wie bspw. die Abschaffung hoher Denominationen im Notenbereich, Festlegung von Barzahlungsobergrenzen und Meldungen grenzübergreifender Bargeldbewegungen. Weiterhin sollten wirtschaftlich Anreize geschaffen werden zur Minderung der Bargeldbewegung bei jeglichen Transaktionen. Verbote der Bargeldverwendung sollten von öffentlicher Seite vermieden werden, da es Einwände hervorrufen könnte. Stattdessen soll auf wirtschaftliches De-Cashing mit Kosten-Nutzen-Abwägungen gesetzt werden unter Zuhilfenahme politischer Anpassungen und gleichzeitiger Aufklärungskampagnen, um den Verdacht einer völligen Kontrolle der Menschen zu zerstreuen (Kireyev 2017:22).

8.2 Bargeldloses Schweden

Traditionell war die Sveriges Riksbank (Schwedische Reichsbank) für die Bargeldmanagementaufgabe in Schweden zuständig. Im Jahr 2004 entschied diese, die Aufgabe an eine Vereinigung zu übertragen, welche zu diesem Zweck gegründet wurde. Gründungsmitglieder dieser Vereinigung, der Banker's Depository (BDB) (BDB Bankernas Depå AB), waren die Danske Bank, die Nordea Bank AB, die Skandinaviska Enskilda Banken AB (SEB) und die Svenska Handelsbanken. Diese hielten das Eigentum an der Gesellschaft zu jeweils 20%. Im Jahr 2010 gründeten dieselben Agierenden weiterhin die Bankomat AB für das Geldautomatenhandling. Die Verwahrung, Zählung und Transport des Bargeldes übernahmen private Sicherheitsunternehmen (Eriksson 2014:3 f.). Im Jahr 2017 fusionierten beide Unternehmen zu einer Gesellschaft, wobei der Name Bankomat AB behalten wurde. Damit war für den größten Teil des gesamten Bargelds Schwedens, lagernd in 10 Depots, und dessen Handling eine Gesellschaft zuständig, welche im Eigentum der „Danske Bank A/S Dänemark, Sverige Filial, Nordea Bank AB (publ), Skandinaviska Enskilda Banken AB (publ), Svenska Handelsbanken AB (publ) und ATM Holding AB (Swedbank AB (publ) und Sparbankerna“ (Manhheimer Swartling 2017) zu jeweils 20% bestehen (Manhheimer Swartling 2017). Laut Eriksson sind insbesondere die Swedbank, die SEB und die Nordea Bank mit ihren bankeigenen Unternehmen MasterCard und Visa die treibenden Kräfte in der Bargeldabschaffung. Ihr Profit wird umso größer, je mehr Zahlungen über Karten vorgenommen werden (Eriksson 2014:4). Im Jahr 2014 legten mehrere Banken Überweisungsgebühren für ihren mobilen Zahlungsdienst Swish i.H.v. einer Krone (~ 1 €) bzw. einer Krone und 50 Öre (~ 1,50 €) fest (Hedelius 2014). Aufgrund von Protesten ihrer Kunden, ließ sich die Umsetzung nicht realisieren (Eriksson 2014:4) Die Banken gaben an, dass es sich um Fehler auf ihrer Webseite handle oder dass es eine solche Entscheidung gar nicht gab. Stattdessen wurde die Einführung der geplanten Gebühren auf unbestimmte Zeit verschoben. Hedelius nahm an, dass die Banken ab diesem Zeitpunkt die Strategie verfolgten, noch mehr Kunden an Swish zu binden, um damit eine Gebühreneinführung umsetzen zu können (Hedelius 2014). Die Macht der Banken

verstärkte sich zusehends. Teilweise kam es zu Ablehnungen von Transaktionen seitens der Banken, wenn es mit „unmoralischen oder unangemessen[en]“ (Eriksson 2014:5) unternehmerischen Aktivitäten verbunden war. So musste ein Geschäft, welches mit Horrorfilmen handelte, Insolvenz anmelden, da keine Bank die Zahlungsabwicklung mehr übernahm. Ebenso wurde die Abwicklung von sämtlichen Zahlungen an Wikileaks eingestellt sowie bei vielen Onlineshops aufgrund unmoralischen Angebots. Die Begründung dafür war, dass mit der Abwicklung gegen Visa-Richtlinien verstoßen werde. Die Strategien der Banken ist es, das Bargeld künstlich zu verteuern sowie den Umgang dessen zu verkomplizieren. Maßnahmen sind bspw. die Schließung von Filialen, die Verweigerung der Annahme und Ausgabe von Bargeld durch Filialen oder der Rückbau von Geldautomaten. Im März 2014 lag die Quote der Filialen in Schweden, welche kein Bargeld mehr annahmen oder ausgaben bereits bei 58%. Geldautomaten wurde stark rückgebaut. Bis zum September 2013 wurden bereits 645 Automaten abgebaut, mit Gründung der Bankomat weitere 250. Schweden nahm damit den letzten Platz gemessen an der Automatendichte in der EU ein. Zusätzlich wurde die Ausgabehöhe immer weiter eingeschränkt. Im Jahr 2007 betrug die Höchstgrenze bei Abhebungen 10.000 Schwedische Kronen (SEK) pro Tag und maximal 25.000 SEK innerhalb von vier Tagen. Im Jahr 2014 gab es bereits eine Obergrenze von 1.000-2.000 SEK pro Tag und 5.000-20.000 SEK innerhalb einer Woche bei den Abhebungen. Für das Abheben von Bargeld mittels Kreditkarte werden inzwischen Gebühren i.H.v. 2-4% auf den Ausgabebetrag verlangt, im Minimum jedoch 20-40 Kronen (Eriksson 2014:6 f.). Seit 2011 ist es zudem verboten, Bargeld in Schließfächern aufzubewahren. Bei Diebstahl lehnen die Banken jegliche Verantwortung ab. Entworfen haben diese Regelung die Banken selbst. Seit 2013 hat der BDB drastisch die Preise für den Währungskauf und Währungsverkauf erhöht. Die Teuerungsrate bewegte zwischen 20% - 1.200%. Aufgrund der Bargeldhoheit konnten die Banken damit ihre eigene Preispolitik betreiben. Eine weitere Maßnahme der Abschaffung ist der regelmäßige Besuch von Banken bei Unternehmen, um sie davon zu überzeugen, künftig nur noch elektronische Zahlungen zu akzeptieren (Eriksson 2014:6 f.). Nach außen werden Gründe für die Abschaffung wie hohe Kosten des Bargelds oder die Schädigung der Umwelt propagiert. Unterstützung erfahren die Banken durch den schwedischen Finanzverband, MasterCard und Visa. Ein anderer angeführter Grund ist, dass Bargeld unhygienisch sei. Initiator der Behauptung ist MasterCard. Weiterhin werden Handelsgeschäfte vor Überfällen gewarnt, wenn sie weiterhin Bargeld verwenden (Eriksson 2014:8 f.). Auf gesellschaftlicher Ebene werden Schattenwirtschaft, Korruption und Lobbyismus sowie Umweltschädigungen durch Geldtransporte gegen das Bargeld gebraucht. Eriksson stellt fest, dass sich die Kriminalität in Schweden aufgrund der Bargeldeinschränkung zum einen ins Internet und zum anderen bspw. bei physischen Diebstählen auf andere wertige Objekte verlagert hat (Eriksson 2014:9). In Bezug auf die propagierten hohen Kosten des Bargelds führt Eriksson eine Studie von Occam aus dem Jahr 2013 an, welche belegt, dass Bargeldzahlungen um mehr als 50% günstiger waren bei der Untersuchung von 50 Unternehmen im Gegensatz zur Zahlung mit Debitkarten. Bei zusätzlicher Berücksichtigung von Zahlungen mit Kreditkarte und deren fällig werdende Gebühren, waren Barzahlungen zu 74% günstiger. Auch das Argument der Umweltschädlichkeit aufgrund des Transportes kann widerlegt werden, denn durch die Verknappung der Automaten insbesondere in ländlichen Gebieten, sind Unternehmen und Privatpersonen gezwungen weite Strecken zurückzulegen, was den CO₂-Ausstoß erheblich erhöht. Auch von Bankenseite selbst wurde das Argument widerlegt. Als die EU eine neue Regelung in Bezug auf den Verzicht von Transaktionsgebühren vorschlug, gaben die Banken an, dass sie dann aufgrund von Mindereinnahmen i.H.v. 5 Mrd. € keinen bargeldlosen Zahlungsverkehr mehr unterstützen würden. Umweltbelange oder Sicherheitsbedenken spielten dann doch keine große Rolle mehr (Eriksson 2014:12).

8.3 Der gläserne Mensch

Bezüglich des gleichzeitig mit der Bargeldabschaffung einhergehenden Aufbaus einer biometrischen Datenbank in Indien äußerte Bill Gates im Jahr 2015: „Es ist eine wundervolle Sache, in ein Land zu gehen und ein breites Identifikationssystem aufzubauen. Indien ist ein interessantes Beispiel. Dort wird das Aadhaar-System, eine zwölfstellige Identifikationsnummer, die mit biometrischen Merkmalen unterlegt ist, gerade im ganzen Land allgegenwärtig. Wir haben vor, diese ID so zu nutzen, dass, wenn Sie irgendeine öffentliche Dienstleistung haben wollen, sagen wir, Sie gehen in eine Arztpraxis, wir in der Lage sein werden, diese ID zu nutzen, um sehr schnell Ihre Gesundheitsdaten aufzurufen. Wenn Sie von einem Teil des Landes in einen anderen umziehen, werden Sie verfolgt [tracked] und bedient.“ (Gates zitiert nach Häring 2018:87). Der Behauptung der Regierung, eine solche Datenbank würde den finanziellen Ausschluss der Armen beenden, widersprach Professorin Khera am Indian Institute of Technology bereits im Jahr 2011 (Häring 2018:88) in Bezug auf die Einführung einer Unique Identification (UID). Hauptgründe für den Widerspruch waren Probleme bei der Umsetzbarkeit und der fehlende Erfolg aufgrund von Identitätsfälschungen. Darüber hinaus wären die Kosten des Systems im Vergleich zu anderen Möglichkeiten immens hoch. Insgesamt gibt Khera zu bedenken, dass die Einführung einer solchen UID den Menschen mehr schaden als nützen würde und schon deshalb öffentlich diskutiert werden müsse (Khera 2011:42). Eine Verbesserung für den Zugang zu staatlichen Leistungen würde nicht eintreten, da es andere Gründe für den sozialen Ausschluss gibt als die angeführte fehlende UID. Zum einen sei dies die unzureichende Abdeckung von staatlichen Programmen mit zu geringer Mittelunterstützung und zum anderen die fälschliche Klassifizierung der Bedürftigen (Khera 2011:39). Nach Einführung der UID im Jahr 2016 traten die befürchteten Nachteile aufgrund technischer Fehler und Bedienfehler ein. Fehlerhaft war u.a. die Scannung der Fingerabdrücke bei der Ersterfassung der biometrischen Daten. Die Folge war, dass viele Menschen aufgrund eines fehlenden Identitätsnachweises nicht für staatliche Programme zugelassen wurden. Einer Studie der Bundesstaatsregierung Telanganas in Indien aus dem Jahr 2017 zufolge, lag die Fehlerrate bei der Ersterfassung von Landarbeitern bei knapp 1/3 aller Erfassten, welche aufgrund dessen keinen Lohn mehr erhielten. Die Einführung der Datenbank mit biometrischen Merkmalen wurde zudem ohne gesetzliche Ermächtigung geschaffen. Erst spät in 2016 schuf die Regierung ein passendes „Finanzgesetz“ (Häring 2018:90) in Bezug auf die Verwendung der UID. Sie wurde verpflichtend für das Zahlen von Steuern, Finanzgeschäfte und für das Beantragen und Empfangen sozialer Leistungen. Private Unternehmen wie Arztpraxen oder Onlineshopping Dienstleister, e.g. Amazon, schlossen sich dem an. Zusätzlich sorgte die Regierung für die Verbindung aller Datenbanken und Daten untereinander. Darüber hinaus ist diese Datenbank von jeder natürlichen und juristischen Person öffentlich einsehbar. Alle Daten sind demnach öffentlich für Jedermann verfügbar, wenn Zugriff auf die gewünschte UID besteht (Häring 2018:90). Dementsprechend häufen sich Fälle über Missbrauch und Schwachstellen des Systems. Wer diese jedoch öffentlich macht, muss mit Repressalien von Regierungsseite rechnen, wie es bereits in mehreren Fällen nachgewiesen wurde. Zudem gibt es keine geklärte Haftungsfrage in Bezug auf Datendiebstahl (Häring 2018:91). Aber nicht nur in Indien gibt es Bestrebungen der totalen Überwachung. Die automatische Kontenabfrage in Deutschland wurde bereits nach den terroristischen Anschlägen in Amerika am 11.09.2001 zum Zweck der Terrorbekämpfung im Jahr 2003 im Kreditwesengesetz (KWG) umgesetzt. Banken und Kreditinstitute müssen gemäß diesem Gesetz Daten über alle Konten und Lagerungsmöglichkeiten bereitstellen. Erfasst werden weiterhin Name, Geburtsdatum, Tag der Einrichtung des Kontos/Depots und Tag der Auflösung sowohl vom Inhaber als auch von den Kontoverfügbaren. Im Jahr 2005 wurde der Zugriffsberechtigtenkreis auf Finanz- und Sozialämter und Arbeitsagenturen ausgeweitet. Rechtliche Grundlage für den Abruf der Informationen bietet § 93 der Abgabenordnung (AO). Im Jahr 2016 wurde die Berechtigung zum Abruf auch den Gerichtsvollziehern gestattet. Seit Ende 2016 gilt dies auch für Beträge unterhalb von 500 €. Bis zum Ende des Jahres 2019 genügte die Übermittlung der Stammdaten der Konten an die abfragenden Behörden, ab Anfang 2020 wurde es auf die Adresse und die Steueridentifikationsnummer erweitert, um eine bessere Auswertung durch das Bundeszentralamt für Steuern (BZSt) durchführen zu können. Nur bei hinreichendem Verdacht bzw. einer hinreichenden Vermutung soll es höchststrichterlich erlaubt sein, Auskünfte einzuholen. Seit 2005 steigt die Zahl der Abrufe rasant. Waren es zu diesem Zeitpunkt noch 10.201 Abfragen, bewegen

sich die Abfragen im Jahr 2020 bereits bei über 1.000.000 Abrufen (Deutscher Bundestag 2021:1 f.) und im Jahr 2021 bei 1.140.000 (Tab. 15) (Seibel 2022).

Tab. 15 Gesamtzahl der durchgeführten Kontenabrufe des BZSt 2005 - 2021

Jahr	2005 ¹	2010 ¹	2015 ¹	2019 ¹	2020 ¹	2021 ²
Anzahl der Zugriffe	10.201 ¹	57.933 ¹	302.150 ¹	915.257 ¹	1.014.704 ¹	1.140.000 ²

Quellen: ¹ Deutscher Bundestag 2021:2, ² Seibel 2022

Ob hier alle Abrufe rechtlich gerechtfertigt waren, kann nicht geklärt werden. Der drohende Missbrauch von Daten ist hingegen nachweisbar zur Realität geworden. Dutzende Fälle belegen, wie durch Behörden Daten verwendet wurden, obwohl keine Rechtmäßigkeit bestand. In Bayern gab es seit dem Jahr 2017 182 Verfahren wegen unrechtmäßiger Datenabfragen innerhalb der Polizeibehörden (Oser 2021). In den Bundesländern Berlin, Hamburg und Hessen kam es zu über 400 unberechtigten Abfragen durch Polizeibehörden. Beim BKA wird lediglich jede eintausendste Abfrage auf Rechtmäßigkeit überprüft (Biselli 2020). Im Jahr 2017 wurden Daten über Personen in Berlin im Einwohnermeldeamt in 561 Fällen unberechtigt abgerufen (Ehmann 2017). Selbst Fälle illegaler Datenabfragen aus politischen Überzeugungen traten auf. Bspw. wurden in Hessen Daten unberechtigt von Polizist:innen aus dem rechtsextremen Milieu abgefragt (dieDatenschützer Rhein Main 2021), in Berlin ließen sich illegale Abfragen auf das linke Milieu zurückverfolgen (Betschka/Fröhlich 2020). Datenmissbrauch wurde in Verbindung mit der Corona-Pandemie festgestellt, indem die Strafverfolgungsbehörden und Staatsanwaltschaften unberechtigt auf die Kontaktverfolgung der Luca-App zurückgriffen, obwohl dieser der reinen Kontaktnachverfolgung dient. Insgesamt soll es sich dabei auf über 500 Fälle belaufen. Zugriff auf diese Daten verbietet dabei das Infektionsschutzgesetz seit dem 19.11.2020. Der Bundesdatenschutzbeauftragte äußerte sich dabei folgendermaßen zu den Missbrauchsfällen: „Solange es Daten gibt, auf die die Behörden grundsätzlich zugreifen können, lassen sich unerlaubte Abfragen und Missbrauch der Daten daher nicht ausschließen.“ (Kelber o.D. zitiert nach Deker 2022). Das BKA sammelte im Jahr 2020 über 100 Mio. Datensätze von grenzüberschreitenden Flugreisenden von 70 Fluggesellschaften. Erfasst wurden dabei die Namen, Adressen, Staatsangehörigkeiten, Rufnummern und die gewählte Zahlungsmöglichkeit. Die Begründung dafür lautete auf Terrorismusbekämpfung. Gespeichert werden diese Daten über fünf Jahre und werden darüber hinaus an Nicht-EU-Staaten übergeben (Lutz/Müller 2021). Regierungen sind mit Staatstrojanern oder spezieller Spionagesoftware ausgestattet. So warnte Apple vor der Verwendung der Spionage Software Pegasus für Smartphones durch Polizei und Geheimdiensten die betroffenen Personen (Biermann 2021a), Facebook warnte 50.000 Nutzende aus mehr als einhundert Ländern, dass sie bereits durch Spionagetätigkeiten mittels dieser Software betroffen sind. Bei späteren Untersuchungen wurde festgestellt, dass trotz bestehender Unsicherheit einer Rechtmäßigkeit und der öffentlichen Kritik des Einsatzes einer solchen Spionagesoftware zum Zeitpunkt des Kaufs diese vom BKA und Bundesnachrichtendienst (BND) verwendet wurden. Bei den Untersuchungen wurde weiterhin festgestellt, dass Regierungen diese Software nutzten, um u.a. Politiker:innen der Opposition, Journalist:innen, Menschenrechtsaktivist:innen sowie deren Familien auszuspionieren und zu überwachen (Biermann 2021b). Seit dem Jahr 2021 sind die Nutzung solcher Spionagetools und die anlasslose Massenüberwachung gemäß BND-Gesetz für die Nachrichtendienste unter Ausnutzung von Sicherheitslücken zulässig (Amnesty International 2021). Heutzutage werden umfassend Daten über Bürger erfasst, e.g. Daten über die Finanzen, Positionsbestimmungen, Kommunikationen sowie biometrische Daten. Darüber hinaus Daten über den Gesundheitszustand, das Konsumverhalten oder Interessen. Der Trend geht dabei zur vollständigen Verknüpfung zum Zwecke der Zusammenhangesuntersuchung oder um Prognosen zu treffen (Ehlers 2018:3). Und wiederholt gibt es Versuche seitens der Bundesregierung bezüglich einer bis dato unzulässigen Vorratsdatenspeicherung. Den letzten Versuch der Einführung gab es im Jahr 2021 in Form eines Positionspapiers seitens der großen Koalition von CDU und SPD während bereits laufender Koalitionsgespräche der Grünen, FDP und SPD. Solche Positionspapiere dienen für Beratungen innerhalb der EU. Darin heißt es, dass die Vorratsdatenspeicherung wieder eingeführt und dabei umfassend ausgeweitet werden soll. Inhaltlich bezieht es sich damit auf Planungen der EU-Kommission mit den angesprochenen Zielen. Geplant sei demnach nicht nur eine Vorratsdatenspeicherung einzuführen, sondern auch die Ausweitung derer auf alle Messenger Dienste und

Videotelefonie bzw. Videokonferenzen. Weiterhin sämtliche Daten bezüglich E-Mail-Kommunikationen, sowie IP-Adressen und dazugehörige Daten: „Um die Identifizierung von Internetnutzern zu ermöglichen, ist es erforderlich, nicht nur die IP-Adresse, sondern auch den Zeitstempel und, wo einschlägig, die zugewiesene Portnummer zu speichern.“ (Bundesregierung 2021 zitiert nach Hipp 2021). Die Begründung für die umfangreiche Speicherung lautet dabei auf den Schutz der nationalen Sicherheit und die Abwehr von Terrorismus. Weiterhin wird die umfangreiche Speicherung von Daten ganzer geografischer Gebiete, Bewegungs- und Kommunikationsdaten in „[...] wohlhabenden Wohngebieten“, Kirchen, Schulen, Einkaufszentren und sogar die von Demonstrationsteilnehmern“ (EU-Kommission o.D. zitiert nach Hipp 2021) angestrebt (Hipp 2021). Dabei ist die Effizienz von Massenüberwachungen mehr als umstritten. In Bezug auf die National Security Agency (NSA) Affäre im Jahr 2013, wo u.a. hochrangige Politiker e.g. Bundeskanzlerin Merkel ausspioniert wurden, untersuchten Bergen et al. die Effektivität von Massenüberwachungen m.H.v. von Telefondaten, nachdem der damals amtierende US-Präsident Obama das Programm verteidigte und angab, dass durch die Maßnahmen mindestens fünfzig terroristische Anschläge verhindert wurden. Eingeführt wurde das Programm nach dem Terroranschlag im September 2011. Bergen et al. kamen zu dem Schluss, dass die Massenüberwachung und Speicherung der Metadaten der Telefonkommunikation keinen signifikanten Einfluss auf die Terroranschlagsverhinderung hatten. Einen nur sehr geringen Einfluss hatte sie bei der Verhinderung terroristischer Handlungen, e.g. die Beschaffung monetärer Mittel für Terrororganisationen. Nachgewiesen wurde der Erfolg der Auswertung der Daten lediglich in einem Fall (Bergen/Sterman/Schneider et al. 2014:1 f.). Luca, Mcleod und Demets et al. untersuchten die Effektivität von biometrischen Massenüberwachungen in Deutschland, den Niederlanden und Polen. Dabei wurden in Bezug auf Deutschland der Einsatz der Gesichtserkennung via Kamera, Fingerabdrücke auf Personalausweisen, die Online Alters- und Identitätsüberprüfung und die digitale Epidemieüberwachung betrachtet. Dabei stellten sie fest, dass die Überwachung aus politischen Gründen und durch das Engagement der Privatwirtschaft entstanden sind. Die Gesichtserkennung wird inzwischen für die Überwachung von Bagatelldelikten und nichtkriminellen Aktivitäten verwendet. Darüber hinaus wurde die Einhaltung der Rechtmäßigkeit der Verwendung der Daten durch Behörden auf die Verantwortung der Bürger abgewälzt. Das gleiche gilt in Bezug auf die Fingerabdruckerfassung auf den Personalausweisen mit dem Risiko, dass die Daten missbräuchlich e.g. für Identitätsdiebstähle verwendet werden können. Darüber hinaus können sie kommerziell durch Unternehmen verwendet werden. Luca, Mcleod und Demets et al. sehen daher die biometrische Massendatenerfassung und Verwendung als einen Eingriff in die verfassungsmäßigen Grundrechte an und warnen, dass dies künftig von weit größerer Bedeutung sein könnte (Luca/Mcleod/De Mets et al. 53 f.). Eine Abwälzung der Datenfreigabe durch die Bürger wurde bereits im Jahr 2018 offenbar. In dem Report des Weltwirtschaftsforums mit dem Titel „The Known Traveller - Unlocking the potential of digital identity for secure and seamless travel“ sind dabei einige Abschnitte für Vorschläge der Abwälzung markant. In dem Bericht geht es um die Erfassung von Daten von grenzüberschreitenden Reisenden. Damit solle die Sicherheit erhöht und die Abfertigung der Passagiere beschleunigt werden, da mit Steigungen im Aufkommen von Reisenden gerechnet wird (World Economic Forum 2018:5). Die Reisenden erhalten eine „Known Traveller Digital Identity“ (World Economic Forum 2018:4), welche auf dem Grundsatz basieren solle „[...]“, dass der einzelne Reisende die Kontrolle über die Verwendung seiner eigenen Identität und ihrer Komponenten hat. Aufgrund dieser dezentralisierten Kontrolle über die Komponenten seiner Identität kann ein Reisender den Nachweis seiner Identitätsinformationen - gesichert durch Distributed-Ledger-Technologie und Kryptographie - während seiner gesamten Reise an staatliche und private Stellen übermitteln. Der Zugang zu verifizierten persönlichen biometrischen, biografischen und historischen Reisedaten wird es den Einrichtungen entlang der Reise ermöglichen, eine erweiterte Risikobewertung vorzunehmen, die Identität der Reisenden zu überprüfen und einen nahtlosen Zugang durch biometrische Erkennungstechnologie zu ermöglichen.“ (World Economic Forum 2018:4). Weiter heißt es auf Seite sechs des Berichts: „Bei den Bemühungen um einen Wandel müssen drei zentrale Werte beachtet werden. Erstens müssen sich die Regierungen verpflichten, individuelle Risikobewertungen von Reisenden einzuführen. Auf diese Weise können sie die große Mehrheit der Reisenden, die ein geringes Risiko darstellen, effizienter identifizieren und bearbeiten. Eine solche Vorabprüfung spart Zeit, die besser für die

Erkennung von Risiken und Bedrohungen genutzt werden kann. Zweitens darf das Streben nach globaler Interoperabilität keinen Vorrang vor der Souveränität der Regierungen bei Entscheidungen über die Sicherheit ihrer Bürger haben. Das Konzept der digitalen Identität des bekannten Reisenden wahrt das Recht der Regierungen, ihre eigenen Einwanderungs- und Sicherheitsentscheidungen zu treffen, und wahrt gleichzeitig den Grundsatz der Verhältnismäßigkeit. Schließlich muss dem Reisenden die Möglichkeit gegeben werden, von einer passiven Rolle zu einer aktiven Partnerschaft im Sicherheitsprozess überzugehen. Indem sie die Weitergabe ihrer digitalen Identität selbst bestimmen, werden die Reisenden in den Sicherheitsprozess eingebunden und kommen in den Genuss einer personalisierten und nahtlosen Reise.“ (World Economic Forum 2018:6). Bereitgestellt durch die Bürger sollen demnach biometrische Daten, biografische Daten und Daten über die geplante Reise. Diese sollen sowohl an staatliche Einrichtungen als auch an private Unternehmen übermittelt werden wie bspw. Hotels, Fluggesellschaften oder Autovermietungen „für die Erstellung von Risikoprofilen, die Überprüfung und den Zugang“ (World Economic Forum 2018:14). Darüber hinaus sollen die Datenabfragen mit nationalen Datenbanken verknüpft werden e.g. für die Identitätsüberprüfung (World Economic Forum 2018:14). Weiterhin heißt es, dass Reisende weiter ihren Status der Vertrauenswürdigkeit ausbauen können, indem sie weitere Daten zur Verfügung stellen können: „Wichtig ist, dass die Reisenden nach dem derzeitigen Vorschlag die Bescheinigungen zu einem Profil des Bekannten Reisenden zusammenfassen und ihren Anspruch auf Einhaltung der Vorschriften, Vertrauen und Legitimität als Reisender zunehmend stärken. Durch den Erwerb weiterer Bescheinigungen wird der Status Bekannter Reisender weiter ausgebaut, was zu einer sichereren und nahtloseren Reise für alle Beteiligten beiträgt.“ (App. 45) (World Economic Forum 2018:15). Welche Daten dies betrifft wird nicht weiter ausgeführt. Kruchem vermutet Daten über den Ausbildungsstand oder Kreditwürdigkeit (Kruchem 2020:2). Im Umkehrschluss bedeuten diese Vorschläge, dass der Reisende grundsätzlich verdächtig ist oder von ihm ein hohes Risiko ausgeht, wenn er nicht freiwillig bereit ist, seine Daten umfassend zur Verfügung zu stellen. Die freiwillige Hergabe der Daten durch den Reisenden und die Nichterfassung in einer zentralen Datenbank soll zudem datenschutzrechtliche Probleme wie die unberechtigte Erhebung durch Behörden oder Privatunternehmen lösen (Häring 2018:209). Das Projekt wurde im Jahr 2021 in den Niederlanden und Kanada gestartet (Kruchem 2020:4). Verfechter sind die USA und die EU (Kruchem 2020:3). Mitglieder des World Economic Forums sind neben zahlreichen Banken, e.g. die DB, HSBC, Citi Bank oder die Standard Bank Group, Zahlungsdienstleister wie Visa, MasterCard und PayPal. Aber auch gemeinnützige Organisationen wie die Bill & Melinda Gates Foundation (World Economic Forum - Our Partners o.D.).

8.4 Conclusio

Die Vorteile des Bargelds sind gleichzeitig die Nachteile für Zahlungsdienstleister, Tech-Unternehmen, Regierungen und den Handel. Sicherheitsbehörden sehen Probleme in der Anonymität des Bargelds. Aber auch die Zahlungsdienstleister und IT-Firmen hadern mit dieser Anonymität, erschwert sie nachweislich eine umfangreiche Datenerfassung und Profilerstellung der Nutzenden (Häring 2018:13 f.). Insbesondere MasterCard und Visa forcieren mit ihren Kampagnen in der Öffentlichkeit die Abnahme von Bargeld aus rein wirtschaftlichen Gründen. Sie streben eine vollständige Abschaffung des Bargelds an, um sämtliche Zahlungen zu digitalisieren in Aussicht auf erhöhte Gewinnmargen. Dazu bedingen sie sich Regierungen, deren Gesetzesbeschlüsse und Maßnahmen, welche das Bargeld als zu teuer, zu unsicher und als Unterstützung für diverse kriminelle Delikte dämonisieren. Darüber hinaus wären die durch die Digitalisierung gewonnenen Daten von Interesse für Regierungen. Weltweit sind die Bestrebungen der Regierungen in der Bargeldabschaffung in Zusammenarbeit mit dem Finanzsektor und Big-Data-Unternehmen zu beobachten (Häring 2018:13 f.). Indien und Schweden sind Beispiele für die angestrebte Bargeldbeseitigung und stellen dar, dass die Abschaffung keineswegs auf der Entscheidung der Nutzenden beruht, sondern stark dem Einfluss exogener Kräfte unterliegt. Ähnliche Bestrebungen sind bspw. in den UK zu beobachten. Seit dem Jahr 2015 ist eine stark schrumpfende Bargeldversorgung festzustellen. Angefangen bei 4.514 Filialschließungen der Banken, davon 736 im Jahr 2021. Die Schließungen sollen im Jahr 2022 fortgeführt werden. Händler weigern sich inzwischen Bargeld anzunehmen mit der Begründung Bargeld übertrage Corona. Große Einzelhandelsketten

forcieren die Abschaffung mit dem Bestreben der Personaleinsparung durch vollständige Automatisierung der Bezahlvorgänge. MasterCard und Visa streben auch hier nachweislich die Abschaffung an in Aussicht auf die Generierung höherer Umsätze und der Einführung von hohen Transaktionsgebühren (Musto 2022). Auch in Deutschland ist der Trend der Einschränkung der Bargeldverfügbarkeit zu beobachten. Unter dem Stichwort der Digitalisierung kam es bereits zu vielen Filialschließungen. Im Zeitraum von 2005 und 2015 schlossen 10.200 Filialen. Das entspricht annähernd 27% aller Filialen (App. 37, App. 38). Besonders die ländlichen Regionen sind davon betroffen (App. 39). (Schwartz/Dapp/Beck et al. 2017:1 f.). Aber auch in den Niederlanden mit 66%, Belgien mit 48% und Dänemark mit 53% Schließungen geht ein Rückbau des Filialnetzes von statten. Deutschland befindet sich gegenüber diesen Staaten im Mittelfeld der Filialdichte (App. 40). Geschätzt wird, dass im Jahr 2035 jede zweite Filiale geschlossen sein wird (App. 41) (Schwartz/Dapp/Beck et al. 2017:3). Schwartz et al. geben an, dass die Filialausdünnung „zu leichten Einschränkungen der Erreichbarkeit“ (Schwartz/Dapp/Beck et al. 2017:4) führt (Schwartz/Dapp/Beck et al. 2017:4). Das bestätigt auch die Verbraucherzentrale Bundesverband (VZBV) im Jahr 2021. Anhand eines Vergleichs zweier Befragungen aus den Jahren 2019 und 2021 kamen sie zu folgenden Feststellungen. Die Befragten gaben an, bereits Probleme in der Beschaffung von Bargeld gehabt zu haben (App. 42) (VZVB 2022:9). Gründe dafür waren (App. 43):

die Nichtverfügbarkeit von Geldautomaten	mit	32%,	
technische Störungen	mit	25%,	
und fehlende Bank- Sparkassenfilialen	mit	16%	(VZVB 2022:10).

Auch bei Bezahlvorgängen traten Probleme auf. So hatten die Befragten Probleme aufgrund (App. 44):

der Aufforderung zur bargeldlosen Zahlung,	23%,
Zahlung mit Bargeld sei nicht erwünscht	19%
oder die Annahme des Bargelds wurde verweigert,	11%
da der Händler nur Kartenzahlung akzeptierte (VZBV 2021:11).	

9 Fazit

Bargeld ist seit tausenden von Jahren in verschiedenen Formen essenziell für die Volkswirtschaft. Der Trend des Zahlungsverhalten in Bezug auf Bargeld ist rückläufig und wird sich auch weiterhin rückentwickeln. Daher ist es umso wichtiger, dass Staaten Bezug nehmend auf unbare Zahlungen in der Verpflichtung sind, Datenschutz, Sicherheit der Daten und vor allem den Missbrauch von Daten streng zu regulieren und zu überwachen. Trotzdem ist zu beachten, dass das Zahlen mit Bargeld gesetzlich verankert ist und wie dargestellt, Freiheit für die Menschen bedeutet. Zusätzlich sorgt es dafür, dass Gebühren für unbare Zahlungen im Rahmen bleiben. Grundsätzlich jedoch sollten die Menschen für sich entscheiden, welches Zahlungsmittel sie wählen und wofür. Daher kann einer Bargeldbegrenzung und Bargeldabschaffung nur widersprochen werden (Noack/Philipp 2016:19). Wie dargelegt wurde, wäre die Bargeldabschaffung weder das Non-plus-ultra für die Kriminalitätsbekämpfung noch die Lösung von Problemen der Makroökonomie, welche durch fehlerhafte wirtschaftspolitische Entscheidungen ausgelöst wurden. Die Beseitigung solcher Probleme sollten nur mit Hilfe der Wirtschaftspolitik erfolgen und nicht durch eine Bargeldabschaffung. Auch die Abwägung der Vorteile digitalen Bargelds mit der eventuellen Verringerung des Datenschutzes sollte grundsätzlich den Menschen überlassen werden. Die Gefahr des Ausweichens auf Substitute wie andere digitale Währungen könnte forciert werden, wenn den Menschen die Abschaffung des Bargelds aufgezwungen wird. Weiterhin wäre es ein „[...] unnötiger Verlust an Freiheit, Rechtssicherheit, Notenbankgewinnen und Effizienz“ (Bacher/Beck 2015:40). Geld stellt Vertrauen in das Bruttosozialprodukt und in die Politik dar. Wenn auch nur geringste Zweifel aufkämen, digitales Geld unterläge einem direkten Zugriff und der Willkür staatlicher Behörden, wäre das Vertrauen darin verloren (Bacher/Beck 2015:40). Die Spuren des Bargelds sind kaum nachzuvollziehen, bei unbaren Zahlungsmethoden schon und bieten damit wichtige Informationsquellen. Es ist heutzutage ein Leichtes, Daten zu analysieren, aufzubewahren und auszuwerten, sowie diese einer Person zuzuordnen. Dies kann durch Unternehmen verwendet werden, um gezielt für Angebote von Gütern oder Dienstleistungen werben zu können. Allein aus Sicht der Umsatzsteigerung sind daher Daten für Unternehmen hoch interessant für Werbemaßnahmen. Daten selbst stellen daher inzwischen ein wichtiges Wirtschaftsgut dar und in der Regel muss nicht einmal eine Vergütung für den Lieferanten der Information gezahlt werden. Zusätzlich können personenbezogene Daten des Zahlungsverkehrs mit weiteren Daten verknüpft werden wie bspw. den Social Media. Der Schutz der Privatsphäre ist das Recht eines jeden Menschen. Diejenigen, welche Zugriff auf personenbezogene Daten und die Möglichkeit einer Analyse haben, können einen tiefen Blick in die Privatsphäre erlangen. Daher bietet Bargeld auch den größten Datenschutz, da es keine Daten hinterlässt. Bargeld ist jedoch nicht nur aus Sicht der Wirtschaft bedeutungsvoll. Bargeldabschaffungs- und Bargeldbeschränkungs-befürworter begrüßen die Möglichkeit stärkerer Kontrollen von Finanztransaktionen in Bezug auf Kriminalität bei elektronischen Zahlungsmethoden. Diesen sind allerdings Gefahren des Missbrauchs der Daten und Freiheitsbeschränkungen für Bürger inhärent, wenn es zu einer Bargeldabschaffung käme. Weiterhin wäre eine Abschaffung einem Generalverdacht auf kriminelle Handlungen gleichgesetzt, was wiederum einen Vertrauensverlust bedeutet. Die Verfügung über umfassende Daten des Einzelnen könnten auch missbräuchlich für überwachende Handlungen verwendet werden, das schließt auch zum Zwecke der Politik nicht aus. Trotz des Prinzips der Rechtsstaatlichkeit muss gewährleistet werden, dass ein Missbrauch seitens der Behörden ausgeschlossen ist, denn die Daten über Finanzen verleihen Behörden zusätzliche Macht. Einem Missbrauch, sei es aus persönlichem, ökonomischem oder politischem Zweck, stehen auch keine strengen Datenschutzgesetze oder Verordnungen entgegen. Es ist nicht auszuschließen, dass einzelne Beamte ihre Kompetenzen überschreiten oder Daten von Geheimdiensten verwendet werden. Selbstverständlich kann Bargeld auch dafür verwendet werden, um Steuern zu hinterziehen. Das ist schon aufgrund seiner Anonymität recht einfach. Das heißt jedoch nicht, dass es ursächlich für eine Steuerhinterziehung ist. Die Ehrlichkeit zur Steuerabgabe liegt grundsätzlich darin, dass die Menschen bereit sind, ihre Steuern zu entrichten und nicht, weil es strenge Prüfungen gibt. Und je respektvoller der Umgang der Steuerbehörden mit den Menschen, umso höher dürfte die Bereitschaft sein, Steuern zu entrichten, vorausgesetzt, dass der zu zahlende Steuerbetrag als angemessen betrachtet wird. Eine Bargeldabschaffung könnte hier das Gegenteil bewirken. Wenn die

Menschen sich in einem gefühlten Zustand der Auslieferung sähen, würden sie ihr Vertrauen verlieren. Vergessen werden darf nicht, was Geld für die Menschen bedeutet. Es gibt ihnen das Gefühl von Sicherheit und Freiheit. Daher ist es nur selbstverständlich, dass die Vorteile einer Bargeldabschaffung bzw. Bargeldbeschränkung der Öffentlichkeit fundiert präsentiert werden, denn dann wäre ein Vertrauensverhältnis zwischen Staat und Bürger gewährleistet. Das Argument eines signifikanten Senkens der Kriminalität ist dabei kein fundierter Grund. Kriminalität korreliert weder zwangsläufig mit Bargeld, noch ist dieses dafür kausal. Weiterhin bestehen bereits andere Methoden für illegale Transaktionen ohne Bargeld. Auch Mai plädiert daher dafür, dass die Entscheidungsgewalt für die Wahl des Zahlungsmittels grundsätzlich beim Nutzenden bleibt. Das Vertrauen scheint bis dato zumindest zu bestehen, denn sonst würde die Nutzung unbarer Zahlverfahren nicht stetig steigen (Mai 2017:17 f.). Wie bereits erwähnt, ist das Grundrecht auf Selbstbestimmung verfassungsrechtlich geschützt. Abgeleitet wurde es vom Bundesverfassungsgericht aus dem Persönlichkeitsschutz gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. In einem Urteil über die Volkszählung stellte der Bundesgerichtshof fest, dass das Erstellen eines umfassenden Profils einer Person mit Hilfe zusammengetragener Informationen durch neue Technologien möglich ist. Oftmals können die Menschen aber nicht beurteilen, wer welche Informationen über sie zusammenträgt und verwendet. Darin sieht der Bundesgerichtshof eine Gefährdung der Entscheidungsfreiheit, denn: „Wer das mögliche Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“ (Rieger 2018:51). Darüber hinaus sind weitere Grundrechte gefährdet. Durch Barzahlungsbeschränkungen bspw. müssen Käufer auf unbare Zahlungsmethoden ausweichen. D.h. Käufer werden mittelbar gezwungen, Verträge mit Zahlkartendienstleistern abzuschließen. Damit wird das Grundrecht der allgemeinen Handlungsfreiheit gem. Art. 2 Abs. 1 GG beschränkt und die daraus entstandene Privatautonomie, „[...] also die Freiheit selbst zu entscheiden, ob, mit wem und mit welchem Inhalt Verträge abgeschlossen werden“ (Rieger 2018:51) (Rieger 2018:50 f.). Das Aufheben der Anonymität von Transaktionen verändert die freiheitlichen Grundrechte der Gesellschaft erheblich. Die Abschaffung von Bargeld wird daher zu Recht als Einschränkung einer ‚geprägten Freiheit‘ (Gersbach/ BMWi 2017:12) angesehen. Für die Ausführung seiner Tätigkeiten ist der Staat zwar berechtigt Informationen zu erheben, jedoch bedingt dies gesetzliche Ermächtigungsgrundlagen. Eine Überschreitung dieser Kompetenzen ist bei der Aufhebung der Anonymität für die Verfolgbarkeit von Transaktionsströmen deutlich gegeben. Die Kriminalitätsbekämpfung darf dabei nicht als Zweck dienen, selbst dann nicht, wenn eine Abschaffung dafür nützlich wäre. Das Argument, Bürger würden bereits Informationen über sich umfangreich im Internet veröffentlichen, kann hier nicht verwendet werden, da jeder Bürger für sich freiwillig entscheidet, welche Informationen er veröffentlicht. Grundsätzlich sollte der Bürger daher nicht durch staatliche Einrichtungen gezwungen werden, diese offenzulegen. Denn: „Zum Recht auf freie Entfaltung der Persönlichkeit gehört es, dass man sich für die Dinge, die man tut oder nicht tut, nicht gegenüber Dritten rechtfertigen muss.“ (Gersbach/ BMWi 2017:12). Da das Bestreben zum Erreichen der Freiheitsbeschränkungen „brandaktuell“ ist, zeigt ein veröffentlichter Artikel über eine geforderte weitere Absenkung der Barzahlungsbeschränkung von 1.000 € in Frankreich unter Abgabe der gleichen Argumente (ntv 15.08.2021). Was eine Illegalität der Verwendung von Bargeld betrifft, ist auch aus Sicht des BMWi grundsätzlich eine fehlgeleitete Debatte. Denn wenn alles verboten werden würde, was eine illegale Handlung erleichtern könnte, dann müssten auch Autos abgeschafft werden, da sie sich als Fluchtmittel oder zum Schmuggel eignen. Die Abschaffung wäre ein Eingriff in die Lebensqualität und würde keiner Verhältnismäßigkeit entsprechen. Auch ist die Verwendung eines Autos nicht von vornherein ein Anzeichen für eine illegale Verwendung und selbst wenn, wäre die Abschaffung aufgrund einer Kosteneffizienz an sich weniger von Vorteil für die Bevölkerung als die daraus erwachsenden Vorteile zur Bekämpfung der Kriminalität (Bundesministerium für Wirtschaft 2017:11). Auch die der Bargeldabschaffung aus hygienischen Gründen ist nicht hinreichend unterlegt. Dann müssten auch hier sämtliche Alltagsgegenstände abgeschafft werden, welcher einer Verkeimung unterliegen wie bspw. die öffentlichen Verkehrsmittel (Hungerland/ Qutizau/ Rotterdam et al. 2017:14). Auch hier würde eine Verhältnismäßigkeit in Frage gestellt. Die Debatte über die Bargeldabschaffung wird insgesamt aus drei Haupt Gesichtspunkten geführt: die Innovationen neuerer Zahlverfahren, die illegitime Verwendung von Bargeld und die beschränkende Wirkung

auf die Geldpolitik. Aus Sicht des BMWi ist nicht einer dieser Gründe verhältnismäßig für die Abschaffung oder Beschränkung durch den Staat. Die rückläufige Tendenz von Barzahlungen ist weiterhin keine Begründung für eine Beschleunigung durch den Staat. Ein Vergleich mit anderen Staaten wie bspw. Schweden ist grundsätzlich obsolet, da es für die eigene Entwicklung unerheblich ist, wie sich Schweden entwickelt, sondern ob die verwendeten Zahlungsmittel auf ein Versagen des Marktes in Deutschland bzw. hinweisen. Dies kann derzeit jedoch nicht festgestellt werden. Der Staat, welcher ebenso am Markt teilnimmt, hat das Prägemonopol. Daraus entsteht die Verpflichtung zur Versorgung mit Bargeld, welche grundsätzlich den Bedarf der Verwender und Nachfrager berücksichtigen muss. Dabei sollten die Kosten der Produktion von untergeordnetem Belang sein, zumal diese nur einen geringen Anteil am Nennwert haben und über die Seigniorage abgedeckt werden. Höher wiegt hier die Anonymität der Zahlung mit Bargeld, denn sie „[...] dient dem verfassungsrechtlich gebotenen Schutz der informationellen Selbstbestimmung der Bürger“ (Gersbach/ BMWi 2017:25). Selbst die Überlegungen, Bargeld würde mit Kriminalität einhergehen, sollte nur eine untergeordnete Rolle spielen, zumal Beschränkungen oder Verbote nur bedingt auf die Kriminalitätsbekämpfung wirken“ (Gersbach/ BMWi 2017:25). Die Schaffung und Mehrung von Reichtum ist das Ziel der Kriminalität in seinen Bestrebungen. Sie ist flexibel, vielseitig und anpassungsfähig. Sie ist weiterhin hervorragend vernetzt, widerstandsfähig und einfallreich in Bezug auf die Umgehung von Gesetzen. Durch ihre Fähigkeit zum Wandel entgeht sie trotz oder aufgrund (nur) marginaler Störungen großflächig der Strafverfolgung (Europol 2021:14). Das zeigt u.a. die Entwicklung des Cybercrimes und der Einsatz neuer Technologien durch die OK (Europol 2020:94 f.). Wie festgestellt, durchströmt die Digitalisierung sämtliche Bereiche des Handels, des Privatlebens, der Gesellschaft und der Wirtschaft und schreitet auch weiterhin stetig voran. Daher ist auch eine Anpassung der Kriminalität an die Digitalisierung nicht überraschend. Annähernd jedes kriminelle Delikt besitzt heute eine Online-Komponente. Kriminelle Aktivitäten haben sich mindestens partiell in die digitale Welt verlagert (Europol 2021:26). Wie dargestellt wurde, ist dabei die Form der Vergütung irrelevant, soweit sie für die Kriminalität von entsprechendem Wert ist. Akzeptiert werden Kryptowährungen oder ähnliche Substitute. Luhmann und Ganßmann folgend bedeutet dies, dass es zum einen viele verschiedenen Formen des Geldes gibt und dieses lediglich ein Kommunikationsmedium in einem sozialen System darstellt. Welches davon zur Kommunikation zwischen den Beteiligten anregt, wird innerhalb der sozialen Wirtschaftssysteme entschieden. Des Weiteren leben soziale Systeme durch die ständige Kommunikation, so dass sie gezwungen sind zu kommunizieren, um nicht ihre Existenz zu verlieren (Berghaus 2011:38). D.h. nichts anderes, als das andere Formen des Geldes gewählt werden, solange sie sinnvoll für die Beteiligten erscheinen. Der Sinn liegt hier in einer weiteren Verwendung, e.g. das Erwerben von Dienstleistungen und Gütern. Solange dies möglich ist, wird das System weiter existieren. Das wird auch daran ersichtlich, dass der stetige Übergang zu einer bargeldlosen Wirtschaft neue Anreize für die Kriminalität geschaffen hat und diese auf die Onlinewelt ausweicht (Europol 2021:62) sowie das Substitute wie Gold, Immobilien oder Schmuck von der Kriminalität akzeptiert werden.

Richtig ist die Annahme, dass Bargeld die Geldpolitik zu einem gewissen Maße in der Negativzinspolitik einschränkt oder sie sogar aushebelt. Jedoch ist die Annahme, es wäre von Vorteil, die Negativzinsen willkürlich hoch wählen zu können nicht korrekt, da sie die Relevanz des Zinssatzes für das finanzielle System verkennt. So wären manchen Institutionen wie bspw. der Versicherungswirtschaft aufgrund eines negativen Zinssatzes die Gewinnerwirtschaftung oder die Kostendeckung verwehrt (Gersbach/ BMWi 2017:25 f.). Inzwischen wird die Rechtmäßigkeit von Negativzinsen angezweifelt. In einem Urteil des Berliner Landgerichts weist das Urteil eine unzulässige Doppelbelastung der Konten mittels Kontoführungsgebühr und zusätzlichen Verwahrgebühren durch die Sparda Bank aus. Zudem würden die Banken hohe Erträge m.H. des Negativzinses erzielen können aufgrund der von der EZB eingeräumten Freibeträge für die Verwahrung von Geld (Landgericht Berlin 20217). Eine Unzulässigkeit von Negativzinsen bestätigte auch das Landgericht Düsseldorf gegenüber der Volksbank Rhein-Lippe über Verwahrtentgelte. Damit folgt das LG Düsseldorf der Auffassung des Berliner LGs (VZBV 2022). Banken können derzeit Kredite zu einem Zinssatz von - 1% bei der Erfüllung bestimmter Voraussetzung von der EZB erhalten. Für die Hinterlegung von Geldern bei der EZB müssen sie einen Strafzins von 0,5% an

die EZB verauslagen. D.h. bei Ausnutzung der von der EZB gewährten hohen Freibeträge beziehen sie Kredite zu einem Zinssatz von - 1%, da die hinterlegten Gelder bei der EZB aufgrund der Freibeträge eine Verzinsung von 0% aufweisen. Sollte das eingelagerte Geld den Freibetrag übersteigen, beträgt der Zinssatz für gegebene Kredite - 0,5%. Im Jahr 2020 machte das bspw. bei spanischen Banken Mehreinnahmen von annähernd 1 Mrd. € aus, bei italienischen Banken waren es 1,6 Mrd. € (Sinn 2021:131). Aber auch deutsche Banken profitieren vom Negativzins. So ergaben Recherchen, dass die DB Einnahmen i.H.v. 69 Mio. € erzielte und die Commerzbank 174 Mio. € im Jahr 2020, welche darüber hinaus im genannten Jahr 26% weniger Negativzins im Vergleich zum Vorjahr an die EZB zahlen musste (Bethmann 2021). Die Weiterberechnung des Negativzinses stellt nach Kirchhof einen Verstoß gegen die Eigentumsgarantie des Staates dar. Diese ermöglicht wirtschaftliche Freiheit und die „eigenverantwortliche Gestaltung seines Lebens“ (Kirchhof 2021:154). Verankert ist dies im Artikel 14 des Grundgesetzes und schützt vor dem Zugriff durch Polizei und Finanzwesen. Daher ist jeder Zugriff als ein „Eingriff in ‚Freiheit und Eigentum‘ “ zu werten (Kirchhof 2021:155). Auch die Wirksamkeit des Negativzinses für eine Konjunkturbelebung muss angezweifelt werden, zeichnen sich doch ab dem Jahr 2020 gestiegene Preise für Gold, Kryptowährungen, Immobilien oder Aktien ab, welches die Suche nach Alternativen für Geld von Vermögenden darstellt (Mayer 2021:227). Luhmann sprach bereits 1994 in Bezug auf die Banken von Parasiten, da sie das Privileg besitzen, ihre Lasten in Gewinnerzielungsabsicht zu veräußern. Sie sind damit in der Lage Illiquidität gewinnbringend zu verwerten und in Liquidität umzuformen (Luhmann 1994:145 f.). Darüber hinaus sind sie, wie dargelegt, in kriminelle Aktivitäten e.g. Vermögensverschiebungen, Steuervermeidung, Steuerhinterziehung mit teilweiser Unterstützung durch die Politik sowie Geldwäsche verwickelt, wovon die Terrorismusfinanzierung, der Drogen- und Waffenhandel profitiert. Banken sind jedoch nicht alleinig an der Bargeldabschaffung interessiert. Zahlungsdienstleister wie MasterCard oder Visa wären quasi konkurrenzlos und könnten die Gebühren frei ihrem Gewinnstreben unterwerfen. Der Handel würde zudem durch eine vollständige Digitalisierung durch Personalabbau profitieren (Musto 2022). Deshalb ist auch dieser an einer Abschaffung interessiert und fördert dies regelmäßig durch Forderungen an die Kund:innen zur bargeldlosen Zahlung oder öffentlichen Werbungen für bargeldloses Zahlen (App. 46). Weiterhin sind sowohl Staaten also auch Banken und Finanzdienstleister über alle Maße an Daten interessiert. Bargeld hat daher eine Schutzfunktion vor ausufernder Überwachung durch den Staat und anderen Interessengruppen. Millionen Menschen sind auf die Verfügbarkeit von Bargeld angewiesen. Weiterhin bietet es Schutz für Randgruppen e.g. Migranten, Obdachlose, Menschen mit Beeinträchtigungen oder Sexarbeitern. Ältere wären ebenso von einer Abschaffung betroffen. In den UK bspw. macht das einen Anteil von annähernd 2,4 Mio. aus. Allein das ist für sich bereits ein signifikanter Grund dafür, dem Finanzwesen nicht die Kontrolle über das Geld zu geben. Nicht zu vergessen, dass Banken nicht auf utilitaristischer Basis wirtschaften, weil sie grundsätzlich nur den Menschen Einkommen in Form eines Kredites gewähren, welche sie als risikolos oder risikoarm betrachten. Bargeld ermöglicht weiterhin Kontrolle über die Ausgaben und hilft damit benachteiligten Menschen mit dem Umgang von Geld und dem Zugang von Inklusion. (Musto 2022). Weiterhin ist es nicht betroffen von Cyberangriffen in Bezug auf Diebstahl oder Stromausfälle durch Blackouts, welche u.a. durch Klimaerscheinungen wie Überflutungen, Stürme, Erdbeben oder durch Cyberangriffe selbst entstehen können. So ist es durchaus möglich, dass Cyberkriege unter Staaten zu einem Großangriff auf die kritische Infrastruktur, e.g. die Energieversorgung eines anderen Staates führt. Dafür gab es in der Vergangenheit bereits mehrere Beispiele. So soll die russische Hackergruppe REvil für den Cyberangriff auf Kaseya verantwortlich sein, welcher u.a. dafür sorgte, dass in Schweden über 800 Filialen von Coop nicht mehr geöffnet werden konnten. (Hochstätter 2022). Ein weiteres Beispiel ist der Angriff auf SolarWinds, einem IT-Dienstleister, welcher von tausenden Firmen und Behörden weltweit genutzt wird. Über das Kompromittieren eines Updates von SolarWinds und dessen Übertragung auf die Kund:innen gelang es den Hackern dabei sogar ins Pentagon einzudringen. Betroffen waren viele Unternehmen der kritischen Infrastruktur und Behörden. Auch hier sollen russische Hacker beteiligt gewesen sein (Beuth 2020). Das Hacken im Auftrag von Staaten durchgeführt werden, zeigen die Vermutungen in Bezug auf die Hackergruppe Lazarus. Diese soll im Auftrag Nordkoreas Banken in den USA gehackt und dabei mehr als eine Mrd. \$ erbeutet haben (Muth 2021). Digitales Geld wäre bei einem solchen Angriff auf

die Energieversorgung oder das Finanzwesen selbst ebenso betroffen. So wurde im Februar 2022 ein Cyberangriff auf ukrainische staatliche Institute verzeichnet, bei dem auch staatliche Banken betroffen waren. Das Resultat waren nicht mehr durchführbare Kartenzahlungen (ntv 15.02.2022). Unvorstellbar wäre zudem eine Welt, in der bestimmte Agierende jederzeit wissen, was wann wo gekauft wurde. Oder darüber hinaus, Jemand der entscheidet was gekauft werden darf. Wie der Fall des Horrorvideoladens in Schweden zeigt, ist dies kein zukünftiges, sondern ein reales Szenario mit Hilfe von digitalen Zahlungsmöglichkeiten. Gleichzeitig wäre eine Welt unvorstellbar, in der Käufe und Verkäufe moralischen Erlaubnissen unterliegen würden oder in der der Zugang zum Finanzsystem abhängig gemacht wird von bspw. politischen Einstellungen (Eriksson 2014:13). Wie dargestellt, wird die Abschaffung des Bargelds von Jenen forciert, welche selbst nicht davor zurückschrecken kriminelle Methoden anzuwenden, e.g. der Finanzsektor, welcher auf die Maximierung seiner Gewinne abzielt und damit nur einer Bereicherung dient. Zum anderen sind es Jene denen wir vertrauen sollen und im Vertrauen unsere Daten überlassen, e.g. die Politik im Streben nach Macht durch totalitäre Überwachung oder Privatunternehmen, die darauf aus sind, ihr Profiling vom Menschen zu perfektionieren. Unterstützt durch unwahre Behauptungen sollen die Menschen von einer Bargeldabschaffung überzeugt werden, ohne sie dabei aufzuklären, welche Nachteile daraus erwachsen würden oder welche Nachteile bereits bestehen. Dies erfolgt durch eine Minorität mit monetären Bereicherungs- oder totalitärer Überwachungsbestrebungen.

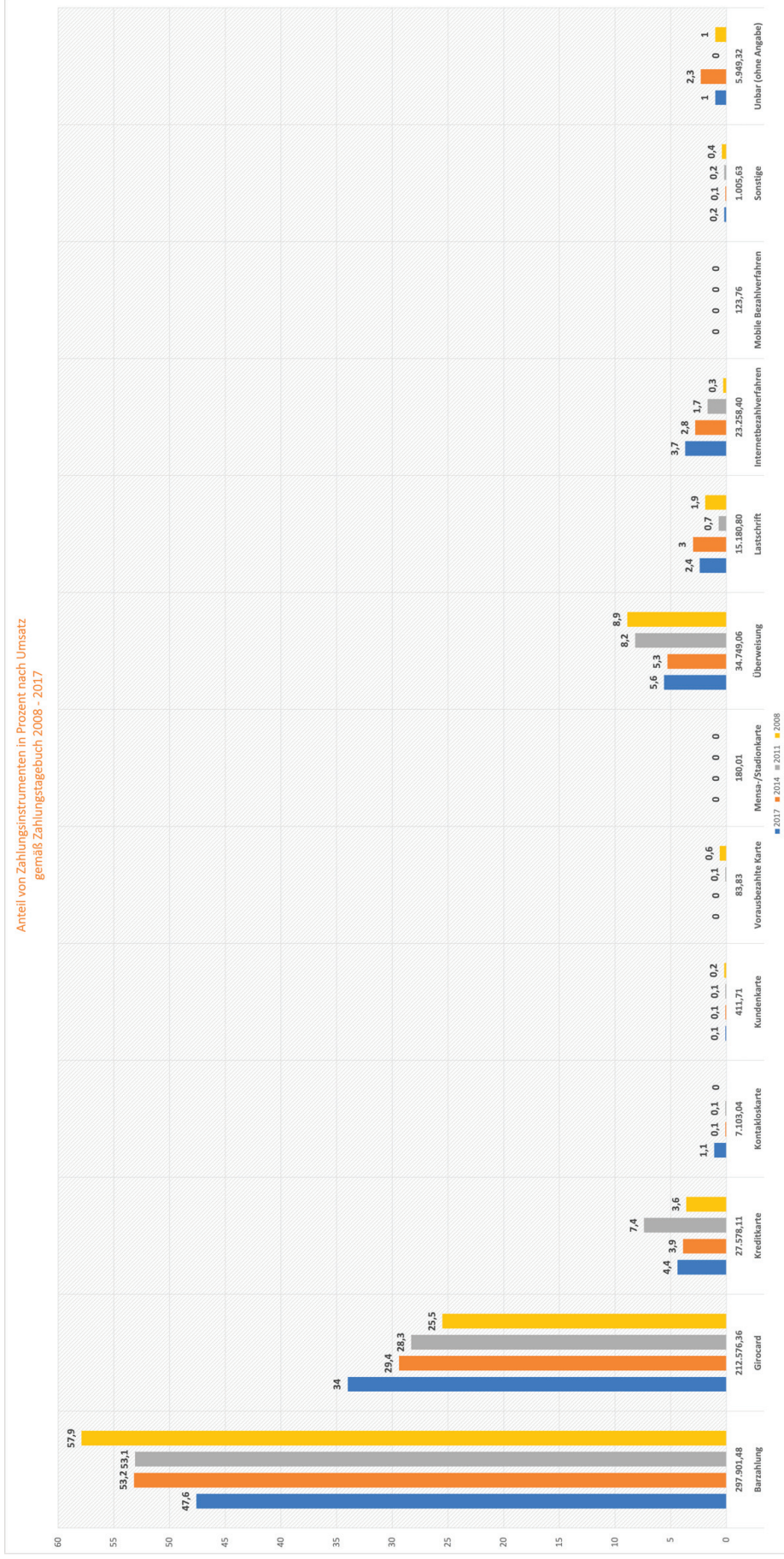
Ob Dostojewski tatsächlich beim Schreiben seines Buches „Aufzeichnungen aus einem Totenhaus“ den Gedanken hatte, Bargeld sei „geprägte Freiheit“ (Dostojewski 1861/1862:40), lässt sich heute nicht mehr feststellen. Fakt ist jedoch, dass Bargeld Freiheit bedeutet, da es uns ermöglicht zu tun und zu lassen was wir möchten, ohne eine etwaige Erfassung oder mit der Pflicht Rechenschaft ablegen zu müssen. Daher sollte bei dem nächsten Bezahlvorgang gut überlegt werden, ob mit Bargeld bezahlt und der Weg der Freiheit gewählt wird oder ob weiter zunehmend unbar bezahlt werden soll mit der Gefahr der Auslieferung einer ubiquitären Möglichkeit einer Überwachung oder einer Entscheidungsmacht Dritter.

Appendix

App. 1	Anteil von Zahlungsinstrumenten in Prozent nach Umsatz gemäß Zahlungstagebuch 2008 - 2017	102
App. 2	Verwendung von Zahlungsinstrumenten in unterschiedlichen Betragsbereichen	103
App. 3	Anforderungen an Zahlungsmittel.....	104
App. 4	Einschätzungen zum Bargeld	105
App. 5	Prozentuale Entwicklung des Münzzählvolumens Berlin	106
App. 6	Prozentuale Entwicklung des Notenzählvolumens Berlin.....	106
App. 7	Gesamtzählvolumen Berlin in %.....	106
App. 8	Prozentuale Entwicklung des Notenzählvolumens CC Neubrandenburg.....	107
App. 9	Prozentuale Entwicklung des Münzzählvolumens CC Neubrandenburg	107
App. 10	Prozentuale Entwicklung des Geldvolumens CC Neubrandenburg	107
App. 11	Banknotenumlauf im Eurosystem	108
App. 12	Entwicklungen der ausgegebenen Banknoten	109
App. 13	Was denken Sie, ist am unhygienischsten?	110
App. 14	Keimbelastung auf Zahlkarten.....	111
App. 15	Kritik an Erhebungsmethoden	112
App. 16	Was ist eine Blockchain?.....	113
App. 17	neun Säulen des Cybercrime-as-a-Service (CCaaS).....	114
App. 18	Aktuelle Kryptomärkte auf DarknetStats	115
App. 19	Screenshot „The hidden wiki“ Net	116
App. 20	Screenshot „The hidden wiki“	117
App. 21	Screenshot „UK Guns and Ammo Store“	118
App. 22	Screenshot „EuroGuns“	118
App. 23	Screenshot „USA Citizenship“	119
App. 24	Screenshot „UK Passports“	119
App. 25	Screenshot „Rent a Hacker“	120
App. 26	Screenshot „Acc Market“	121
App. 27	Screenshot „Dark Mixer“	121
App. 28	Screenshot „Mixabit Bitcoin Mixer“	122
App. 29	Screenshot „EuCanna“	122
App. 30	Screenshot „420prime“	123
App. 31	Screenshot „Tom and Jerry Store“	123
App. 32	Screenshot „DCdutchconnectionUK“	124
App. 33	Notable Cryptocurrency Thefts 2011-2021	125
App. 34	Organisation Chart Wirecard Group.....	126

App. 35	Cum-Ex-Geschäfte Ablauf: Vor und am Dividendenstichtag	127
App. 36	Cum-Ex-Geschäfte Ablauf: nach dem Dividendenstichtag.....	128
App. 37	Filialrückbau zuletzt mit Tempoverschärfung.....	129
App. 38	Alle Kreditinstitutstypen bauen ab	129
App. 39	Ausdünnung in der Breite.....	130
App. 40	Filialdichte in Deutschland im Mittelfeld.....	131
App. 41	Filialdichte 2015 (links) und 2035 (rechts)	132
App. 42	Probleme beim Bargeldbezug (1/2).....	133
App. 43	Probleme beim Bargeldbezug (2/2).....	133
App. 44	Probleme bei Zahlung mit Bargeld.....	133
App. 45	Building a Known Traveller status	134
App. 46	Bye-Bye Bargeld	135

App. 1 Anteil von Zahlungsinstrumenten in Prozent nach Umsatz gemäß Zahlungstagebuch 2008 - 2017

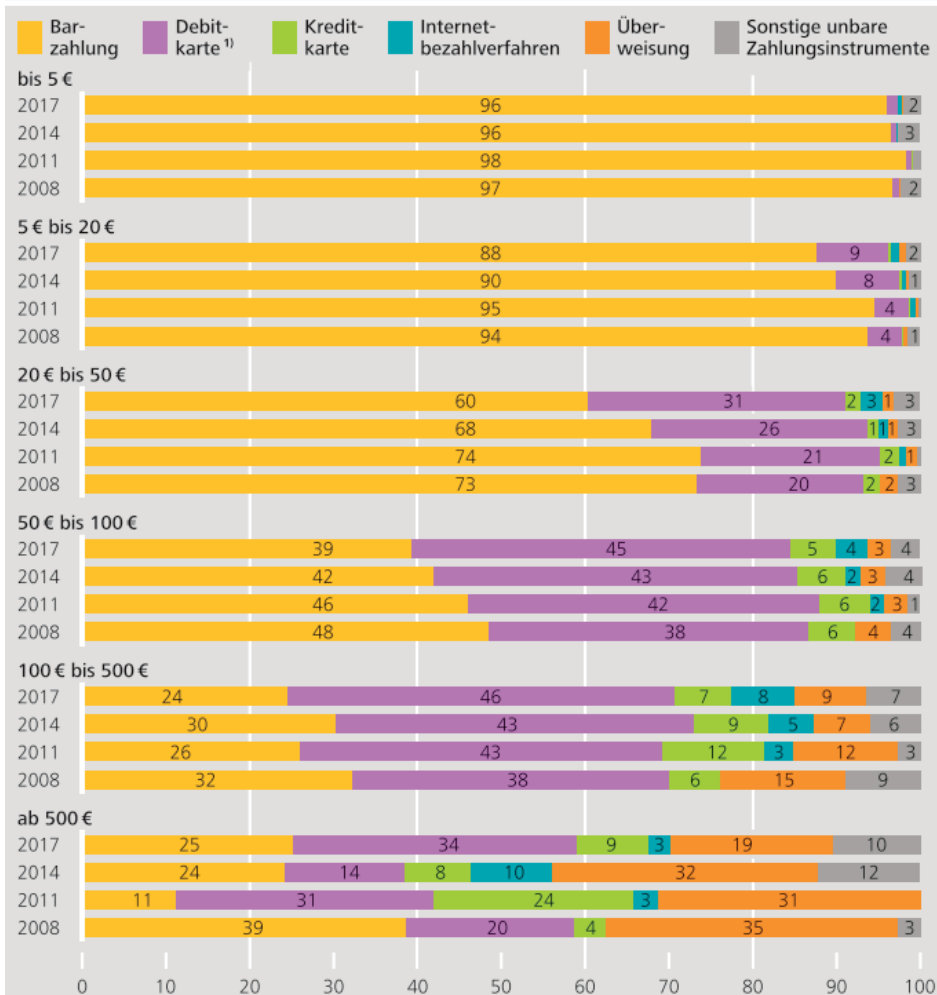


Quelle: eigene Darstellung in enger Anlehnung an Deutsche Bundesbank 2018:24

App. 2 Verwendung von Zahlungsinstrumenten in unterschiedlichen Betragsbereichen

Verwendung von Zahlungsinstrumenten in unterschiedlichen Betragsbereichen

Angaben in % der Transaktionsanzahl, gemäß Zahlungstagebuch



Die Grafik weist den Anteil der verwendeten Zahlungsinstrumente im jeweiligen Betragsbereich gemessen an der Transaktionszahl aus. Das heißt zum Beispiel, dass im Jahr 2017 96% aller Zahlungen bis zum Wert von 5 € mit Bargeld durchgeführt wurden. Aus Gründen der Übersichtlichkeit wurde auf die Beschriftungen für einige Zahlungsinstrumente (< 1%) verzichtet. Abweichungen zu 100% ergeben sich aus Rundungsdifferenzen. Basis: alle Transaktionen, die von den Teilnehmern eingetragen wurden, die das Zahlungstagebuch ausgefüllt haben.

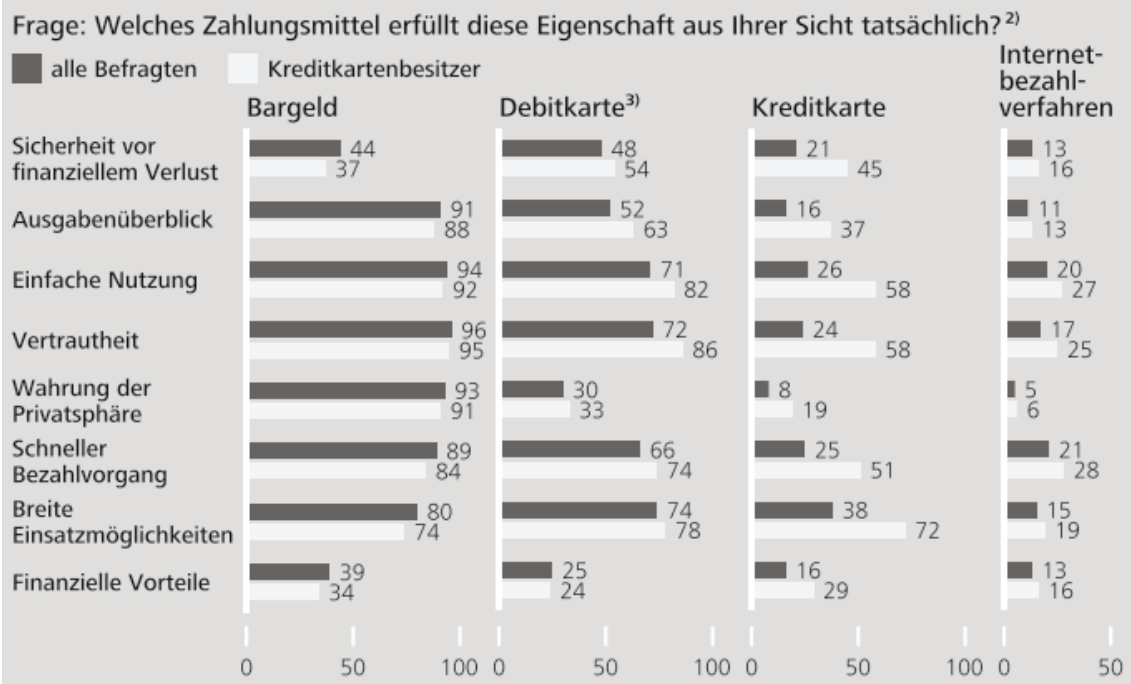
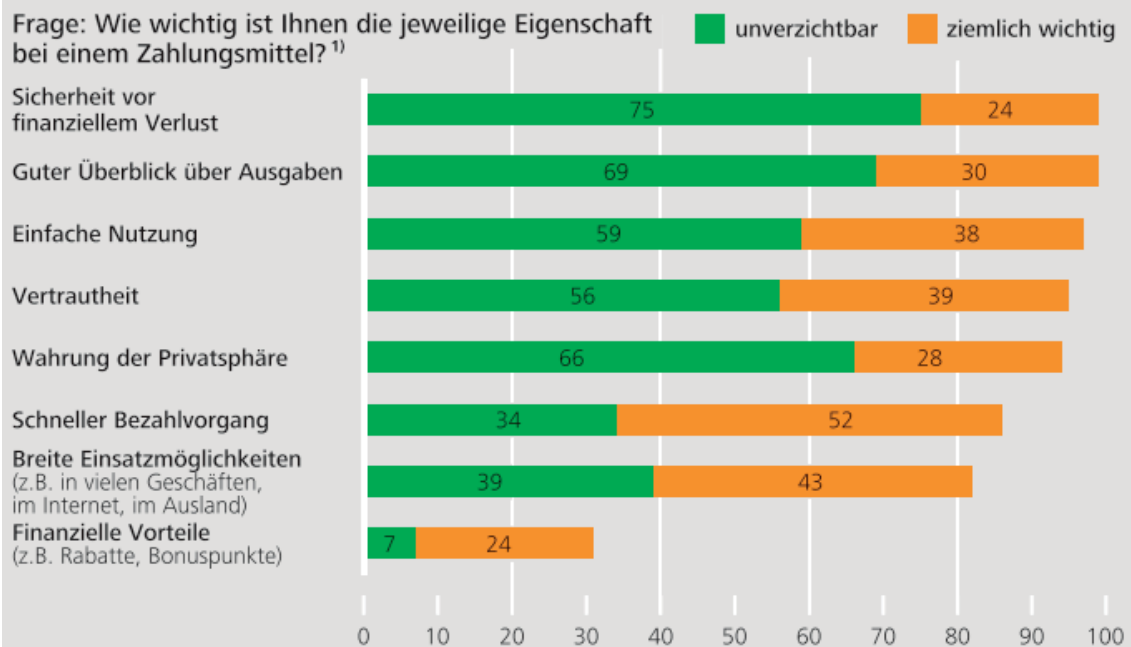
¹ girocard und Debitkartenprodukte der internationalen Kartensysteme.
Deutsche Bundesbank

Quelle: Deutsche Bundesbank 2018:28

App. 3 Anforderungen an Zahlungsmittel

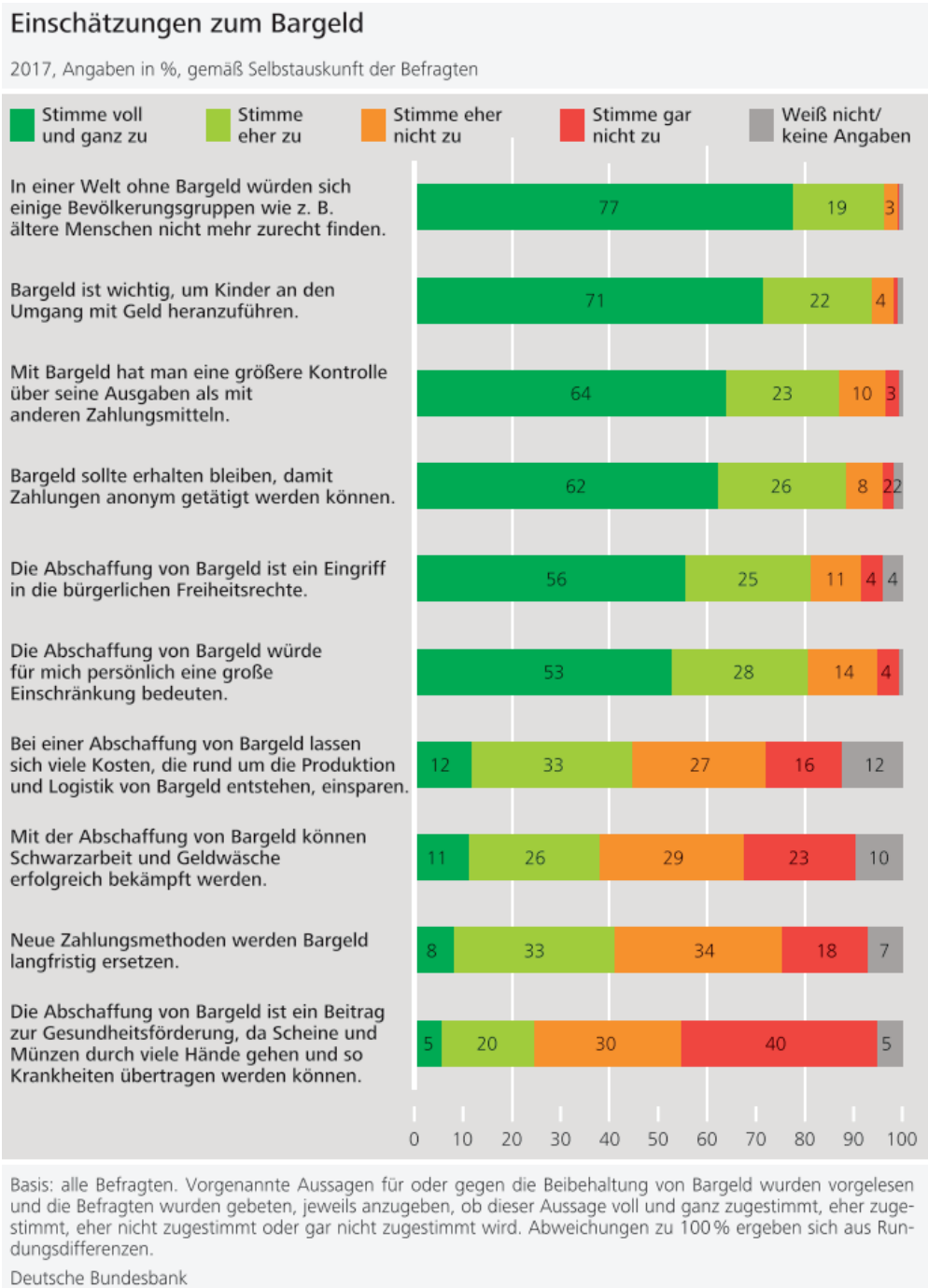
Anforderungen an Zahlungsmittel

2017, Angaben in %, gemäß Selbstausskunft der Befragten



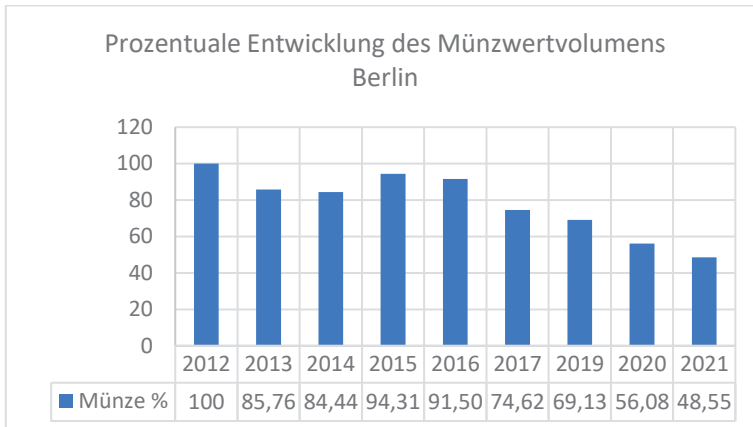
1 Basis: alle Befragten. **2** Basis: alle Befragten und nur Kreditkartenbesitzer. **3** girocard und Debitkartenprodukte der internationalen Kartensysteme.
Deutsche Bundesbank

App. 4 Einschätzungen zum Bargeld



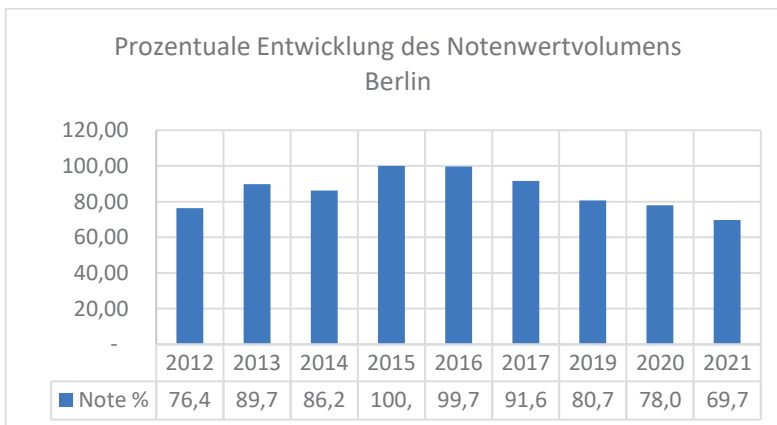
Quelle: Deutsche Bundesbank 2018:38

App. 5 Prozentuale Entwicklung des Münzzählvolumens Berlin



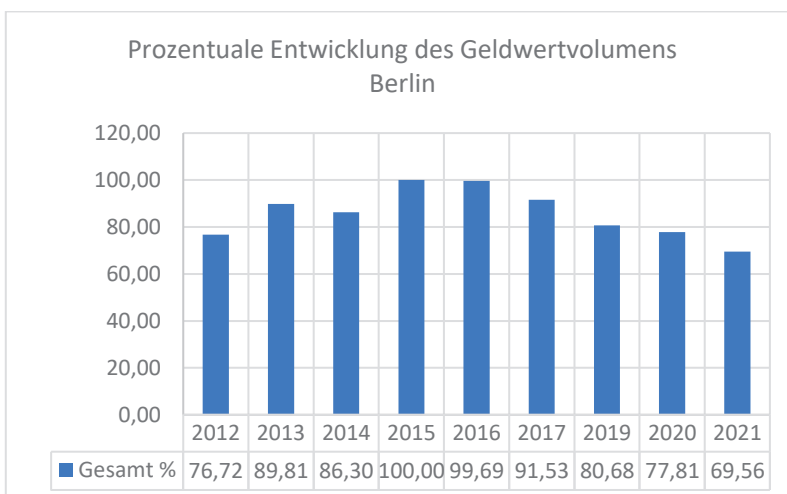
Quelle: Schmidt 2022:3

App. 6 Prozentuale Entwicklung des Notenzählvolumens Berlin



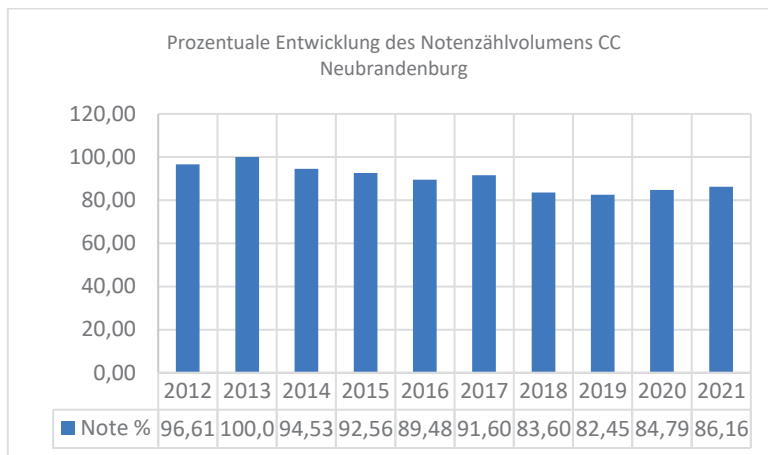
Quelle: Schmidt 2022:3

App. 7 Gesamtzählvolumen Berlin in %



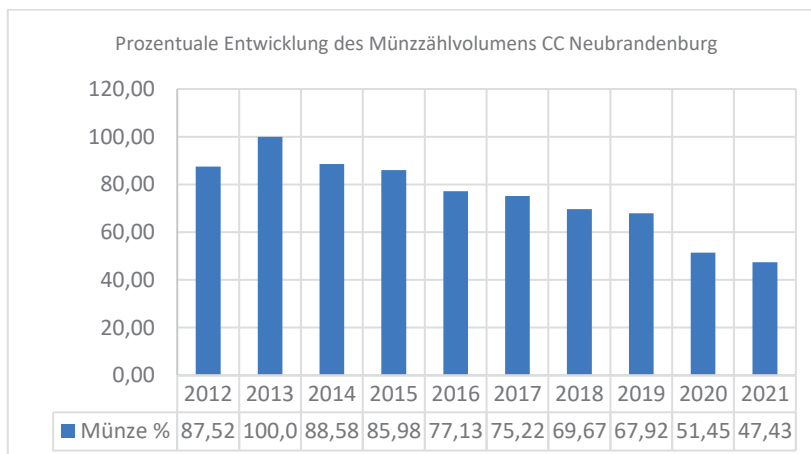
Quelle: Schmidt 2022:4

App. 8 Prozentuale Entwicklung des Notenzählvolumens CC Neubrandenburg



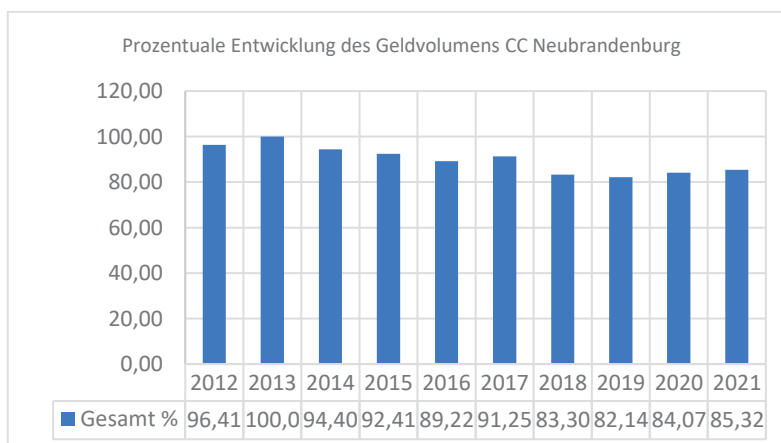
Quelle: Schmidt 2022:6

App. 9 Prozentuale Entwicklung des Münzzählvolumens CC Neubrandenburg



Quelle: Schmidt 2022:6

App. 10 Prozentuale Entwicklung des Geldvolumens CC Neubrandenburg



Quelle: Schmidt 2022:7

App. 11 Banknotenumlauf im Eurosystem

Angaben zum Jahresende						
	Ausgegebene Menge in Mrd €			Jährliche Wachstumsraten		
	Eurosystem	Bundesbank	Eurosystem ohne Bundesbank	Eurosystem	Bundesbank	Eurosystem ohne Bundesbank
2002	358,5	128,9	229,7	–	–	–
2003	436,1	166,0	270,2	21,6 %	28,8 %	17,6 %
2004	501,3	199,7	301,5	14,9 %	20,4 %	11,6 %
2005	565,2	228,9	336,3	12,8 %	14,6 %	11,6 %
2006	628,2	255,2	373,0	11,2 %	11,5 %	10,9 %
2007	676,6	283,3	393,3	7,7 %	11,0 %	5,5 %
2008	762,8	328,4	434,4	12,7 %	15,9 %	10,4 %
2009	806,4	348,1	458,3	5,7 %	6,0 %	5,5 %
2010	839,7	366,7	473,0	4,1 %	5,4 %	3,2 %
2011	888,6	391,8	496,9	5,8 %	6,8 %	5,1 %
2012	912,6	427,5	485,1	2,7 %	9,1 %	–2,4 %
2013	956,2	461,5	494,7	4,8 %	8,0 %	2,0 %
2014	1.016,5	508,4	508,1	6,3 %	10,1 %	2,7 %
2015	1.083,4	552,6	530,8	6,6 %	8,7 %	4,5 %
2016	1.126,2	592,2	534,0	4,0 %	7,2 %	0,6 %
2017	1.170,7	634,7	536,0	4,0 %	7,2 %	0,4 %
2018	1.231,1	690,7	540,5	5,2 %	8,8 %	0,8 %
2019	1.292,7	749,5	543,2	5,0 %	8,5 %	0,5 %

Quelle: Deutsche Bundesbank, 2020a:4

App. 12 Entwicklungen der ausgegebenen Banknoten

Angaben in Mrd € zum Jahresende								
	5 €	10 €	20 €	50 €	100 €	200 €	500 €	Gesamt
2002	6,0	16,4	39,5	121,7	67,3	24,2	83,4	358,5
2003	6,1	16,9	41,1	144,8	81,0	27,1	119,2	436,1
2004	6,2	17,0	41,6	162,8	91,9	28,6	153,1	501,3
2005	6,4	17,6	43,2	181,2	101,8	29,8	185,2	565,2
2006	6,7	19,0	46,7	203,9	111,6	30,6	209,7	628,2
2007	7,1	19,7	49,4	222,1	120,9	31,1	226,3	676,6
2008	7,4	20,3	52,4	245,6	138,1	34,0	265,0	762,8
2009	7,5	20,4	53,8	260,0	147,2	35,7	281,9	806,4
2010	7,6	20,4	55,0	277,5	155,1	36,1	287,9	839,7
2011	7,7	20,7	57,1	302,3	165,0	36,3	299,6	888,6
2012	8,1	21,7	59,8	321,9	170,6	36,9	293,7	912,6
2013	8,4	21,6	61,8	348,1	185,0	39,8	291,6	956,2
2014	8,6	22,4	64,7	375,4	201,6	40,8	303,0	1.016,5
2015	8,8	23,3	68,8	419,9	214,5	41,4	306,8	1.083,4
2016	9,0	23,9	71,8	461,6	243,3	46,7	269,9	1.126,2
2017	9,3	25,0	76,6	491,3	262,4	49,3	256,8	1.170,7
2018	9,7	26,3	80,4	522,3	280,4	51,1	260,8	1.231,1
2019	9,9	27,5	83,8	560,8	305,1	82,5	223,0	1.292,7

Quelle: Deutsche Bundesbank, 2020a:7

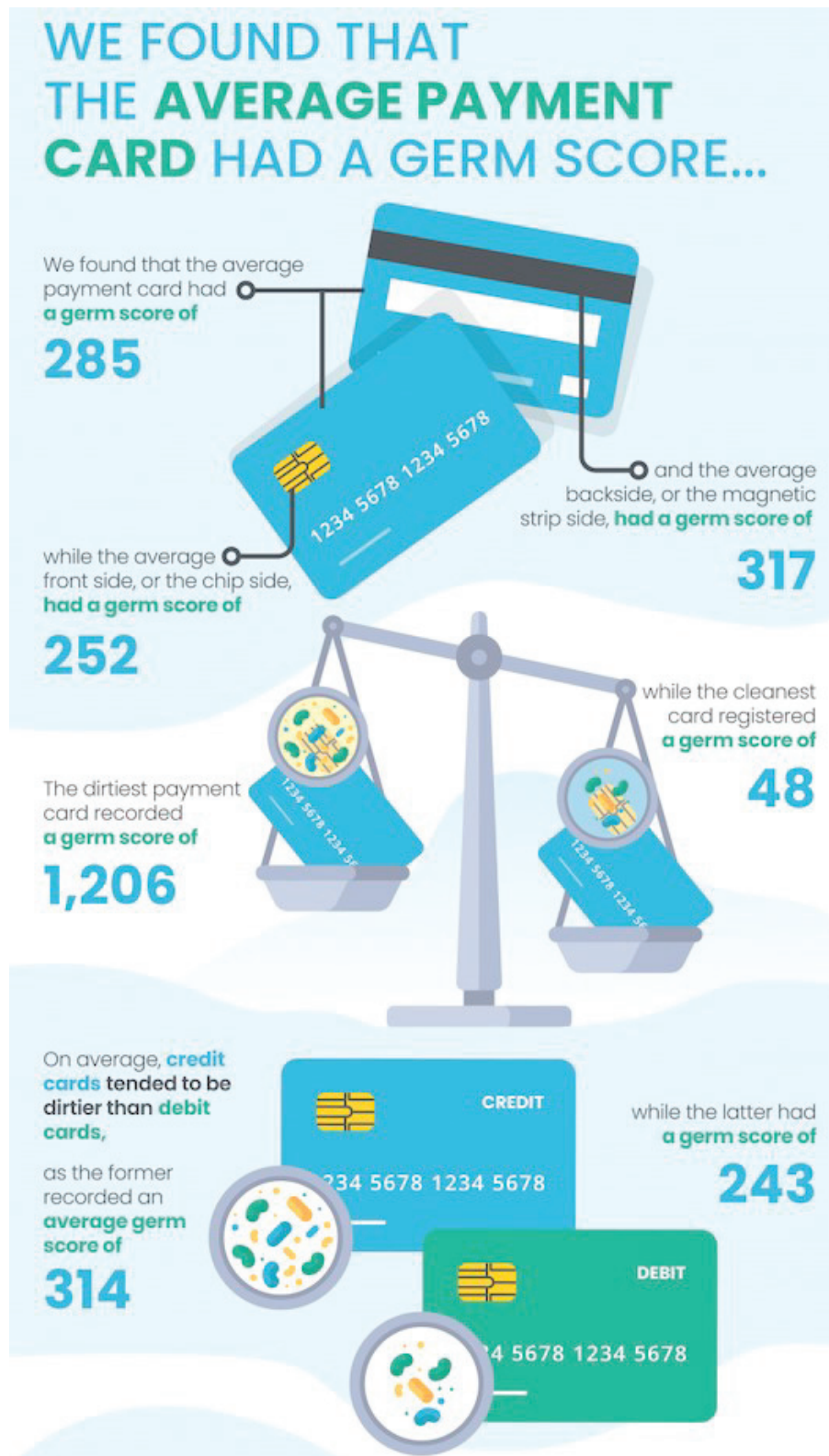
App. 13 Was denken Sie, ist am unhygienischsten?



* Prozentanteil der Befragten, die Geld für den unhygienischsten Gegenstand halten
Die Untersuchung wurde von TNS durchgeführt und fand vom 14. bis 20. Dezember 2012 statt.

Quelle: mastercard Engagement Bureau, 2013, <https://newsroom.mastercard.com/eu/de/photos/infografik-mastercard-dirty-cash/>, abgerufen am 17.07.2021

App. 14 Keimbelastung auf Zahlkarten



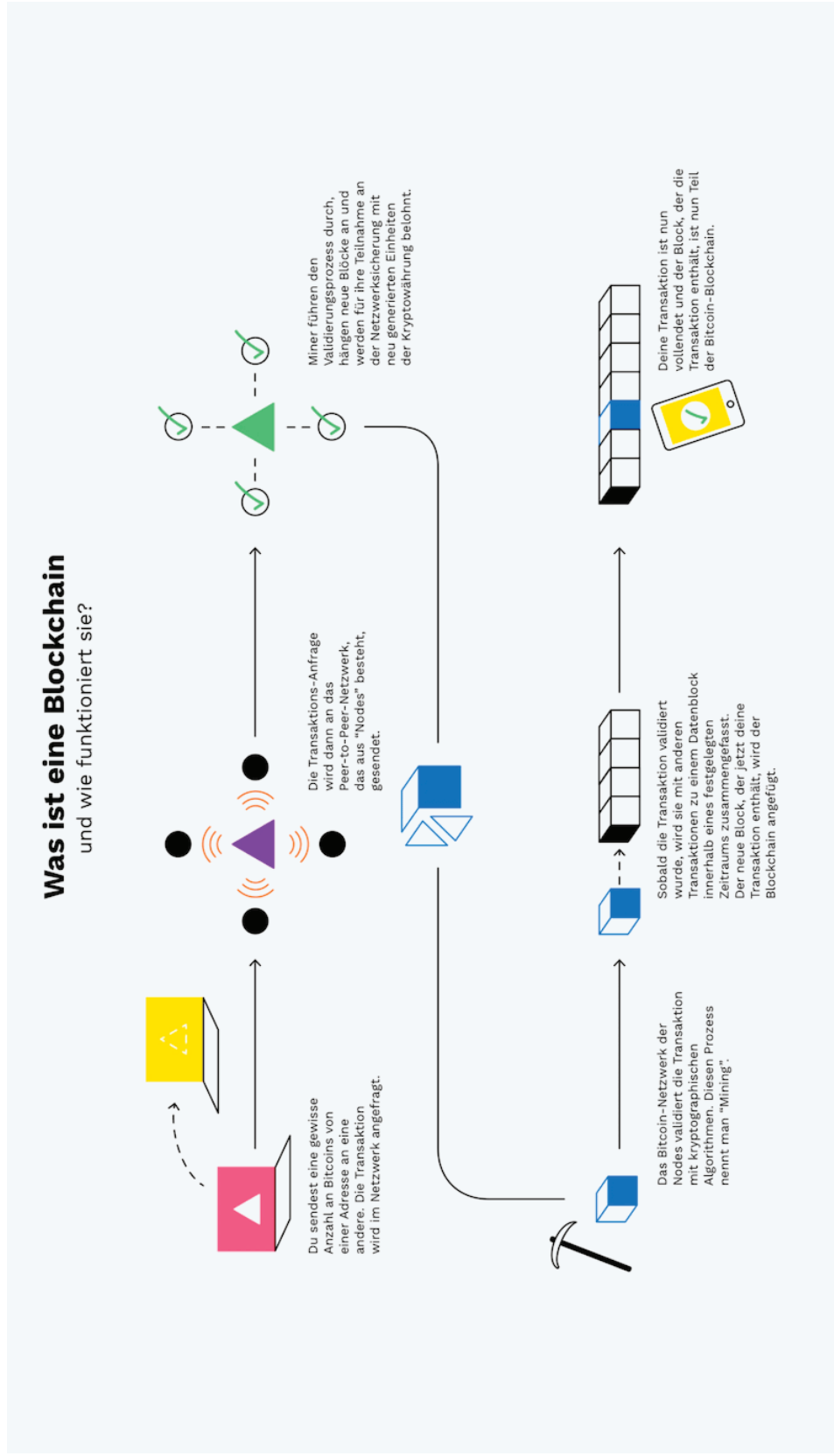
Quelle: Brown/LendEDU 2020. abgerufen am 17.07.2021

App. 15 Kritik an Erhebungsmethoden

<p>Direkte Methoden</p> <p>Befragungen</p>	<p>(1) Häufig werden nur Haushalte befragt.</p> <p>(2) Antwortverweigerungen oder ‚gesellschaftlich gewünschte‘ Antworten sind häufig.</p>
<p>Indirekte Methoden</p> <p>Schätzungen der stat. Ämter mit Ansätzen, die auf der VGR basieren (häufig Diskrepanz-Ansatz)</p>	<p>(1) Kombination von Meso-Schätzungen und fragwürdigen Annahmen.</p> <p>(2) Ergebnisse werden oft nicht veröffentlicht.</p> <p>(3) Dokumentationen zu den Schätzverfahren werden nicht veröffentlicht.</p> <p>(4) Nur partielle Erfassung der Schattenwirtschaft.</p>
<p>Monetäre Ansätze und Physikalische Inputmethode</p>	<p>(1) Schätzungen sind sehr hoch und instabil.</p> <p>(2) Große Abhängigkeit von den Annahmen.</p> <p>(3) Häufig ist eine Disaggregation der Schattenwirtschaft in einzelne Komponenten nicht möglich.</p>
<p>Kausale Methoden</p>	<p>(1) Nur relative Schätzkoeffizienten (keine absoluten Werte) lassen sich ermitteln.</p> <p>(2) Häufig sehr sensitiv bei Datenänderungen.</p> <p>(3) Instabile Schätzergebnisse je nach Datenlage.</p>

Quelle: Schneider/Enste 2000b in Enste/Schneider 2007:285

App. 16 Was ist eine Blockchain?



Quelle: Bitpanda zitiert in Schiller 2019, abgerufen am 15.11.2021

App. 17 neun Säulen des Cybercrime-as-a-Service (CCaaS)



Quelle: BKA 2021b:46


App. 18 Aktuelle Kryptomärkte auf DarknetStats

DarknetStats

All the darkweb news you need and more


LATEST
POPULAR
HOT
TRENDING

HOME
NEWS & ARTICLES
MARKETS LIST
TUTORIALS
MARKETS CHART
CONTACT US
🔍




CANNABIS

SCOTTISH PEDOPHILE WHO DOWNLOADED SICK CHILD SEX ABUSE IMAGES FROM DARK WEB JAILED




CANNABIS

THE DARK WEB'S BIGGEST CANNABIS ONLY MARKET IS RETIRING




CANNABIS

WASHINGTON MAN ACCUSED OF USING DARK WEB TO HIRE KIDNAPPER DENIED BAIL




CANNABIS

BRITISH MAN GETS 6 MONTHS PRISON FOR DOWNLOADING CHILD PORN FROM DARKNET



CANNABIS

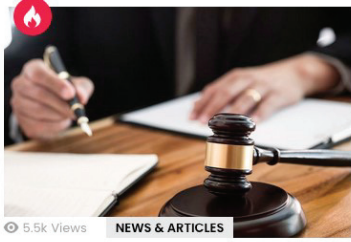
IRISH MAN ACCUSED OF IMPORTING CANNABIS FROM CALIFORNIA USING DARK WEB



CANNABIS

SILK 2.0 ADMIN 'CTHULHU' ORDERED TO PAY \$493,550 IN BITCOIN BY LIVERPOOL COURT

LATEST STORIES




5.5k Views

NEWS & ARTICLES

Wall St Market Vendor 'RaptureReloaded' Sent to 96 Months Behind Bars

Earlier today, at the federal courthouse in Brooklyn, Joanna De [...] [MORE](#)

by Kofi Anash 30 days ago



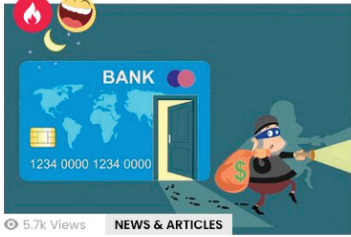
5.9k Views

NEWS & ARTICLES

Tripwithscience - How a U.S Army Veteran Made Millions Off Dark Web Selling Psychedelics

A 25-year military veteran quietly became one of the more [...] [MORE](#)

by G Raymond about a month ago




5.7k Views

NEWS & ARTICLES

Former Bank Employee Pleads Guilty to Wire Fraud Using Identities Purchased from Darknet

Scheme Sought Over \$250,000 in Fraudulent Transactions WASHINGTON - Danielle [...] [MORE](#)

by N.Walden



5.3k Views

NEWS & ARTICLES

British Man Arrested for Importing Guns Via Dark Web

A GWENT criminal used the dark web to import a [...] [MORE](#)

by N.Walden

MARKETS LIST

Top Markets

Dream Market

Markets

World Market

Cannazon Market

Asean (Asap) Market

White House Market

Majestic Garden

Alphabay Market

Liberty Market

Bohemia Market

MGM Grand Market

Monopoly Market

Dark Fox Market

Torrez Market

Tor2door Market

Cartel Market

Scam Markets

Dark0de Reborn

Quelle: DarknetStats. <https://www.darknetstats.com/>. abgerufen am 05.12.2021

App. 19 Screenshot „The hidden wiki“ Net



HOME BLOG POST

The-Hidden-Wiki | Dark Web Links | Dark Web Sites in 2021

To access dark web links, install [TOR Browser](#)

Sites To Dark Web Links

Introduction Points

- [OnionLinks](#) - .Onion link directory.
- [The Hidden Wiki](#) - New Hidden Wiki
- [Another Hidden Wiki](#) - Another hidden wiki like link collection.
- [The Dark Web Pug](#) - Pug's Ultimate Dark Web Guide
- [Hidden Wiki](#) - The Original Hidden Wiki

Financial Services

Currencies, banks, money markets, clearing houses, exchangers:

- [AccMarket](#) - Premium Paypal, Ebay and bank accounts.
- [Cardshop](#) - USA CVV KNOWN BALANCE & Worldwide CC & CVV.
- [Dark Mixer](#) - Anonymous bitcoin mixer
- [Mixabit](#) - Bitcoin mixer
- [VirginBitcoins](#) - Buy freshly mined clean bitcoins
- [ccPal](#) - PayPals, Ebays, CCs and more
- [Webuybitcoins](#) - Sell your Bitcoins for Cash, Paypal, WU etc
- [HQER](#) - High Quality Euro bill counterfeits
- [Counterfeit USD](#) - High Quality USD counterfeits
- [EasyCoin](#) - Bitcoin Wallet and Mixer
- [Onionwallet](#) - Anonymous and secure bitcoin wallet and mixer

Commercial Services

- [DarkWebHackers](#) - Dark Web Hackers for hire.
- [Mobile Store](#) - Best unlocked cell phones vendor
- [Kamagra 4 Bitcoin](#) - Like Viagra but cheaper
- [OnionIdentityServices](#) - Fake passports and ID cards for bitcoin
- [UkGunsAndAmmo](#) - Uk Guns and Ammo Store
- [USfakeIDs](#) - US fake ID store
- [EuroGuns](#) - Your #1 european arms dealer.
- [Apples4Bitcoin](#) - Iphones, Ipad and more for bitcoin
- [UKpassports](#) - real UK passports
- [USAcitizenship](#) - become a citizen of the USA
- [Rent-A-Hacker](#) - Hire a hacker for Bitcoin

Recent Posts

- 📄 [Dark Web Links and Best Darknet Market News in 2021](#)
- 📄 [Hidden Wiki Links and Bitpharma European Onion Drug Store](#)
- 📄 [Hidden Wiki Links & Dark web Users & Hidden Wiki Users 2021](#)
- 📄 [Hidden Wiki & Brainmagic Dark Web Psychedelic Era 2021](#)
- 📄 [Dark web links and dark web drug links including cannabis 2021](#)
- 📄 [Dark Web Links To The Dutch Connection For The UK](#)
- 📄 [Dark Web Links CANNABIS and get more dark web links 2021](#)
- 📄 [Dark Web Links - TOM AND JERRY - COCAINE, HEROIN FROM NL](#)
- 📄 [Important things about the hidden wiki must know in 2021](#)
- 📄 [Dark web sites take downs in 2020, Is it true? Learn more](#)
- 📄 [Get dark web sites links and dark web links in 2020](#)
- 📄 [Dark web sites in 2020 | How online black markets work](#)
- 📄 [Dark Web Sites_Silk Road -Tale of first darknet market 2020](#)
- 📄 [Get dark web links and visit the dark web sites in 2020](#)
- 📄 [Dark web links & Dark web sites | Know all about it in 2020](#)
- 📄 [Hidden Wiki Questions And Answers](#)
- 📄 [Tor- All You Need to Know About It!](#)
- 📄 [A Guide To The Hidden Wiki](#)
- 📄 [Information About The Hidden Wiki](#)

Quelle: „The hidden wiki“. <https://the-hidden-wiki.net/>. abgerufen am 05.12.2021

The Hidden Wiki

Welcome to The Hidden Wiki – The Front Page of the Dark Web.

Add The Hidden Wiki to your bookmarks and spread it!!

To access darkweb sites on The Hidden Wiki, install [TOR Browser](#)

Volunteer

- [Bookmark this page](#)
- Defend your right to privacy: donate to the [EFF](#) and [The TOR Project](#)

Hidden Wiki Editor’s picks

Some of the most interesting sites on The Hidden Wiki and the dark web:

1. [Mixabit](#) – Bitcoin mixer
2. [OnionLinks](#) – .Onion Link directory.
3. [Bitpharma](#) – Biggest european .onion drug store
4. [DarkWebHackers](#) – Dark Web Hackers for hire.
5. [Cardshop](#) – USA CVV KNOWN BALANCE & Worldwide CC & CVV .

Introduction Points

Some sites with good .onion lists

- [OnionLinks](#) – .Onion Link directory.
- [The Hidden Wiki](#) – New Hidden Wiki 2019
- [The Original Hidden Wiki](#) – The oldest hidden wiki
- [Another Hidden Wiki](#) Another hidden wiki like link collection.
- [The Dark Web Pug](#) Pug’s Ultimate Dark Web Guide .

Financial Services

Currencies, banks, money markets, clearing houses, exchangers:

- [AccMarket](#) – Premium Paypal, Ebay and bank accounts.
- [Cardshop](#) – USA CVV KNOWN BALANCE & Worldwide CC & CVV .
- [Dark Mixer](#) – Anonymous bitcoin mixer
- [Mixabit](#) – Bitcoin mixer
- [VirginBitcoins](#) – Buy freshly mined clean bitcoins .
- [ccPal](#) – PayPals, Ebays, CCs and more
- [Webbitcoins](#) – Sell your Bitcoins for Cash, Paypal, Wire

Recent Posts

- [New Long V3 Onion Services](#)
- [Version 3 Hidden Service Links On The Hidden Wiki](#)
- [Privacy When Using Sites On The Hidden Wiki](#)
- [Coronavirus And The Dark Web](#)
- [The Uncensored Hidden Wiki](#)
- [How To Use Bitcoin Anonymously On Hidden Wiki Sites](#)

Information

- [Privacy Policy](#)
- [Terms And Conditions](#)
- [Contact](#)

App. 21 Screenshot „UK Guns and Ammo Store“

UK Guns and Ammo Store

Products Info Login Registration

Guns

Only 3 x P99 and 2 x Glock 19 left, we will get new stock of similar weapons once those are sold.

Product	Price	Quantity
Glock 19 - 9mm - new and unused	500 GBP = 0.01335 ₤	1 X Buy now
Walther P99 - 9mm - new and unused	650 GBP = 0.01736 ₤	1 X Buy now

Ammo

Product	Price	Quantity
100 x 9mm Bullets for Glock 19	50 GBP = 0.00134 ₤	1 X Buy now
100 x 9mm Bullets for Walther P99	50 GBP = 0.00134 ₤	1 X Buy now

Quelle: <http://onili244aue7jkvzn2bgaszcb7nznkpyihdhh7evflp3iskfq7vhlzid.onion/>. abgerufen am 05.12.2021

App. 22 Screenshot „EuroGuns“

EuroGuns Products FAQs Register Login

Walther PPK, Kal.7,65

New and unused and unregistered!
Ammo can only be purchased if you also buy the gun.

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 0.01361 ₤	1 X Buy now
Ammo, 50 Rounds	40 EUR = 0.00091 ₤	1 X Buy now

Desert Eagle IMI, Kal.44

New and unused and unregistered!
Ammo can only be purchased if you also buy the gun.

Product	Price	Quantity
Desert Eagle IMI, Kal.44	1250 EUR = 0.02836 ₤	1 X Buy now
Ammo, 50 Rounds	45 EUR = 0.00102 ₤	1 X Buy now

Quelle: <http://hyjgsnkanan2wsrksd53na4xigtzhlz57estwqtpzpha53rxz53pqad.onion/>. abgerufen am 05.12.2021


App. 23 Screenshot „USA Citizenship“

USA

[Products](#) [FAQs](#) [Register](#) [Login](#)

Citizenship

Become a citizen of the USA, real USA passport



We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA!
It will even work if you are not in the USA yet

How we do it? Trade secret! But we can assure you that you won't have any problems with our papers.
We are shipping documents from the USA, international shipping is no problem.
You can use your own name or a new name!
Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase.

The total price is 4000 USD, 1000 USD paid when you order and the other 3000 when we show you photo and video proof of your passport.
The first 1000 USD are needed upfront to see you are serious about it. Once paid we will discuss details in our shop internal message system.

Product	Price	Quantity
Your USA citizenship first payment 25% 1000/4000	1500 USD = 0.03021 ₿	<input type="text" value="1"/> X Buy now
US bank account with online banking and card. Great for cashing out bitcoin. Accounts will last at least 8 years.	1000 USD = 0.02014 ₿	<input type="text" value="1"/> X Buy now

Quelle: <http://pz5uprzhnzcotviraa2fogkua5nlmnu75pbnnqu4fnwgfllldwxog7ad.onion/>. abgerufen am 05.12.2021

App. 24 Screenshot „UK Passports“

UK Passports

[Products](#) [Login](#) [Register](#) [FAQs](#)

Your UK Passport - Name of your choice!



We are selling original UK Passports made with your info/picture.
Your info will get entered into the official passport database.
So it's possible to travel with our passports.
How we do it? Trade secret!
Information on how to send us your information and pictures will be given after purchase!

You can even enter the UK/EU with our passports, we will add a stamp for the country you are in before we send you your passport to any country!
Ideal for people who want to work in the EU/UK.

Product	Price	Quantity
Your original UK passport with your info/pictures This is 50% of the final price, you pay the other 50% once we show you pictures of your new passport	850 GBP = 0.02270 ₿	<input type="text" value="1"/> X Buy now
NEW: UK bank account with online banking and card. Great for cashing out bitcoin. Accounts are created in a secure way to make sure they don't get banned.	700 GBP = 0.01870 ₿	<input type="text" value="1"/> X Buy now

Quelle: <http://wosc4noitfscyywccasl3c4yu31ftpl2adxvprp6sbg4fud6mkrwqqd.onion/>. abgerufen am 05.12.2021

App. 25 Screenshot „Rent a Hacker“

Rent-A-Hacker

[Products](#)
[FAQs](#)
[Register](#)
[Login](#)

Rent-A-Hacker

Experienced hacker offering his services!
 (Illegal) Hacking and social engineering is my business since i was 16 years old. I never had a real job, so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
 I have worked for other people before, now i am also offering my services for everyone with enough cash here.

Prices:
 I am not doing this to make a few bucks here and there, i am not from some crappy eastern europe country and happy to scam people for 50 EUR.
 I am a professional computer expert who could earn 50-100 EUR an hour with a legal job.
 So stop reading if you don't have a serious problem worth spending some cash at.
 Prices depend a lot on the problem you want me to solve, but minimum amount for smaller jobs is 250 EUR.
 You can pay me anonymously using Bitcoin.

Technical skills:

- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i don't know it, i'll learn it very fast
- Anonymity: no one will ever find out who i am or anything about my clients.

Social Engineering skills:

- Very good written and spoken (phone calls) english, spanish and german.
- If i can't hack something technically i'll make phone calls or write emails to the target to get the needed information, i have had people make things you wouldn't believe really often.
- A lot of experience with security practices inside big corporations.

What i'll do:
 I will do anything for money, i'm not a pussy. If you want me to destroy some business or a persons life, i'll do it!
 Some examples:

- Simply hacking something technically
- Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
- Economic espionage
- Getting private information from someone
- Ruining your opponents, business or private persons you don't like, i can ruin them financially and or get them arrested, whatever you like.

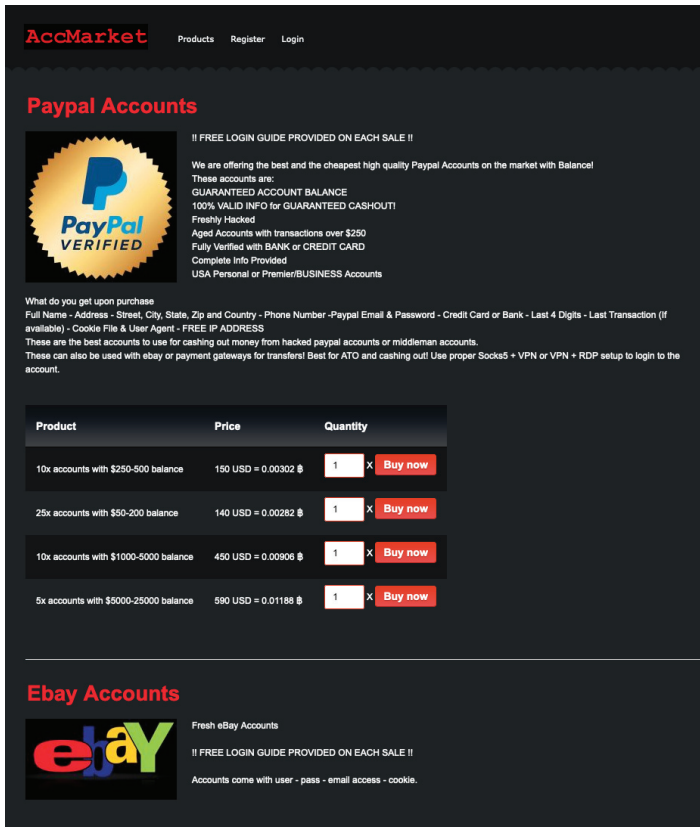
If you want someone to get known as a child porn user, no problem.

**The following prices are estimates, if i think a specific job takes more time and money i will either refund you or you will send the remaining once we talked.
 If you are unsure about which category to choose, choose the lower priced one in question.
 You will only pay for successful jobs, if i can not do anything for you i will refund you. But keep in mind depending on your target specific things might take longer and require an addition payment, but only after i can show some success.**

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.00567 ₿	<div style="border: 1px solid #f1c40f; padding: 2px; display: inline-block;">1</div> X Buy now

Quelle: <http://jn6weomv6klvnwdwcu55miabpwklsmyaf5qrkt4miiif4shrqmvdhqd.onion/>. abgerufen am 05.12.2021

App. 26 Screenshot „Acc Market“



AccMarket Products Register Login

Paypal Accounts

!! FREE LOGIN GUIDE PROVIDED ON EACH SALE !!

We are offering the best and the cheapest high quality Paypal Accounts on the market with Balance
These accounts are:
GUARANTEED ACCOUNT BALANCE
100% VALID INFO for GUARANTEED CASHOUT!
 Freshly Hacked
 Aged Accounts with transactions over \$250
 Fully Verified with BANK or CREDIT CARD
 Complete Info Provided
 USA Personal or Premier/BUSINESS Accounts

What do you get upon purchase
 Full Name - Address - Street, City, State, Zip and Country - Phone Number - Paypal Email & Password - Credit Card or Bank - Last 4 Digits - Last Transaction (if available) - Cookie File & User Agent - FREE IP ADDRESS
 These are the best accounts to use for cashing out money from hacked paypal accounts or middleman accounts.
 These can also be used with ebay or payment gateways for transfers! Best for ATO and cashing out! Use proper Socks5 + VPN or VPN + RDP setup to login to the account.

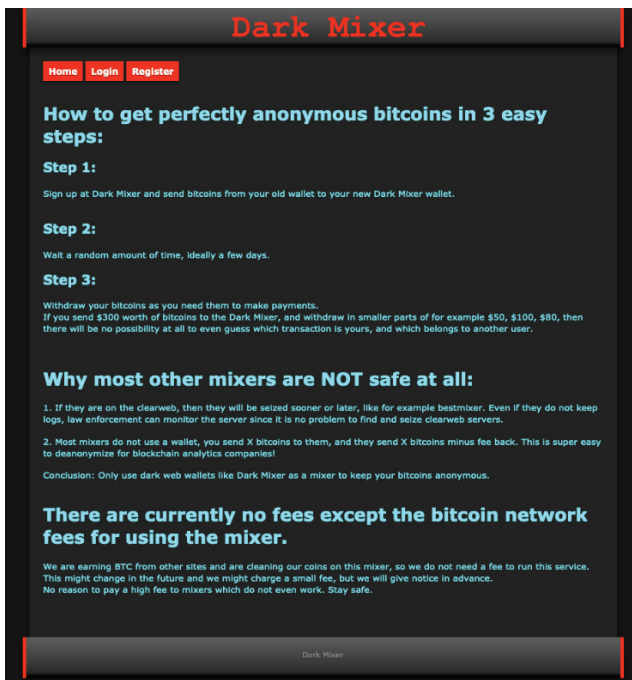
Product	Price	Quantity
10x accounts with \$250-500 balance	150 USD = 0.00302 €	1 X Buy now
25x accounts with \$50-200 balance	140 USD = 0.00282 €	1 X Buy now
10x accounts with \$1000-5000 balance	480 USD = 0.00908 €	1 X Buy now
5x accounts with \$5000-25000 balance	590 USD = 0.01188 €	1 X Buy now

Ebay Accounts

Fresh eBay Accounts
 !! FREE LOGIN GUIDE PROVIDED ON EACH SALE !!
 Accounts come with user - pass - email access - cookie.

Quelle: <http://z7s2w5vruxbp2wzts3snxs24yggbtcdj5kp2f6z5gimouyh3wiaf7id.onion/>. abgerufen am 05.12.2021

App. 27 Screenshot „Dark Mixer“



Dark Mixer

Home Login Register

How to get perfectly anonymous bitcoins in 3 easy steps:

Step 1:
Sign up at Dark Mixer and send bitcoins from your old wallet to your new Dark Mixer wallet.

Step 2:
Wait a random amount of time, ideally a few days.

Step 3:
Withdraw your bitcoins as you need them to make payments.
If you send \$300 worth of bitcoins to the Dark Mixer, and withdraw in smaller parts of for example \$50, \$100, \$80, then there will be no possibility at all to even guess which transaction is yours, and which belongs to another user.

Why most other mixers are NOT safe at all:

1. If they are on the clearweb, then they will be seized sooner or later, like for example bestmixer. Even if they do not keep logs, law enforcement can monitor the server since it is no problem to find and seize clearweb servers.
2. Most mixers do not use a wallet, you send X bitcoins to them, and they send X bitcoins minus fee back. This is super easy to deanonymize for blockchain analytics companies!

Conclusion: Only use dark web wallets like Dark Mixer as a mixer to keep your bitcoins anonymous.

There are currently no fees except the bitcoin network fees for using the mixer.

We are earning BTC from other sites and are cleaning our coins on this mixer, so we do not need a fee to run this service. This might change in the future and we might charge a small fee, but we will give notice in advance.
No reason to pay a high fee to mixers which do not even work. Stay safe.

Dark Mixer

Quelle: <http://cr32aykujaxqkfyrjvt7lxovnadpgmgthb3y4g6jmx6oomr572kbuqd.onion/>. abgerufen am 05.12.2021

App. 28 Screenshot „Mixabit Bitcoin Mixer“

Mixabit Bitcoin Mixer

Info Login Register



Mixabit Features:

- High volume mixer and always a perfect mix with other users bitcoins, there will never be taint to your old bitcoins.
- Safe storage: we keep most of the bitcoins in secure encrypted offline storage.
- Protect your funds with a transaction PIN.
- Anonymous registration: We do not need any private data.
- Very simple user interface, no complicated options and settings.
- For small amounts up to 0.01 BTC there are NO FEES except the bitcoin network fee!
- For larger amounts the fee is only 0.5%.

Mixing best practices:

- Always wait some time before you withdraw and do not withdraw the same amount you deposited at once.
- Ideally just use Mixabit as your wallet, that way there will be no timing or amount correlation between your deposits and your withdrawals.

Quelle: <http://74ck36pbaxz7ra6n7v5pbpm5n2tsdaiy4f6p775qvjmowxged65n3cid.onion/>. abgerufen am 05.12.2021

App. 29 Screenshot „EuCanna“



Products Info Login Register

Buds | Oil | Ointment | Suppositories | Creams | Bath Melts

Soaps | CannaCaps | Edibles | Special Offers

Medical Grade Cannabis Buds



We stock high quality hydroponic and organic cannabis. We are experienced professional cannabis growers who place emphasis on the medicinal value rather than the quantity we produce. This is why you will frequently see strains listed with a 50/50 indica-sativa ratio, as these strains are best for making the Rick Simpson Oil.

Product	Price	Quantity
3.5g Organic White Russian	42 EUR = 0.00096 ₿	1 X Buy now
7g Organic White Russian	70 EUR = 0.00159 ₿	1 X Buy now
14g Organic White Russian	120 EUR = 0.00273 ₿	1 X Buy now
50g Organic White Russian	295 EUR = 0.00672 ₿	1 X Buy now
3.5g Organic Chronic	42 EUR = 0.00096 ₿	1 X Buy now
7g Organic Chronic	70 EUR = 0.00159 ₿	1 X Buy now
14g Organic Chronic	120 EUR = 0.00273 ₿	1 X Buy now
50g Organic Chronic	295 EUR = 0.00672 ₿	1 X Buy now


Quelle: <http://wges3aohuplu6he5tv4pn7sg2qaummlokimim6oaaqo2l7lhx4ufyyd.onion/>. abgerufen am 05.12.2021

App. 30 Screenshot „420prime“

420prime

Products
Login
Registration

420prime - Shipping from United Kingdom



We specialise in legally grown strains of dispensary quality. All our products are imported directly to guarantee you the highest quality from some of the best growers in the world... We reflect this in our prices and believe that ensuring quality of product is far more important than cheap prices. We are professionals, not street dealers, we do our utmost to deliver on our promises on time, every time.

Basically, we love cannabis, and we want everyone to be able to enjoy the finest quality regardless of outdated laws trying to prevent it.

All our packages are shipped safely and discretely using the perfect amount of stealth.

We offer Signed for next day guaranteed delivery by 1pm, or royal mail 1st class (1-3 days). All orders placed before 2pm will be packaged and shipped same day.
Shipping fee is 5 GBP, FREE shipping for orders over 300 GBP.

Product	Price	Quantity
BC Cheese 7g	80 GBP = 0.00214 ₤	<input type="text" value="1"/> X Buy now
BC Cheese 15g	140 GBP = 0.00374 ₤	<input type="text" value="1"/> X Buy now
BC Cheese 30g	220 GBP = 0.00588 ₤	<input type="text" value="1"/> X Buy now
Blue Zkittlez 7g	80 GBP = 0.00214 ₤	<input type="text" value="1"/> X Buy now
Blue Zkittlez 15g	140 GBP = 0.00374 ₤	<input type="text" value="1"/> X Buy now
Blue Zkittlez 30g	220 GBP = 0.00588 ₤	<input type="text" value="1"/> X Buy now
Ghost OG 7g	80 GBP = 0.00214 ₤	<input type="text" value="1"/> X Buy now
Ghost OG 15g	140 GBP = 0.00374 ₤	<input type="text" value="1"/> X Buy now
Ghost OG 30g	220 GBP = 0.00588 ₤	<input type="text" value="1"/> X Buy now
Pink Kush 7g	80 GBP = 0.00214 ₤	<input type="text" value="1"/> X Buy now

Quelle: <http://rbcxodz4socx3rupvmhan2d7pvik4dpqmf4kexz6acyxbucf36a6ggid.onion/>. abgerufen am 05.12.2021

App. 31 Screenshot „Tom and Jerry Store“


Login
Register
Products

Tom and Jerry Store

We have been active during the Agora, Evolution, Silkroad 3 era, then continued through Alphabay and Nucleus, and even the late Dream Market and also Wallstreet, with the same successful concept:
High quality drugs combined with an extremely discreet and fast shipping.

Extremely stealth shipping from the netherlands!

High Quality Cocaine [90%]



We offer High Quality Cocaine 90%+ with FREE SHIPPING !
All orders that come in before 14:00 Dutch local time are shipped the very same day !
Shipping internationally!

Product	Price	Quantity
2g High Quality Cocaine	90 EUR = 0.00205 ₤	<input type="text" value="1"/> X Buy now
5g High Quality Cocaine	200 EUR = 0.00455 ₤	<input type="text" value="1"/> X Buy now
10g High Quality Cocaine	350 EUR = 0.00797 ₤	<input type="text" value="1"/> X Buy now
25g High Quality Cocaine	750 EUR = 0.01708 ₤	<input type="text" value="1"/> X Buy now
50g High Quality Cocaine	1400 EUR = 0.03188 ₤	<input type="text" value="1"/> X Buy now
5g High Quality Crack Cocaine	220 EUR = 0.00501 ₤	<input type="text" value="1"/> X Buy now
10g High Quality Crack Cocaine	420 EUR = 0.00956 ₤	<input type="text" value="1"/> X Buy now

Pure Afghan Heroin #3 [100%]

Hincit: dark real pure Heroin also good for IV use (with citric acid)


Quelle: <http://c5xoy22aad2rqgw3jh2m2irmu563evukqddu5zjandunaimzaye5id.onion/>. abgerufen am 05.12.2021

App. 32 Screenshot „DCdutchconnectionUK“

DCdutchconnectionUK

Products
Login
Registration

DCdutchconnectionUK - Shipping from United Kingdom



DCdutchconnectionUK is BACK after a long hiatus. Lots has changed since we have been gone but our strong stance on providing honest quality products with out adulterants supported by lab results and superb customer feedback has not. We have seen our fair share of success and have an abundance of experience.

Therefore we can assure you that your order will be shipped same day when placed before 3.00pm, ready for next day delivery Mon-Fri. Saturday delivery before 10am (not guaranteed). DCdutchConnectionUK only sells the best there is. Be do NOT sell low purity, cut or low grade products!

Any off our long term customers will know this, We want to let you know that when ordering with DCUK you are getting the very best.

Sometimes this means that this is reflected in the price. We are not the cheapest but we like to think we have the BEST price to quality ratio.
 FREE shipping for all orders 150 GBP+.

Product	Price	Quantity
FISHSCALE COCAINE 1.5g	80 GBP = 0.00214 ₿	<input type="text" value="1"/> X Buy now
FISHSCALE COCAINE 5g	230 GBP = 0.00614 ₿	<input type="text" value="1"/> X Buy now
FISHSCALE COCAINE 10g	400 GBP = 0.01068 ₿	<input type="text" value="1"/> X Buy now
PURE PLATINUM MDMA 92% 15g	80 GBP = 0.00214 ₿	<input type="text" value="1"/> X Buy now
PURE PLATINUM MDMA 92% 30g	150 GBP = 0.00401 ₿	<input type="text" value="1"/> X Buy now
PURE PLATINUM MDMA 92% 50g	200 GBP = 0.00534 ₿	<input type="text" value="1"/> X Buy now
AMNESIA HAZE - THC 21% - NEW BEST BATCH! 15g	110 GBP = 0.00294 ₿	<input type="text" value="1"/> X Buy now
AMNESIA HAZE - THC 21% - NEW BEST BATCH! 30g	190 GBP = 0.00507 ₿	<input type="text" value="1"/> X Buy now
AMNESIA HAZE - THC 21% - NEW BEST BATCH! 55g	310 GBP = 0.00828 ₿	<input type="text" value="1"/> X Buy now
ROCK ISOMER 5-KETAMINE 90% 7g	100 GBP = 0.00267 ₿	<input type="text" value="1"/> X Buy now

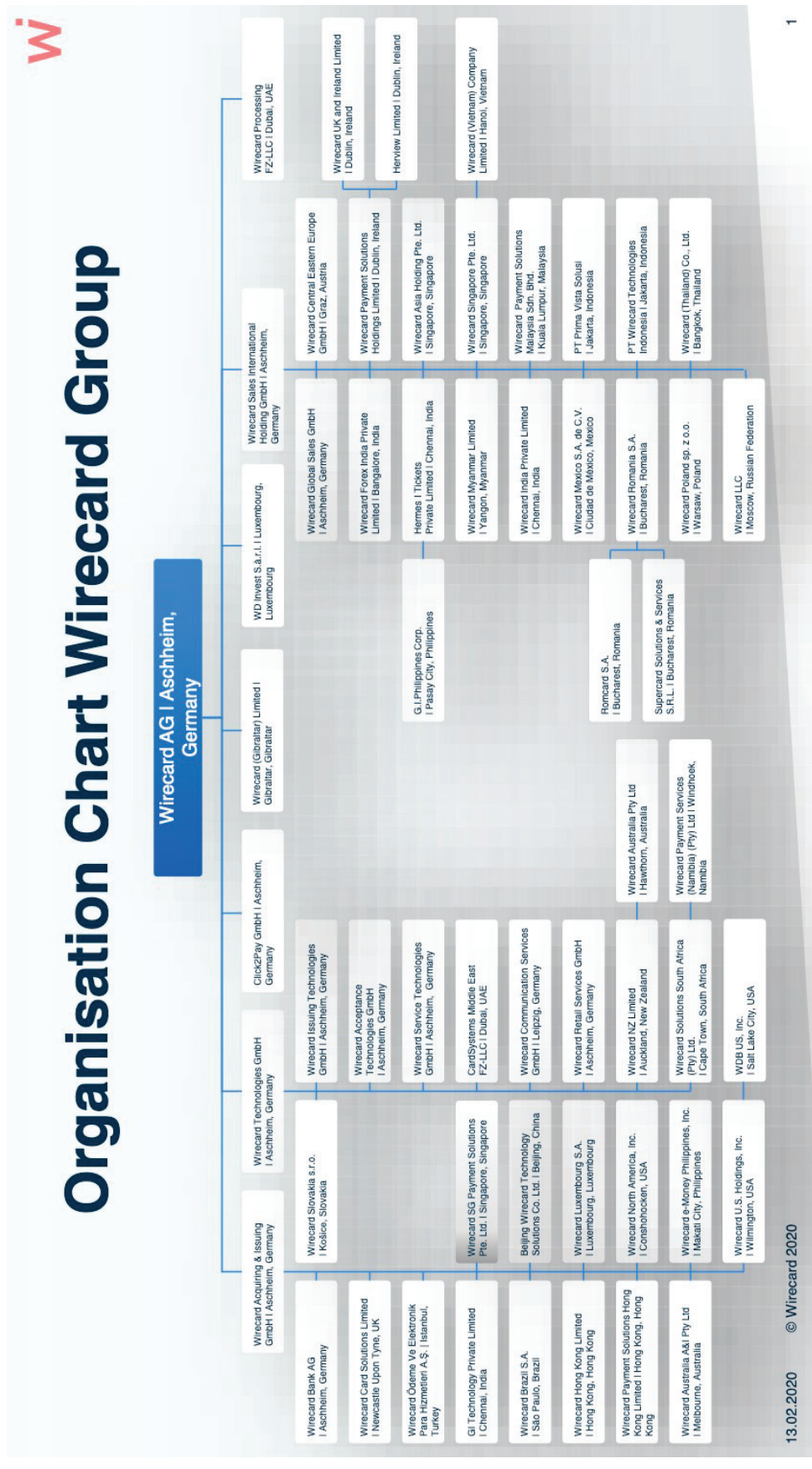
Quelle: <http://wms5y25kttgih54rt2sifsbwsjqrx3vtc42tsu2obksqkj7y666fgid.onion/>. abgerufen am 05.12.2021

App. 33 Notable Cryptocurrency Thefts 2011-2021

No.	Date	Impetus	Original Amount in Coin Stolen	BTC equiv.	USD equiv.	Type
1	June 2011	Mt.Gox Private Key Hack	2,643 BTC	2,643	30,000	Security Breach
2	March 2014	Mt. Gox Transaction Malleability	850,000 BTC	850,000	460,000,000	Security Breach
3	July 2014	Mintpal Hack	8,000,000 Vericoïn	3,225	2,000,000	Security Breach
4	January 2015	Bitstamp Malware Attack	19,000 BTC	19,000	5,100,000	Human Error
5	August 2015	BTER Inside Job	7,170 BTC	7,170	1,750,000	Agency Problem
6	May 2016	Gatecoin Hot Wallet Breach	250 BTC and 185,000 ETH	4,463	2,000,000	Security Breach
7	August 2016	Bitfinex-BitGo Theft	119,756 BTC	119,756	66,000,000	Security Breach
8	April 2017	Yapizon Hot Wallet Breach	3,816 BTC	3,816	5,300,000	Security Breach
9	December 2017	NiceHash Payment Compromise	4,736 BTC	4,736	62,000,000	Security Breach
10	January 2018	Coincheck Virus Hack	523,000,000 NEM	47,711	533,000,000	Human Error
11	February 2018	Bitgrail Hack/Exit Scam	17,000,000 NANO	19,044	170,000,000	Security Breach
12	April 2018	CoinSecure Inside Job	438 BTC	438	3,300,000	Agency Problem
13	June 2018	Bithumb and Coinrail Theft	71,000,000 USD of XRP and ETH	10,394	71,000,000	Security Breach
14	September 2018	Zaif Hot Wallet Breach	5,966 BTC, undisclosed BCH and Monacoin	9,089	60,000,000	Security Breach
15	December 2018	QuadrigaCX Theft	26,350 BTC or 130,000,000 USD	26,350	130,000,000	Agency Problem
16	March 2019	Coinbene Inside Job	100,000,000 USD of HPT, NPSX, MXM, and UDOO	25,202	100,000,000	Agency Problem
17	May 2019	Binance Hack	6,270 BTC	6,270	40,000,000	Human Error
18	June 2019	Bittrue Hack	9,300,000 XRP and 2,500,000 ADA	361	3,900,000	Security Breach
19	November 2019	Upbit Security Breach	342,000 ETH	6,771	51,000,000	Security Breach
20	July 2020	Cashaa Malware Hack	336 BTC	336	3,100,000	Human Error
21	September 2020	KuCoin Security Breach	281,000,000 USD of BTC and ETH	26,137	281,000,000	Security Breach
22	December 2020	EXMO Security Breach	10,500,000 USD of BTC, XRP, ZEC, ETC and ETH	422	10,500,000	Security Breach
23	June 2021	Africrypt Hack	69,000 BTC	69,000	3,600,000,000	Agency Problem
24	August 2021	Liquid Hack	91,350,000 USD of BTC and ETH	1,941	91,350,000	Security Breach
Total Amount Stolen				1,379,691	9,839,980,000	

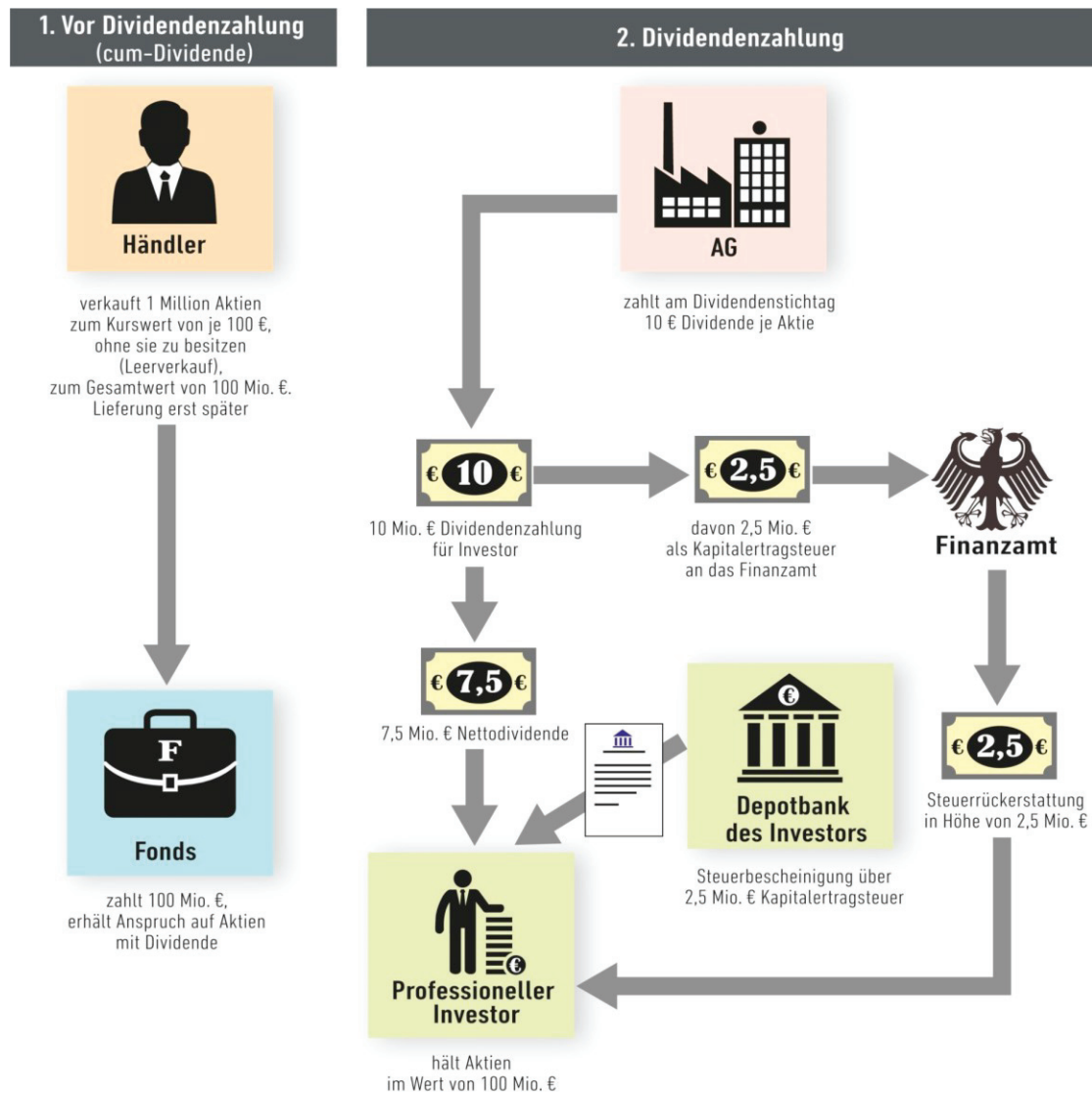
Quelle: Charoenwong/Bernadi 2021:4 f.

App. 34 Organisation Chart Wirecard Group



Quelle: Bundesministerium für Finanzen (BMF), 16.07.2020. https://www.bundesfinanzministerium.de/Content/DE/Downloads/Finanzmarktpolitik/Wirecard-Fragen-und-Antworten/2020716-organisation-chart-wirecard-group.pdf?__blob=publicationFile&v=4, abgerufen am 09.01.2022

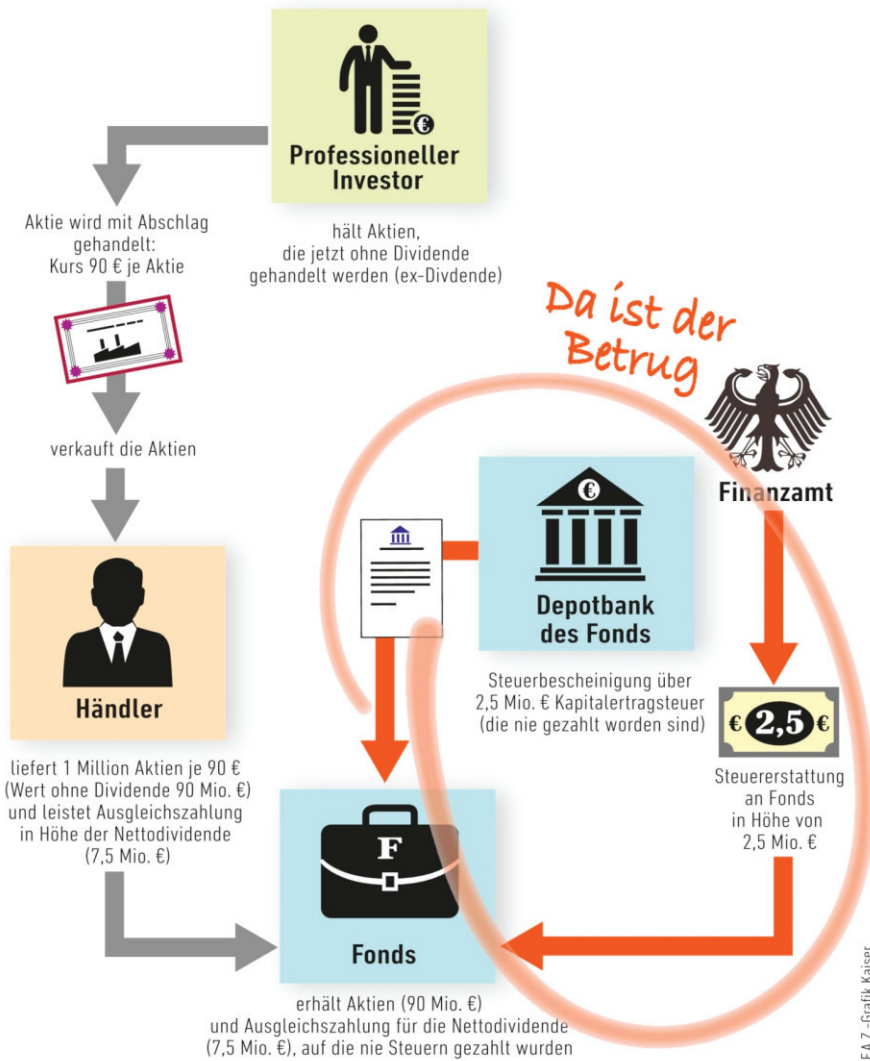
App. 35 Cum-Ex-Geschäfte Ablauf: Vor und am Dividendenstichtag



Quelle: Budras 2016, abgerufen am 10.01.2022

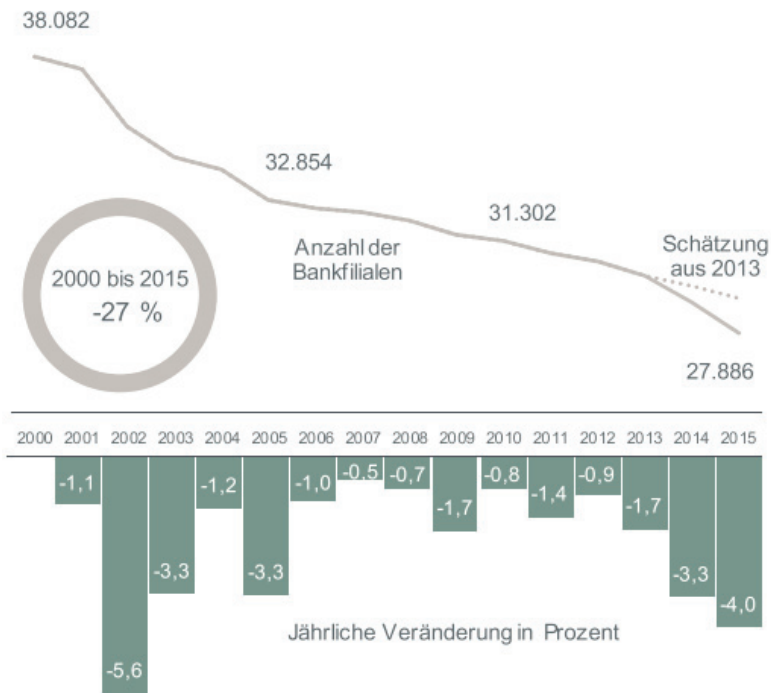
App. 36 Cum-Ex-Geschäfte Ablauf: nach dem Dividendenstichtag

3. Nach Dividendenzahlung (ex-Dividende)



Quelle: Budras 2016, abgerufen am 10.01.2022

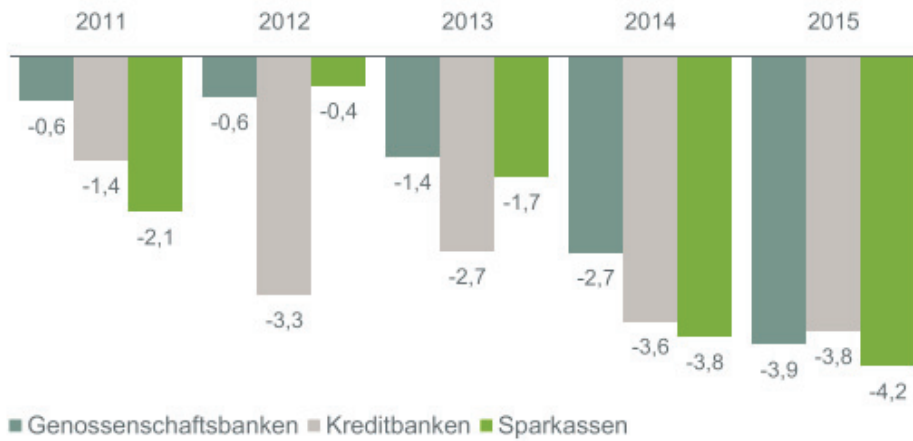
App. 37 Filialrückbau zuletzt mit Tempoverschärfung



Quelle: Schwartz et al. 2017:1

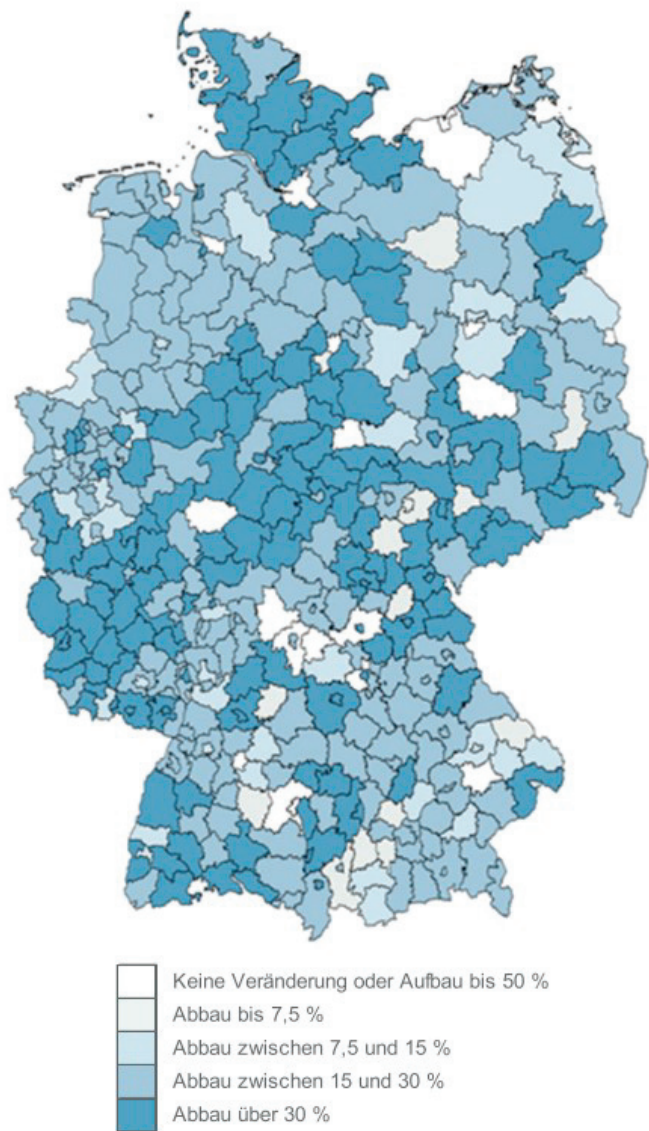
App. 38 Alle Kreditinstitutstypen bauen ab

Jährliche Veränderung der Filialanzahl in Prozent



Quelle: Schwartz et al. 2017:2

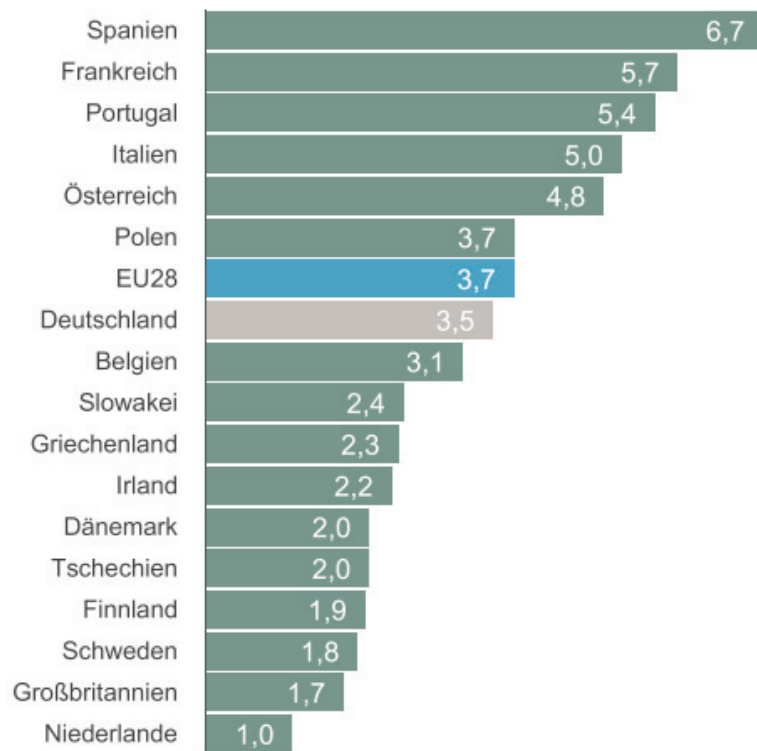
App. 39 Ausdünnung in der Breite



Quelle: Schwartz et al. 2017:2

App. 40 Filialdichte in Deutschland im Mittelfeld

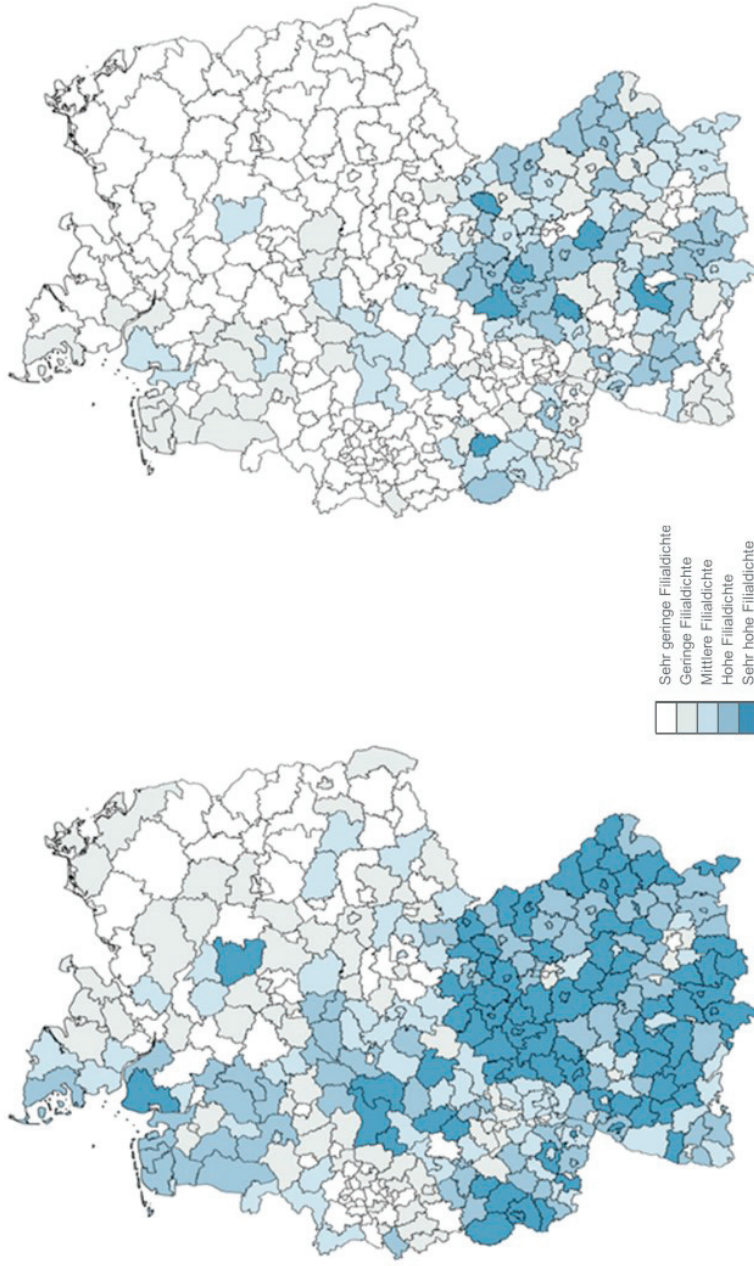
Bankfilialen pro 10.000 Einwohner (Filialdichte); Länderauswahl aus EU28



Quelle: Schwartz et al. 2017:3

App. 41 Filialdichte 2015 (links) und 2035 (rechts)

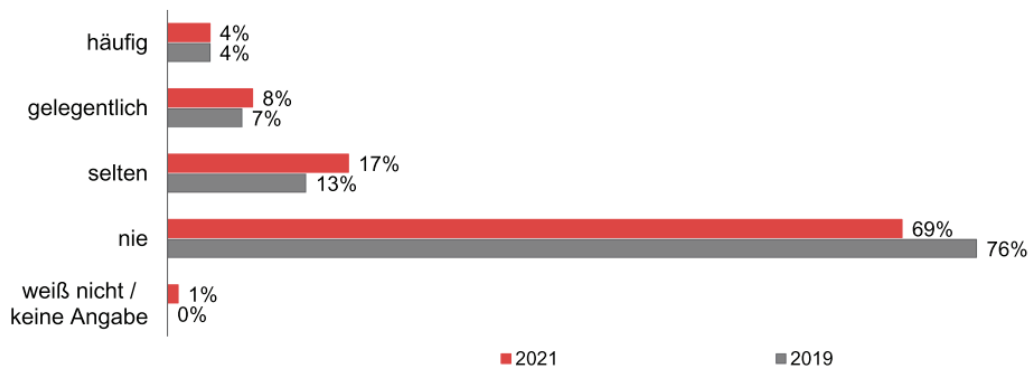
Bankfilialen pro 10.000 Einwohner (Filialdichte) von 402 Kreisen und kreisfreien Städten



Anmerkung: Die Abbildung für das Jahr 2035 unterstellt das „Status quo“-Szenario: Es wird darin unterstellt, dass der Abbau des Filialnetzes mit der gleichen Geschwindigkeit erfolgt, wie er durchschnittlich in den Jahren 2000 bis 2015 beobachtet werden konnte. Eine sehr geringe Filialdichte ist definiert mit Werten unter 2,6, eine geringe Filialdichte liegt bei 2,6 bis 3,2, eine mittlere Filialdichte zwischen 3,2 und 4,0, eine hohe Filialdichte zwischen 4,0 und 5,1 und eine sehr hohe Filialdichte liegt ab einem Wert von 5,1 vor. Zum Vergleich: Deutschland insgesamt erreicht einen Wert von 3,5.

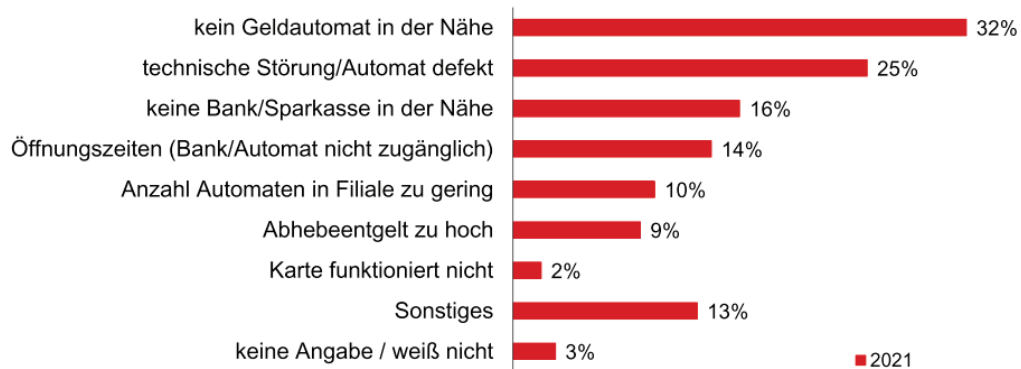
Quelle: Schwartz et al. 2017:4

App. 42 Probleme beim Bargeldbezug (1/2)



Quelle: VZVB 2022:9. abgerufen am 28.01.2022

App. 43 Probleme beim Bargeldbezug (2/2)



Quelle: VZVB 2022:10. abgerufen am 28.01.2022

App. 44 Probleme bei Zahlung mit Bargeld

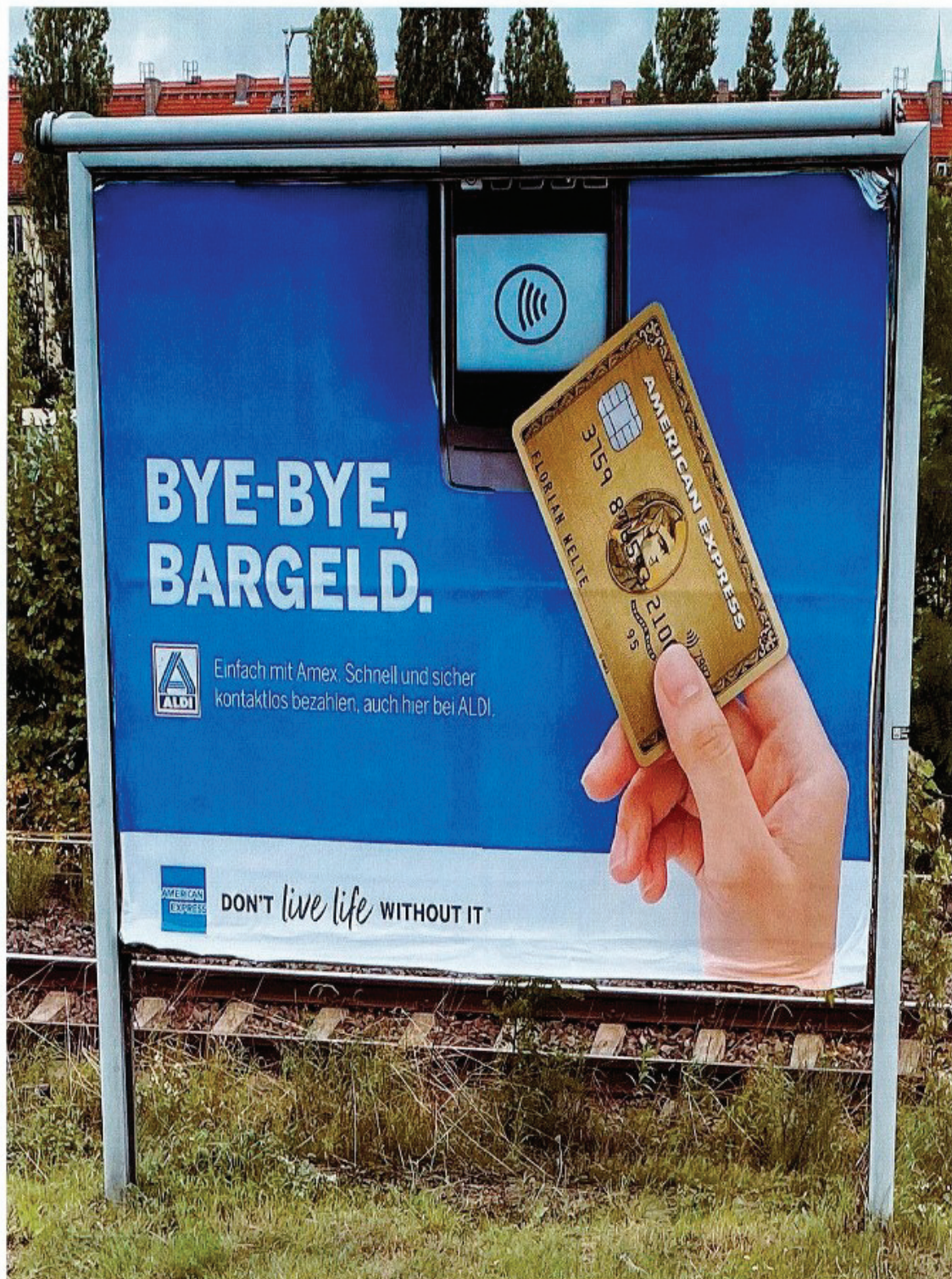


Quelle: VZVB 2022:11. abgerufen am 28.01.2022

App- 45 Building a Known Traveller status

Building a Known Traveller status	★☆☆☆☆	★★☆☆☆	★★★☆☆	★★★★☆	★★★★★
Traveller can securely share biometric and biographic information after enrolment in TruID application	Traveller builds their status by requesting attestations, e.g. university, bank statement or vaccination etc.	Traveller shares attestations needed for visa application (e.g. L1 for work purposes). Based on information shared, the traveller receives a visa from country X	For a following trip, upon arrival the traveller may go to a Known Traveller lane for expedited process due to their low-risk profile	Traveller continues to build their status every time identity information is added or shared	
Attestations	 <p>Passport Details Picture Match Lauren A Gonzales 5582 76323 23rd April, 2026 United States US Passport Service Female, 2'60, April 19'76 Download Details</p> <p>Facial Scan Fingerprint Right 4 Fingers Left 4 Fingers Thumb</p>	<p>Education: M.Ed Updated 29th Aug 2012 Stamp from University X certifying education credential</p> <p>Bank statement Updated 26th Sep 2017 Stamp from Bank Y certifying bank account credit rating AA</p> <p>Yellow fever vaccine Updated 12th Jan 2010 Stamp from Hospital Z certifying vaccination for virus XYZ</p>	<p>Visa: India Updated 29th Sep 2017 Stamp from India consulate travel from Oct-Dec, 2017</p>	 <p>Disembarkation in Progress Lane 2 TruID Active Updated 29th Sep 2017</p>	 <p>TruID Active Updated 29th Sep 2017 Use at locations marked with the symbols below. View Tutorial TruID Active Connections not available. Show QR Code</p>

App. 46 Bye-Bye Bargeld



Quelle: Silke Zöllner, Pressesprecherin des BDGW. aufgenommen in Berlin am 31.08.2021. per Mail zur Verfügung gestellt am 09.09.2021

Literatur- / Quellenverzeichnis

- Amnesty International (2021).** Deutschland: Neues BND-Gesetz ermöglicht anlasslose Massenüberwachung. Pressemitteilung 25.03.2021.
<https://www.amnesty.de/allgemein/pressemitteilung/deutschland-bnd-gesetz-massenueberwachung>. abgerufen am 12.08.2021
- Bacher, U./Beck, H. (2015).** Bargeld lacht - oder: sollen wir Bargeld abschaffen?. In: *Zeitschrift für das gesamte Kreditwesen : Pflichtblatt der Frankfurter Wertpapierbörse*, no. 68, 2015, pp. 38–41, https://www.hs-pforzheim.de/fileadmin/user_upload/uploads_redakteur/Die_Hochschule/Oeffentlichkeit/05.Publicationen/KONTUREN/KONTUREN2016/Bargeld_lacht.pdf. abgerufen am 03.07.2021
- Balbierer, T./Baumann, S./Bovensiepen, N. et al. (2021).** Pandora Papers - Neues Steueröasen-Leak belastet Hunderte Politiker. *Süddeutsche Zeitung:online*. 03.10.2021.
<https://www.sueddeutsche.de/projekte/artikel/politik/pandora-papers-geheimgeschaeftedevon-politikern-enttarnt-e500259/>. abgerufen am 02.01.2022
- Baumann, S./Hübscher, B./Klotz, U. (2017).** Virtuelles Schwarzarbeiten in der Plattformökonomie: Die Zuständigkeit staatlicher Aufsichtsorgane im Zeitalter der Digitalisierung. In: *Jahrbuch Der Schweizerischen Verwaltungswissenschaften*, 8(1), 11–27. <http://doi.org/10.5334/ssas.104>. abgerufen am 19.05.2021
- Bergemann, M./Ter Haseborg, V. (2021).** Die Wirecard Story - Die Geschichte einer Milliarden-Lüge. FinanzBuch Verlag München. ISBN 978-3-96092-775-4.
https://www.buecher.de/shop/muenchen/die-wirecard-story-ebook-pdf/ter-haseborg-volker-bergemann-melanie/products_products/detail/prod_id/59949153/. abgerufen am 09.01.2022
- Berghaus, M. (2011).** Luhmann leicht gemacht – Eine Einführung in die Systemtheorie. 3. überarbeitete und ergänzte Auflage 2011, Böhlau Verlag Köln; Weimar; Wien. ISBN 978-3-412-09204-7
- Bergen, P./Stermann, D./Schneider, E. et al. (2014).** Do NSA's Bulk Surveillance Programs Stop Terrorists?. *New America*. <http://www.jstor.org/stable/resrep10476>. abgerufen am 08.01.2022
- Bernstein, M. (2021).** Wie analoge Diebe 100.000 Euro in Bitcoin klauen konnten. *Süddeutsche Zeitung:online*, 02.04.2021.
<https://www.sueddeutsche.de/muenchen/muenchen-polizei-ueberfall-bitcoin-1.5254164>. abgerufen am 18.12.2021

- Bethmann, F. (2021).** Banken - Das rentable Geschäft mit den Negativzinsen. ZDFheute, 06.04.2021. <https://www.zdf.de/nachrichten/wirtschaft/negativzinsen-banken-verwahrtgelt-100.html>. abgerufen am 29.01.2022
- Betschka, J./Fröhlich, A. (2020).** Berliner Polizei blockiert Auskünfte - LKA-Staatsschützer riefen Daten späterer Opfer rechter Morddrohung ab. Der Tagesspiegel:online, 14.08.2020. <https://www.tagesspiegel.de/berlin/berliner-polizei-blockiert-auskuenfte-lka-staatsschuetzer-riefen-daten-spaeterer-opfer-rechter-morddrohung-ab/26096758.html>. abgerufen am 30.01.2022
- Better Than Cash Alliance (o.D.).** Members. Better Than Cash Alliance:online. <https://www.betterthancash.org/about/members>. abgerufen am 13.08.2021
- Better Than Cash Alliance (o.D.).** Why Digital Payments. Better Than Cash Alliance:online. <https://www.betterthancash.org/about/members>. abgerufen am 13.08.2021
- Beuth, P. (2020).** SolarWinds-Hack - Der Spionagefall des Jahres. Spiegel Netzwelt:online, 18.12.2020. <https://www.spiegel.de/netzwelt/netzpolitik/solarwinds-hack-der-spionagefall-des-jahres-a-0b728cc4-d375-4cb9-9450-3635ca8172a0>. abgerufen am 13.09.2021
- Biermann, K. (2021a).** NSO-Spionagesoftware – Achtung, Ihr iPhone wird vom Geheimdienst überwacht. Zeit Online, 25.11.2021. <https://www.zeit.de/digital/datenschutz/2021-11/nso-spionagesoftware-pegasus-apple-iphone/komplettansicht>. abgerufen am 26.11.2021
- Biermann, K. (2021b).** Spionagesoftware – Facebook warnt 50.000 Betroffene vor staatlicher Überwachung. Zeit Online, 16.12.2021. <https://www.zeit.de/digital/datenschutz/2021-12/facebook-schutz-staatliche-ueberwachung-pegasus>. abgerufen am 17.12.2021
- Biselli, A. (2020).** Unberechtigte Datenabfragen bei Bundespolizei und BKA. Netzpolitik:online, 05.10.2020. <https://netzpolitik.org/2020/kleine-anfrage-unberechtigter-datenabfragen-bei-bundespolizei-und-bka/>. abgerufen am 12.10.2021
- Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2020a).** Digitaler Euro auf der Blockchain - Infopapier. Berlin. <https://www.bitkom.org/Bitkom/Publikationen/Digitaler-Euro-auf-der-Blockchain>. abgerufen am 24.06.2021
- Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2020b).** Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der digitalen Welt. Berlin. <https://www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-vernetzten-Welt>. abgerufen am 19.05.2021

- Bognanni, M./Mascolo, G. (2021).** „Neue Form der Organisierten Kriminalität“. tagesschau:online, 07.06.2021. <https://www.tagesschau.de/investigativ/ndr-wdr/cum-ex-brorhilker-101.html>. abgerufen am 20.01.2022
- Boumans, D./Schneider, F. (2019).** Ausmaß und Auswirkungen der Schattenwirtschaft – Ergebnisse der Sonderfragen des Ifo World Economic Survey | Veröffentlichung | Ifo Institut.“ *Ifo Schnelldienst*, vol. 72, no. 24, Dec. 2019, pp. 90–95, <https://www.ifo.de/publikationen/2019/aufsatz-zeitschrift/ausmass-und-auswirkungen-der-schattenwirtschaft-ergebnisse>. abgerufen am 19.05.2021
- Böhm, H. (2012).** Steueroasen im Vergleich - Entwicklungen im Zuge der Finanz- und Wirtschaftskrise. Diplomarbeit. Universität Wien, Fakultät für Wirtschaftswissenschaften. urn:nbn:at:at-ubw:1-30011.43702.411863-0. doi 10.25365/thesis.23061. <https://theses.univie.ac.at/detail/20619#>. abgerufen am 02.01.2022
- Braunschweig, C. / Pichler, B. (2021).** Der Ursprung des Geldes (Geld und Geldgebrauch). In: Die Kreditgeldwirtschaft. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-31277-0_2. abgerufen am 24.06.2021
- Breier, S. (2017).** Die Bedeutung von Geld. In: Geld Macht Gefühle. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54601-7_4. abgerufen am 24.06.2021
- Brodbeck, K.-H. (2014).** Phänomenologie des Geldes. Working Paper Serie der Institute für Ökonomie und Philosophie Nr. Ök-3, 10/2014. Cusanus Hochschule. Bernkastel-Kues. https://www.researchgate.net/publication/270220379_Phanomenologie_des_Geldes. abgerufen am 25.06.2021
- Brown, M./LendEDU (2020).** Dirty Money: New Research Reveals the Filthiness of Our Cash, Cards, & Coins | LendEDU. 16. Juni 2020, <https://lendedu.com/blog/dirty-money-credit-cards/>. abgerufen am 17.07.2021
- Brown, S. D. (2016).** Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal*. 2016; 89(4):327-339. <https://doi.org/10.1177/0032258X16658927>. abgerufen am 08.11.2021
- Bruni, F./ Llewellyn, D. T. (2009).** Preface. In: Congdon, T./Goodhart, C./Eisenbeis, R. et al.: THE FAILURE OF NORTHERN ROCK: A MULTI-DIMENSIONAL CASE STUDY. SUERF – The European Money and Finance Forum. Wien. ISBN 978-3-902109-46-0. <https://www.suerf.org/studies/2141/the-failure-of-northern-rock-a-multi-dimensional-case-study>. abgerufen am 08.08.2021

- Budras, C. (2016).** Der größte Steuerbluff aller Zeiten. Frankfurter Allgemeine Zeitung (FAZ):online, 13.06.2016. <https://www.faz.net/aktuell/finanzen/cum-ex-geschaefte-der-groesste-steuerbluff-aller-zeiten-14281836.html>. abgerufen am 10.01.2022
- Buiter, W. (2009).** In eine bessere Zukunft mit negativen Zinsen. *Humane Wirtschaft*, no. 4, Apr. 2009, pp. 3–9, https://humane-wirtschaft.de/wp-content/uploads/2009/04/buiter_nullzins.pdf. abgerufen am 30.06.2021
- Bullough, O. (2019).** The great American tax haven: why the super-rich love South Dakota. The Guardian:online, 14.11.2019. <https://www.theguardian.com/world/2019/nov/14/the-great-american-tax-haven-why-the-super-rich-love-south-dakota-trust-laws>. abgerufen am 04.10.2021
- Bund der Steuerzahler e.V. (2021).** Steuerzahlergedenktag 2021. *steuerzahler.de*, 2021, <https://www.steuerzahler.de/steuerzahlergedenktag/?L=0>. abgerufen am 24.07.2021
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2021).** Die Lage der IT-Sicherheit in Deutschland 2021. Bonn. https://www.bsi.bund.de/DE/Service-Navi/Publicationen/Lagebericht/lagebericht_node.html. abgerufen am 21.10.2021
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2020).** Virtuelle Währungen/Virtual Currency (VC). 18.09.2020. https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html. abgerufen am 17.11.2021
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2021).** Bericht zur Sonderauswertung Mitarbeitergeschäfte mit Bezug zu Wirecard von BaFin-Beschäftigten, Anzeigezeitraum 01. Januar 2018 - 30. September 2020. 05.02.2021. https://www.bafin.de/SharedDocs/Downloads/DE/Bericht/dl_bafin-bericht_zur_sonderauswertung_mitarbeitergeschaeft.html. abgerufen am 09.01.2022
- Bundesanzeiger (o.D.).** Transparenzregister - Fragen & Antworten. <https://www.transparenzregister.de/treg/de/hilfe?1>. abgerufen am 05.01.2022
- Bundeskriminalamt (BKA) (2018).** Bundeslagebild Cybercrime 2017. 27.09.2018. Wiesbaden. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html. abgerufen am 24.12.2021
- Bundeskriminalamt (BKA) (2020a).** Bundeslagebilder Organisierte Kriminalität - Bundeslagebild Organisierte Kriminalität 2019. 6 Nov. 2020. Wiesbaden. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html. abgerufen am 23.07.2021

Bundeskriminalamt (BKA) (2020b). Bundeslagebild Korruption 2019. 02.11.2020.

Wiesbaden.

https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Korruption/korruption_node.html. abgerufen am 19.07.2021

Bundeskriminalamt (BKA) (2020c). Bundeslagebild Cybercrime 2019. 30.09.2020.

Wiesbaden. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html. abgerufen am 19.05.2021

Bundeskriminalamt (BKA) (2020d). Lageprodukte aus dem Bereich Cybercrime - Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie. 30.09.2020. Wiesbaden.

https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html. abgerufen am 19.05.2021

Bundeskriminalamt (BKA) (2021a). Bundeslagebild Angriffe auf Geldautomaten 2020. 15.

Juni 2021. Wiesbaden. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/AngriffeGeldautomaten/angriffeAufGeldautomaten_node.html. abgerufen am 23.07.2021

Bundeskriminalamt (BKA) (2021b). Bundeslagebild Cybercrime 2020. 10.05.2021.

Wiesbaden. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html. abgerufen am 19.05.2021

Bundesministerium der Finanzen (BMF) (2016). Monatsbericht des BMF. April 2016.

https://www.bundesfinanzministerium.de/Monatsberichte/2001-2016/Inhalte/Monatsbericht-Archiv-Downloads/2016/monatsbericht-2016-04-deutsch.pdf?__blob=publicationFile&v=3. abgerufen am 03.07.2021

Bundesministerium der Finanzen (BMF) (2017). BMF-Monatsberichtbericht August 2017 -

Vierte EU-Geldwäscherichtlinie – Novellierung des Geldwäschegesetzes.

<https://www.bundesfinanzministerium.de/Monatsberichte/2017/08/Inhalte/Kapitel-3-Analysen/3-3-EU-Geldwaescherichtlinie-Novellierung-Geldwaeschegesetz.html>. abgerufen am 11.08.2021

Bundesministerium der Finanzen (BMF) (2019). Erste Nationale Risikoanalyse 2018/2019.

Oktober 2019, https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.html. abgerufen am 20.05.2021

BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT e. V. (BDSW)/Bundesvereinigung Deutscher Geld- und Wertdienste (BDGW) / BDLS Bundesverband der Luftsicherheitsunternehmen (2021). Sicherheitswirtschaft in Deutschland.

https://www.bdgw.de/images/statistik-satz/Statistik-satz_BDSW_BDGW_BDLS_16072021.pdf. 16.07.2021. abgerufen am 19.07.2021

Burch, E. (2021). Kryptowährungen einfach erklärt - Was sind die Vor- und Nachteile?.

02.04.2021. <https://blog.hslu.ch/majorobm/2021/04/02/kryptowahrungen-einfach-erklart-sind-die-vor-und-nachteile/>. abgerufen am 18.11.2021

Bussmann, K. (2015): Dunkelfeldstudie über den Umfang der Geldwäsche in Deutschland und über die Geldwäscherisiken in einzelnen Wirtschaftssektoren - Zusammenfassung. Aug. 2015, [https://busmann.jura.uni-](https://busmann.jura.uni-halle.de/forschung/abgeschlossene_projekte/geldwaeschestudie_i/)

[halle.de/forschung/abgeschlossene_projekte/geldwaeschestudie_i/](https://busmann.jura.uni-halle.de/forschung/abgeschlossene_projekte/geldwaeschestudie_i/). abgerufen am 18.05.2021

Cabinakova, J./Knümann, F./Horst, F. (2019). Kosten der Bargeldzahlung im Einzelhandel - Studie zur Ermittlung und Bewertung der Kosten, die durch die Bargeldzahlung im Einzelhandel verursacht werden. Deutsche Bundesbank - Zentralbereich Bargeld.

Frankfurt am Main. <https://www.bundesbank.de/de/publikationen/berichte/studien/kosten-der-bargeldzahlung-im-einzelhandel-776464>. abgerufen am 10.05.2021

Chakravorti, B. (2017). Early Lessons from India's Demonetization Experiment. Harvard

Business Review:online, 14.03.2017. <https://hbr.org/2017/03/early-lessons-from-indias-demonetization-experiment>. abgerufen am 22.01.2022

Charoenwong, B./Bernardi, M. (2021). A Decade of Cryptocurrency 'Hacks': 2011 – 2021

(October 1, 2021). Available at SSRN: <https://ssrn.com/abstract=3944435> / <https://dx.doi.org/10.2139/ssrn.3944435>. abgerufen am 14.12.2021

CipherTrace (2021a). Cryptocurrency Crime and Anti-Money Laundering Report. February

2021. Report-CAML-20210128. <https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/>. abgerufen am 24.08.2021

CipherTrace (2021b). What Exactly is a Virtual Asset Service Provider (VASP)? - The Differences

Between a VASP, MSB, Money Transmitter, Digital Asset Customer, and How it Impacts Crypto Compliance. <https://ciphertrace.com/what-exactly-is-a-virtual-asset-service-provider-vasp/>. abgerufen am 28.12.2021

Coinwissen (o.D.). Vor und Nachteile von Kryptowährungen. [https://www.coinwissen.de/vor-](https://www.coinwissen.de/vor-und-nachteile-von-kryptowahrungen/)

[und-nachteile-von-kryptowahrungen/](https://www.coinwissen.de/vor-und-nachteile-von-kryptowahrungen/). abgerufen am 18.11.2021

- Conrads, F. (2018).** Ist Bares noch Wahres? Zur Zukunft Des Bargelds." In:
WOCHENSCHAU, 69. Jahrgang - Sonderausgabe „Geld und Geldpolitik“, Aug. 2018, pp.
 12–17, Wochenschau Verlag.
[https://www.bundesbank.de/resource/blob/759192/ec39b74903cc68ef9d7743b6337ea453/
 mL/wochenschau-sonderausgabe-data.pdf](https://www.bundesbank.de/resource/blob/759192/ec39b74903cc68ef9d7743b6337ea453/mL/wochenschau-sonderausgabe-data.pdf). abgerufen am 30.06.2021
- Correctiv (2021).** Cumex Files. Correctiv:online, 21.10.2021. [https://correctiv.org/top-
 stories/2021/10/21/cumex-files-2/](https://correctiv.org/top-stories/2021/10/21/cumex-files-2/). abgerufen am 11.01.2022
- Daubenberger, M./Salewski, C./Schröm, O. (2021).** Bankier suchte Hilfe bei Scholz.
 tagesschau:online, 09.09.2021. [https://www.tagesschau.de/investigativ/panorama/warburg-
 101.html](https://www.tagesschau.de/investigativ/panorama/warburg-101.html). abgerufen am 11.01.2022
- De Groen, W. P./Busse, M./Zarra, A. (2017).** Study on an EU initiative for a restriction on
 payments in cash - Final Report. Ecorys/Centre for European Policy Studies (CEPS).
 December 2017. Brüssel. [https://ec.europa.eu/info/news/economy-finance/security-union-
 commission-publishes-report-restriction-payments-cash-2018-jun-13_en](https://ec.europa.eu/info/news/economy-finance/security-union-commission-publishes-report-restriction-payments-cash-2018-jun-13_en). abgerufen am
 04.07.2021
- Deker, C. (2022).** Corona-Kontaktnachverfolgung - Polizei fragt in mehr als 100 Fällen Daten
 ab. ZDFheute:online, 20.01.2022. [https://www.zdf.de/nachrichten/politik/corona-
 kontaktdaten-abfrage-datenschutz-100.html](https://www.zdf.de/nachrichten/politik/corona-kontaktdaten-abfrage-datenschutz-100.html). abgerufen am 30.01.2022
- Deutsche Bundesbank (2018).** Zahlungsverhalten in Deutschland 2017 Vierte Studie über die
 Verwendung von Bargeld und unbaren Zahlungsinstrumenten.
[https://www.bundesbank.de/de/publikationen/berichte/studien/zahlungsverhalten-in-
 deutschland-737966](https://www.bundesbank.de/de/publikationen/berichte/studien/zahlungsverhalten-in-deutschland-737966). abgerufen am 27.06.2021
- Deutsche Bundesbank (2019).** Bargeldnachfrage in der Schattenwirtschaft. Monatsbericht
 März 2019. Frankfurt am Main
[https://www.bundesbank.de/de/publikationen/berichte/monatsberichte/monatsbericht-
 maerz-2019-781628](https://www.bundesbank.de/de/publikationen/berichte/monatsberichte/monatsbericht-maerz-2019-781628). abgerufen am 30.06.2021
- Deutsche Bundesbank (2020a).** Zahlen & Fakten rund ums Bargeld - Abbildungen, Tabellen
 und Erläuterungen zum Bargeld. Stand März 2020, [https://docplayer.org/195687681-Zah-
 len-fakten-rund-ums-bargeld-abbildungen-tabellen-und-erlaeuterungen-zum-bargeld-deut-
 sche-bundesbank-stand-maerz-2020.html](https://docplayer.org/195687681-Zahlen-fakten-rund-ums-bargeld-abbildungen-tabellen-und-erlaeuterungen-zum-bargeld-deutsche-bundesbank-stand-maerz-2020.html). abgerufen am 17.05.2021
- Deutsche Bundesbank (2020b).** Von Bargeld geht kein besonderes Infektionsrisiko für Bürger
 aus. 17 Mar. 2020, [https://www.bundesbank.de/de/aufgaben/themen/von-bargeld-geht-
 kein-besonderes-infektionsrisiko-fuer-buerger-aus--828542](https://www.bundesbank.de/de/aufgaben/themen/von-bargeld-geht-kein-besonderes-infektionsrisiko-fuer-buerger-aus--828542). abgerufen am 04.07.2021

- Deutsche Bundesbank (2021).** Zahlungsverhalten in Deutschland 2020 - Bezahlen im Jahr der Corona-Pandemie - Erhebung über die Verwendung von Zahlungsmitteln. 14.01.2021. <https://www.bundesbank.de/de/publikationen/berichte/studien/zahlungsverhalten-in-deutschland-2020-855642>. abgerufen am 24.06.2021
- Deutscher Bundestag (2017).** Beschränkungen von Bargeldzahlungen WD 4 - 3000 - 058/17. Wissenschaftliche Dienste 4: Haushalt und Finanzen. <https://www.bundestag.de/resource/blob/525382/131e434f07765aea13023a2d9cd9fce2/WD-4-058-17-pdf-data.pdf>. abgerufen am 11.08.2021
- Deutscher Bundestag (2021).** Drucksache 19/26831 - Anzahl und Entwicklung von Kontoabfragen durch Sozialbehörden. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten René Springer, Uwe Witt, Jörg Schneider, Ulrike Schielke-Ziesing und der Fraktion der AfD. 19.02.2021. Berlin. <https://dserver.bundestag.de/btd/19/268/1926831.pdf>. abgerufen am 23.07.2021
- Díaz-Struck, E./Reuter, D./Armendariz, A. et al./International Consortium of Investigative Journalists(ICIJ) (2021).** Pandora Papers: An offshore data tsunami. ICIJ:online, 03.10.2021. <https://www.icij.org/investigations/pandora-papers/about-pandora-papers-leak-dataset/>. abgerufen am 18.11.2021
- dieDatenschützer Rhein Main (2021).** Rechtsextreme Polizist*innen in Hessen nutzen Polizeicomputer für illegale Datenabfragen – Innenminister erklärt Datenschutz zur Privatsache der Betroffenen. dieDatenschützer Rhein Main:online, 09.03.2021. <https://ddrm.de/rechtsextreme-polizistinnen-in-hessen-nutzen-polizeicomputer-fuer-illegale-datenabfragen-innenminister-erklaert-datenschutz-zur-privatsache-der-betroffenen/>. abgerufen am 30.01.2022
- Dion-Schwarz, C./Manheim, D./Johnston, P. (2019).** Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats, Santa Monica, Calif.: RAND Corporation, RR-3026, 2019. As of August 17, 2021: https://www.rand.org/pubs/research_reports/RR3026.html. abgerufen am 24.08.2021
- Direzione Investigativa Antimafia (2020).** RELAZIONE del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia, Gennaio-Giugno 2020. Rom. <https://direzioneeinvestigativaantimafia.interno.gov.it/semestrali/sem/2020/1sem2020.pdf>. abgerufen am 20.06.2021
- Donath, A./Golem (2021).** EZB-Konzept - Digitaler Euro soll Bargeld ähneln. Golem - IT-News für Profis:online, 27.05.2021. <https://www.golem.de/news/ezb-konzept-digitaler-euro-soll-bargeld-aehneln-2105-156805.html>. abgerufen am 11.08.2021

- Dostojewski, F. M. (1861/1862).** Aufzeichnungen aus einem Totenhaus. In der Übersetzung von Alexander Eliasberg. Hofenberg Digital. Verlag der Contumax GmbH & Co. KG. Herausgegeben von Karl-Maria Guth, Berlin 2016. Erstdruck 1861/62 in der Zeitschrift Wremja. ISBN 978-3-8430-6695-2
- Durgeloh Oliva, T. (2020).** EU-Geldwäschegesetz. LinkedIn:online, 10.01.2020. <https://de.linkedin.com/pulse/eu-geldwaeschegesetz-thomas-durgeloh-oliva>. abgerufen am 11.08.2021
- Earl, M./Perring, F. (2016).** Zatarra-Report. Zatarra Research & Investigations. <https://viceroy-research.org/wp-content/uploads/2020/07/final-main-report-zatarra-edited-3.pdf>. abgerufen am 09.01.2022
- Ehlers, U. D. (Hrsg.) (2018).** Die gesellschaftlichen Folgen der Digitalisierung für die Bürger/innen – Arbeitspapiere zur Digitalisierung 2030. Duale Hochschule Baden-Württemberg, Karlsruhe. <https://competence.files.wordpress.com/2018/11/dhbw-ehlers-digitalisierung-thema-bc3bcrgerunddigitalisierung1.pdf>. abgerufen am 21.10.2021
- Ehmann, E. (2017).** Datenschutzverstoß im Meldeamt: Geldstrafe!. Datenschutz Praxis:online, 13.02.2017. <https://www.datenschutz-praxis.de/pleiten-pech-pannen/datenschutzverstoss-meldeamt-geldstrafe/?icomefrom=/fachartikel/datenschutzverstoss-meldeamt-geldstrafe/>. abgerufen am 20.12.2021
- Eisermann, D. (2020).** Kryptowährungen als Risiko für die öffentliche Sicherheit und Terrorismusbekämpfung - Gefahrenanalyse und Probleme der Regulierung. Counter Extremism Project (CEP) / Berlin Risk. Berlin, April 2020. <https://berlinrisk.com/new-publication-kryptowaehrungen-als-risiko-fur-die-offentliche-sicherheit-und-terrorismusbekampfung/>. abgerufen am 24.08.2021
- Emisoft (2021a).** Die länderspezifischen Kosten für Ransomware 2021 (sic!). Malwarelabor von Emisoft, 27.04.2021. <https://blog.emisoft.com/de/38525/die-laenderspezifischen-kosten-fuer-ransomware-2021/>. abgerufen am 03.12.2021
- Emisoft (2021b).** Statistikbericht zu Ransomware (2. Quartal 2021). Malwarelabor von Emisoft, 06.07.2021. <https://blog.emisoft.com/de/38875/statistikbericht-zu-ransomware-2-quartal-2021/>. abgerufen am 03.12.2021
- Enste, D. H. (2019a).** Verluste der Unternehmen durch Schwarzarbeit. *Wirtschaftsdienst* **99**, 152–154 (2019). <https://doi.org/10.1007/s10273-019-2411-2>. abgerufen am 19.05.2021

- Enste, D. H. (2019b).** Korruption, Kartelle und Schwarzarbeit: 18 Prozent Umsatzverluste. IW-Kurzbericht no. 5472019, 13 Aug. 2019. Institut der Deutschen Wirtschaft.
<https://www.iwkoeln.de/studien/dominik-h-enste-18-prozent-umsatzverluste-433986.html>.
 abgerufen am 23.07.2021
- Enste, D. H./Schneider, F. (2007).** Schattenwirtschaft und Schwarzarbeit — Von Mythen, Missverständnissen und Meinungsmonopolen. *List Forum* **33**, 251–286 (2007).
<https://doi.org/10.1007/BF03373969>. abgerufen am 24.07.2021
- Eriksson, B. (2014).** Korten på bordet (Karten auf den Tisch). Cash Rebellion. Stockholm (Schweden). <https://www.kontantupproret.se/boken/>. abgerufen am 20.01.2022
- Eriksson, B. (2021).** Korttricket - SÅ BLIR DU LURAD PÅ NÄTET (Kartentrick - Wie man online betrogen wird). Cash Rebellion. Stockholm (Schweden). <https://www.kontantupproret.se/boken/>. abgerufen am 20.01.2022
- Europäische Kommission (2016).** Ein Aktionsplan für ein intensiveres Vorgehen gegen Terrorismusfinanzierung – Mitteilung der Kommission an das Europäische Parlament und den Rat. COM(2016) 50 final, 3 Feb. 2016.
https://www.bundesrat.de/SharedDocs/drucksachen/2016/0001-0100/64-16.pdf?__blob=publicationFile&v=6. abgerufen am 03.07.2021
- Europäische Kommission (2018).** Bericht der Kommission an das Europäische Parlament und den Rat über Barzahlungsbeschränkungen. COM(2018) 483. Generaldirektion Wirtschaft und Finanzen, 12. Juni 2018. [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2018\)483&lang=de](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)483&lang=de). abgerufen am 03.07.2021
- European Parliament, Directorate-General for Internal Policies of the Union/ Snyers, A./Houben, R. (2018).** Cryptocurrencies and blockchain : legal context and implications for financial crime, money laundering and tax evasion, European Parliament.
<https://data.europa.eu/doi/10.2861/280969>. abgerufen am 23.12.2021
- Europäischer Rat/Europäische Kommission (2015).** RICHTLINIE (EU) 2015/ 849 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 20. Mai 2015 - zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/ 2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/ 60/ EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/ 70/ EG der Kommission. Generaldirektion Wirtschaft und Finanzen, 20. Mai 2015. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L0849>. abgerufen am 11.08.2021

- Europäischer Rat/Europäische Kommission (2018).** RICHTLINIE (EU) 2018/843 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, 30. Mai 2018. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018L0843&from=EN>. abgerufen am 22.12.2021
- Europäischer Rat/Rat der Europäischen Union (o.D.)** Steuern: EU-Liste nicht kooperativer Länder und Gebiete. <https://www.consilium.europa.eu/de/policies/eu-list-of-non-cooperative-jurisdictions/>. abgerufen am 05.01.2021
- Europäisches Verbraucherzentrum Deutschland (2020).** Bargeld-Obergrenze im EU-Ausland. *EVZ Online*, 9 Jan. 2020, <https://www.evz.de/finanzversicherungen/hoechstgrenzen-bargeldzahlung.html>. abgerufen am 03.07.2021
- Europäische Zentralbank (EZB) (2016).** EZB stellt Produktion und Ausgabe der 500-€-Banknote ein. *EZB Online*, 04. Mai 2016. <https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.de.html>. abgerufen am 03.07.2021
- Europäische Zentralbank (EZB) (2017).** Was ist Seigniorage?. *EZB Online*, 7. April 2017. <https://www.ecb.europa.eu/explainers/tell-me/html/seigniorage.de.html>. abgerufen am 10.08.2021
- Europäische Zentralbank (EZB) (2021).** Ein digitaler Euro. *EZB Online*. https://www.ecb.europa.eu/paym/digital_euro/html/index.de.html. abgerufen am 11.08.2021
- Europol (2020).** Internet Organised Crime Threat Assessment (IOCTA) 2020. Den Haag. 05.10.2020. aktualisiert am 07.12.2021. <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020>. abgerufen am 28.12.2021
- Europol (2021).** European Union - Serious and Organised Crime Threat Assessment (SOCTA) 2021; A corrupting influence: The infiltration and undermining of Europe's economy and society by organized crime. Publications Office of the EU. Den Haag. 11.05.2021. DOI: 10.2813/02362. <https://op.europa.eu/en/publication-detail/-/publication/6e5575ce-c34b-11eb-a925-01aa75ed71a1>. abgerufen am 08.12.2021
- Fassbinder, K. (2019).** Keime: Kann Bargeld krank machen? | Apotheken-Umschau. *Apotheken Umschau Online*, 6 Dec. 2019. <https://www.apotheken-umschau.de/mein-koerper/keime-kann-bargeld-krank-machen-722357.html>. abgerufen am 17.07.2021

- Federal Bureau of Investigation (FBI) (2012).** (U) Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity. 24.04.2012. https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf. abgerufen am 19.12.2021
- Fend, R. (2018).** Scholz, Kubicki, Merz: Die Rolle der Spitzenpolitiker bei Cum Ex. Correctiv:online, 08.11.2018. <https://correctiv.org/aktuelles/cumex-files/2018/11/08/scholz-kubicki-merz-die-rolle-der-spitzenpolitiker-bei-cum-ex/>. abgerufen am 11.01.2022
- Financial Action Task Force (FATF) (2013a).** The Role of Hawala and other similar Service Providers in Money Laundering and Terrorist Financing. Oktober 2013. Paris (France). <https://www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html>. abgerufen am 20.12.2021
- Financial Action Task Force (FATF) (2013b).** Guidance for a Risk based Approach – Prepaid Cards, Mobile Payments and Internet-based Payment services. Juni 2013. Paris (France). <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html>. abgerufen am 26.12.2021
- Financial Action Task Force (FATF) (2014).** Virtual Currencies: Key Definitions and Potential AML/CFT Risks. Juni 2013. Paris (France). <https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>. abgerufen am 27.10.2021
- Financial Intelligence Unit (FIU) (2019).** Jahresbericht 2018. Köln. https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html. abgerufen am 24.12.2021
- Financial Intelligence Unit (FIU) (2020).** Jahresbericht 2019. Köln. https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html. abgerufen am 24.12.2021
- Financial Intelligence Unit (FIU) (2021).** Jahresbericht 2020. Köln. https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html. abgerufen am 24.12.2021
- Fitzgibbon, W./Cenziper, D./Georges, S./ International Consortium of Investigative Journalists (ICIJ) (2021).** US Offshore Havens - Suspect foreign money flows into booming American tax havens on promise of eternal secrecy - Confidential documents lay bare the inner workings of U.S. trust industry that serves global leaders and the super rich. ICIJ:online, 04.10.2021. <https://www.icij.org/investigations/pandora-papers/us-trusts-offshore-south-dakota-tax-havens/>. abgerufen am 29.12.2021

Fuest, C./Hugger, F./Neumeier, F. (2021). Gewinnverlagerung deutscher Großunternehmen in Niedrigsteuerländer - wie hoch sind die Steueraufkommensverluste?. ifo Schnelldienst, 2021, 74, Nr. 01, S. 38-42. München. <https://www.ifo.de/publikationen/2021/aufsatz-zeitschrift/gewinnverlagerung-deutscher-grossunternehmen>. abgerufen am 05.01.2022

fuldainfo (02.08.2020). Studie: Schwarzarbeit in Deutschland nimmt wegen Corona zu. 02.08.2020. <https://www.fuldainfo.de/studie-schwarzarbeit-in-deutschland-nimmt-wegen-corona-zu/>. abgerufen am 19.05.2021

G20 Financial Inclusion Experts Group (2010). ATISG Report: Innovative Financial Inclusion Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group. 25.05.2010. <https://www.mfw4a.org/publication/innovative-financial-inclusion-principles-and-report-innovative-financial-inclusion>. abgerufen am 23.01.2022

Ganßmann, H. (2002). Das Geldspiel. In: Deutschmann C. (eds). Die gesellschaftliche Macht des Geldes. Leviathan (Zeitschrift für Sozialwissenschaft), vol 21. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-322-91614-3_2. abgerufen am 26.01.2022

Gasser, J./Benz, A./Hess, M. (2019). Negativzinsen: von der Notfallmassnahme zur «neuen Normalität» -und zurück? - Eine Studie der SBVg zu der Wirksamkeit und den Folgen der Negativzinspolitik. Schweizerische Bankiervereinigung. Basel. https://www.finews.ch/images/download/SBVg_Negativzins_DE_1s.pdf. abgerufen am 15.07.2021

Genzmer, J./Kogel, D. (2021). Pandora Papers - Ein riesiger Skandal ohne Aufschrei. Deutschlandfunk Kultur:online, 23.10.2021. <https://www.deutschlandfunkkultur.de/pandora-papers-ein-riesiger-skandal-ohne-aufschrei-100.html>. abgerufen am 24.12.2021

Gersbach, H./Bundesministerium der Wirtschaft und Energie (BMWi) (2017). Zur Diskussion um Bargeld und die Null-Zins-Politik der Zentralbank - Gutachten des Wissenschaftlichen Beirats beim Bundesministerium für Wirtschaft und Energie. 09.02.2017. Berlin. <https://www.bmwi.de/Redaktion/DE/Publikationen/Ministerium/Veroeffentlichung-Wissenschaftlicher-Beirat/gutachten-wissenschaftlicher-beirat-gutachten-diskussion-um-bargeld.html>. abgerufen am 10.05.2021

Global Alliance For Tax Justice/Tax Justice Network (2021). The State of Tax Justice 2021. 16.11.2021. <https://taxjustice.net/reports/the-state-of-tax-justice-2021/>. abgerufen am 02.01.2022

- Glory Global Solutions (Germany) GmbH (2020).** Glory Cash Report 2020: Zahlungs- und Einkaufsverhalten in Zeiten der Pandemie - Neue Herausforderungen und Chancen für die Customer Experience im Einzelhandel. https://www.glory-global.com/-/media/GloryGlobal/Downloads/DE-DE/Cash-Report_DE_DE/GLORY-CASH-REPORT-2020.pdf. abgerufen am 17.05.2021
- Grauer, K./Updegrave, H. (2021).** The 2021 Crypto Crime Report Everything you need to know about ransomware, darknet markets, and more. Chainalysis. <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>. abgerufen am 24.08.2021
- Grauer, K./Kueshner, W./Updegrave, H. (2022).** The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime. Chainalysis. <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>. abgerufen am 16.02.2022
- Groß, J./Klein, M./ Sandner, P. (2020).** Digitale Zentralbankwährungen: Chancen, Risiken und Blockchain-Technologie. *Wirtschaftsdienst* 100, 545–549 (2020). <https://doi.org/10.1007/s10273-020-2702-7>. abgerufen am 15.07.2021
- Gutierrez, C. (2010).** MasterCard goes to War with Cash. *Forbes:online*, 15.09.2010. <https://www.forbes.com/2010/09/15/mastercard-credit-consumer-markets-equities-financial-visa.html?sh=81d8a7321325>. Abgerufen am 20.02.2022
- Harris, A. (2020).** Don't Be a Dactylochrematophobe! . *Cash Essentials:online*, 20.04.2020. <https://cashesentials.org/dont-be-a-dactylochrematophobe/>. abgerufen am 17.07.2021
- Häring, N. (2018).** Schönes neues Geld - PayPal, WeChat, Amazon Go – Uns droht eine totalitäre Weltwährung. Campus Verlag, Frankfurt am Main. ISBN 978-3-593-43930-3
- Häußling, R. (2018).** Geld. In: Kopp, J./ Steinbach A. (eds). *Grundbegriffe der Soziologie*. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-20978-0_24. abgerufen am 21.06.2021
- Hedelius, P. (2014).** Swishnotan skjuts upp! (Swishnotan verschoben!). *Svenska Dagbladet:online*, 05.06.2014. <http://blog.svd.se/hedeliusaffarer/2014/06/05/swish-vad-fel-det-blev/>. bgerufen am 26.01.2022
- Hempel, K. (2021).** Cum-Ex-Geschäfte sind strafbar. *tagesschau:online*, 28.07.2021. <https://www.tagesschau.de/wirtschaft/cum-ex-bgh-urteil-103.html>. abgerufen am 11.01.2022
- Henkel, T. (2020).** Darknet – die dunkle Seite des Internets?. In: Rüdiger TG., Bayerl P. (eds). *Cyberkriminologie*. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-28507-4_7. abgerufen am 19.08.2021

- Hennies, M. O. (2016).** Bargeld als elementarer Bestand einer freiheitlichen Gesellschaftsordnung. Cash as an elementary component of liberal social order. Estonian Discussions on Economic Policy, 24(1). <https://doi.org/10.15157/tpep.v24i1.12985>. abgerufen am 30.06.2021
- Herger, N. (2016).** Wie funktionieren Zentralbanken? - Geld- und Währungspolitik verstehen. Springer Fachmedien Wiesbaden. <https://doi.org/10.1007/978-3-658-07876-8>. abgerufen am 24.06.2021
- Hetzer, W. (2014).** Ist die Deutsche Bank eine kriminelle Vereinigung?. Die Kriminalpolizei - Zeitschrift der Gewerkschaft der Polizei. Wien. 04/2014. S. 1-16. <https://www.kriminalpolizei.de/ausgaben/2014/maerz/detailansicht-maerz/artikel/ist-die-deutsche-bank-eine-kriminelle-vereinigung.html>. abgerufen am 28.12.2021
- Hickel, R. (2016).** Im Minuszinskapitalismus - Das billige Geld und das Versagen der Politik. In: Blätter für deutsche und internationale Politik, 61. Jahrgang, 11/2016. Blätter Verlagsgesellschaft Berlin. S. 83-90. <https://www.blaetter.de/download/pdf/27484>. abgerufen am 16.05.2021
- Hipp, D. (2021).** Positionspapier der Großen Koalition - Zum Abschied noch ein »Ja« zur Vorratsdaten-Speicherung. Spiegel Netzwelt:online, 27.10.2021. <https://www.spiegel.de/netzwelt/netzpolitik/grosse-koalition-zum-abschied-noch-ein-ja-zur-vorratsdaten-speicherung-a-266cd41b-8589-4b0a-bb9e-4d78067d5fda>. abgerufen am 28.10.2021
- Hirdina, R. (2016).** Die gesetzliche Einschränkung von Bargeldzahlungen und die Abschaffung von Bargeld auf dem rechtlichen Prüfstand. Weidener Diskussionspapiere Nr. 57. Dezember 2016. Ostbayerische Technische Hochschule Amberg-Weiden. Weiden i.d.OPf. <http://hdl.handle.net/10419/149391>. abgerufen am 18.05.2021
- Hochstätter, M. (2022).** Cyber-War und Energie-Versorgung - Mit Putins Hackern droht auch uns der Blackout, doch nur Österreich warnt seine Bürger. Focus Online, 30.01.2022. https://www.focus.de/politik/deutschland/cyber-war-und-energie-versorgung-habt-angst-und-rechnet-mit-dem-schlimmsten-mit-putins-hackern-kommt-der-blackout_id_45088024.html. abgerufen am 30.01.2022
- Hornetsecurity (o.D.).** Crypto Mining: Definition und Funktion erklärt - Welche Gefahren birgt Crypto Mining für Unternehmen und wie kann man sich dagegen schützen?. <https://www.hornetsecurity.com/de/wissensdatenbank/crypto-mining/>. abgerufen am 15.11.2021

- Horten, B. / Gräber, M. (2020).** Cyberkriminalität - Übersicht zu aktuellen und künftigen Erscheinungsformen. *Forens Psychiatr Psychol Kriminol* 14, 233–241 (2020).
<https://doi.org/10.1007/s11757-020-00605-0>. abgerufen am 19.08.2021
- Huber, E. (2019).** Cybercrime. In: Cybercrime. Springer VS, Wiesbaden.
https://doi.org/10.1007/978-3-658-26150-4_3. abgerufen am 19.08.2021
- Hungerland, F./Quitau, J./Rotterdam, J. et al. (2017).** Bargeld: ohne Zukunft?. In: Die Zukunft des Geldes - das Geld der Zukunft, Strategie 2030 - Vermögen und Leben in der nächsten Generation, No. 24, S. 8-17. Berenberg Bank und Hamburgisches WeltWirtschaftsInstitut (HWWI), Hamburg.
<https://www.econstor.eu/bitstream/10419/162390/1/890366063.pdf>. abgerufen am 19.05.2021
- International Consortium of Investigative Journalists (ICIJ) (2020).** FinCen Files: Global banks defy U.S. crackdowns by serving oligarchs, criminals and terrorists - The FinCEN Files show trillions in tainted dollars flow freely through major banks, swamping a broken enforcement system. 20.09.2020, aktualisiert am 21.09.2020 und 22.12.2020.
<https://www.icij.org/investigations/fincen-files/global-banks-defy-u-s-crackdowns-by-serving-oligarchs-criminals-and-terrorists/>. abgerufen am 24.06.2021
- International Institute for Counter-Terrorism (ICT) (2021).** Cyber Report January-March 2021. 04.08.2021. Herzliya (Israel).
<https://www.ict.org.il/Article/2708/CyberReportJanuaryMarch2021#gsc.tab=0>. abgerufen am 20.12.2021
- Iwersen, S./Votsmeier, V./Bender, R. (2019).** Cum-Ex-Deals - Die Chronik. Handelsblatt:online, 16.03.2016, akt. am 06.09.2019.
<https://www.handelsblatt.com/finanzen/banken-versicherungen/cum-ex/vom-renditeturbo-zum-karrierekiller-cum-ex-deals-die-chronik/13033390.html?ticket=ST-3800253-Ap7syCxRHEVeLsiu1jgy-ap4>. abgerufen am 11.01.2022
- Jasch, A./Companisto (2017).** Kryptowährungen - Die 10 wichtigsten im Überblick.
<https://www.companisto.com/de/academy/anlageformen-und-strategien/kryptowaehrungen-die-10-wichtigsten-im-berblick>. abgerufen am 16.08.2021
- Jakubeit, R. (2021).** The Wirecard scandal and the role of BaFin - A case for unifying capital markets supervision in the European Union. Working Paper 5/2021, 22.03.2021. Luiss School of European Political Economy. <https://sep.luiss.it/research/working-papers/2021/03/22/r-jakubeit-wirecard-scandal-and-role-bafin-case-unifying-capital->
abgerufen am 07.01.2022

- Katarzyna, C. (2019).** Cryptocurrencies: Opportunities, Risks and Challenges for Anti-Corruption Compliance Systems. 2019 OECD Global Anti-Corruption & Integrity Forum, 20.-21.03.2019. Paris. <https://www.oecd.org/corruption/integrity-forum/academic-papers/Ciupa-Katarzyna-cryptocurrencies.pdf>. abgerufen am 24.08.2021
- Khera, R. (2011).** The UID Project and Welfare Schemes. Economic and Political Weekly, Vol. 46, Issue No. 09, 26 Feb, 2011. <https://www.epw.in/journal/2011/09/perspectives/uid-project-and-welfare-schemes.html>. abgerufen am 22.01.2022
- Kirchhof, P. (2021).** Geld im Sog der Negativzinsen. Verlag C.H. Beck oHG, München. ISBN 978-3-406-77869-8
- Kireyev, A. P. (2017).** The Macroeconomics of De-Cashing. IMF Working Papers, Volume 2017: Issue 071. <https://doi.org/10.5089/9781475589252.001>. abgerufen am 24.08.2021
- Klein, D. (2021).** Report: Italian Mafia Exploits Cryptocurrency and the Deep Web. OCCRP - Organized Crime and Corruption Reporting Project. 24.08.2021. <https://www.occrp.org/en/daily/15061-report-italian-mafia-exploits-cryptocurrency-and-the-deep-web>. abgerufen am 13.09.2021
- Kleine, J./Krautbauer, M./Weller, T. (2013).** Cost of Cash: Status Quo und Entwicklungsperspektiven in Deutschland. Steinbeis Research Center for Financial Services - Center for Payment Studies. München. http://www.steinbeis-research.de/images/pdf-documents/CFP_Cost_Of_Cash_Studie_Steinbeis_Deutsch.pdf. abgerufen am 15.07.2021
- König, J. (2016).** Bares bleibt Wahres - Bargeld als Garant für Freiheit und Eigentum. In: *Argumente zu Marktwirtschaft und Politik*, no. 136, Nov. 2016, p. 20, http://www.stiftung-marktwirtschaft.de/uploads/tx_ttproducts/datasheet/Argument_136_Bargeld_2016_11.pdf. abgerufen am 30.06.2021
- Kösters, W./Hebler, M. (2005).** Geld. In: Schubert K. (eds). Handwörterbuch des ökonomischen Systems der Bundesrepublik Deutschland. VS Verlag für Sozialwissenschaften, Wiesbaden. https://doi.org/10.1007/978-3-322-80897-4_41. abgerufen am 21.06.2021
- Kruchem, T. (2020).** Manuskript zur Radiosendung: Digitale Identität aller Menschen - Fortschritt oder globale Überwachung?. SWR2:online, 20.10.2020. <https://www.swr.de/swr2/wissen/digitale-identitaet-aller-menschen-fortschritt-oder-globale-ueberwachung-swr2-wissen-2020-11-03-100.html>. abgerufen am 31.01.2022

- Krüger, M./ Seitz F. (2014).** Kosten und Nutzen des Bargelds und unbarer Zahlungsinstrumente - Übersicht und erste Schätzungen (Modul 1), Eine Studie im Auftrag der Deutschen Bundesbank.
<https://www.bundesbank.de/resource/blob/599416/a32478d9dc70fb9eff49616eb36c3cd8/mL/kosten-und-nutzen-des-bargelds-2014-data.pdf>. abgerufen am 18.05.2021
- Landgericht Berlin (2021).** Urteil in dem Rechtsstreit Bundesverband der Verbraucherzentralen und Verbraucherverbände • Verbraucherzentrale Bundesverband e.V. gegen Sparda-Bank Berlin eG. Aktenzeichen: 16 O 43/21, 28.10.2021.
https://www.vzbv.de/sites/default/files/2021-11/LG_Berlin_28.10.2021_%28002%29.pdf. abgerufen am 23.12.2021
- Langerock, J. (2019).** Off the Hook: How the EU is about to whitewash the world's worst tax havens. Oxford Committee for Famine Relief (Oxforder Komitee zur Linderung von Hungersnot) (OXFAM). Oxford (UK). doi: 10.21201/2019.4146.
<https://www.oxfam.org/en/research/hook-how-eu-about-whitewash-worlds-worst-tax-havens>. abgerufen am 21.05.2021
- Leisinger, C. (2021).** Nach der Pipeline-Erpressung schauen die Behörden bei Kryptowährungen genauer hin. Neue Zürcher Zeitung, (NZZ):online.
<https://www.nzz.ch/wirtschaft/der-colonial-pipeline-hack-bringt-das-fass-zum-ueberlaufen-ld.1625142>. abgerufen am 10.05.2021
- Letzgus, O. (2017).** Mobile Payment und Bargeld – Ergänzung oder Verdrängung?. In: Hierl L. (eds) Mobile Payment. Edition Bankmagazin. Springer Gabler, Wiesbaden.
https://doi.org/10.1007/978-3-658-14118-9_4. abgerufen am 10.05.2021
- Luca, M./McLeod, R./De Mets, L. et al. (2021).** The Rise and Rise of Biometric Mass Surveillance in the EU - A legal Analysis of biometric Mass Surveillance Practices in Germany, The Netherlands, And Poland. European Digital Rights (EDRi)/Edinburgh International Justice Initiative (EIJI). <https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/>. abgerufen am 08.01.2022
- Luhmann, N. (1994).** Die Wirtschaft der Gesellschaft. Suhrkamp Verlag Frankfurt am Main, 1. Auflage 1994. ISBN 978-3-518-28752-1
- Luhmann, N./ Baecker, D. (Hrsg.) (2004).** Einführung in die Systemtheorie. Carl-Auer-Systeme Verlag, Heidelberg, Zweite Auflage 2004. ISBN 3-89670-459-1
- Luhmann, N. (2018).** Soziale Systeme - Grundriß einer allgemeinen Theorie. Suhrkamp Verlag, Frankfurt am Main, 17. Auflage 2018. ISBN 978-3-518-28266-3

- Lutz, M./Müller, U. (2021).** Rasterfahndung bei Fluggästen - Deutliche Kritik an anlassloser Massenspeicherung. Welt:online, 14.11.2021. <https://www.welt.de/235033190>. abgerufen am 21.12.2021
- Mader, P. (2017).** Wem nützt finanzielle Inklusion? - FinanzdienstleisterInnen und große Konzerne suchen neue Geschäfte im globalen Zahlungsverkehr. Rundbrief Forum Umwelt & Entwicklung, 3/2017. https://www.researchgate.net/publication/320244306_Wem_nutzt_finanzielle_Inklusion. abgerufen am 23.01.2022
- Mai, H. (2017).** Bargeld, Freiheit und Verbrechen: Bargeld in der digitalen Welt. Deutsche Bank Research. Frankfurt am Main. https://www.deutschebank.de/dam/deutschebank/de/shared/pdf/20170112_Bargeld_Freiheit_und_Verbrechen_Bargeld_in_der_digitalen_Welt.pdf. abgerufen am 10.05.2021
- Mai, H. (2018).** Bargeld und Kriminalität. In: Lempp, J./Pitz, T./Sickmann, J. (eds). Die Zukunft des Bargelds. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-21720-4_9. abgerufen am 21.07.2021
- Mai, H. (2021).** Digitaler Euro für alle - Politische Ambitionen treffen auf ökonomische Realitäten. Gastkommentar. In: Wiener Zeitung:online, 08.07.2021. <https://www.wienerzeitung.at/meinung/gastkommentare/2111803-Digitaler-Euro-fuer-alle.html>. abgerufen am 30.07.2021
- Maisch, M./Keuchel, J. (2019).** Undurchsichtige Transfers - Wie Geldwäscher mit Hawala-Banking Geld in andere Staaten transferieren. Handelsblatt:Online, 19.11.2019. <https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/undurchsichtige-transfers-wie-geldwaescher-mit-hawala-banking-geld-in-andere-staaten-transferieren/25245524.html?ticket=ST-4080724-ZxC3OMz1ha5bSgSMOUGz-cas01.example.org>. abgerufen am 24.08.2021
- Malekos Smith, Z./Lostri, E./Lewis, J. A. (2020).** The Hidden Costs of Cybercrime. Studie von McAfee und Center for Strategic and International Studies (CSIS). Dezember 2020. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>. abgerufen am 24.11.2021
- Malik, N. (2018).** How Terrorists use Encryption, the Darknet, and Cryptocurrencies. The Henry Jackson Society - Centre for Response to Radicalisation and Terrorism (CRT). London (UK). ISBN 978-1-909035-45-4. <http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf>. abgerufen am 24.08.2021

- Mannheimer Swartling (2017).** Bankomat AB and BDB Bankernas Depå AB merge and will become one company. Mannheimer Swartling, 02.01.2017.
<https://www.mannheimerswartling.se/en/assignment/bankomat-ab-and-bdb-bankernas-depa-ab-merge-and-will-become-one-company/>. abgerufen am 26.01.2022
- Mansholt, M. (2018).** Er war einer der meistgesuchten Verbrecher der USA - nun jagt er Gangster im Darknet | stern:online, 04.01.2018. <https://www.stern.de/digital/online/er-war-einer-der-meist-gesuchten-verbrecher-der-usa---nun-jagt-er-gangster-im-darknet-7808640.html>. abgerufen am 16.11.2021
- Mansholt, M. (2021a).** El Salvador setzt auf Bitcoin als Staatswährung: Der holprige Start in die Zukunft | stern:online, 08.09.2021. <https://www.stern.de/digital/online/el-salvador-setzt-auf-bitcoin-als-staats-waehrung--der-holprige-start-in-die-zukunft-30724070.html>. abgerufen am 16.11.2021
- Mansholt, M. (2021b).** Eine Million Bitcoin aus illegalen Deals: Einer der größten Online-Geldwäscher geht in die Falle | stern:online, 29.04.2021.
<https://www.stern.de/digital/online/eine-million-bitcoin-schmutziges-geld--einer-der-groessten-online-geldwaescher-geht-in-die-falle-30506188.html>. abgerufen am 16.11.2021
- MasterCard (2014).** Studie: Bargeld Ist Eine Ekelige Angelegenheit | Europe Hub. *Mastercard Engagement Bureau Pressemitteilung*, 6 May 2014,
<https://newsroom.mastercard.com/eu/de/press-releases/studie-bargeld-ist-eine-ekelige-angelegenheit/>. abgerufen am 17.07.2021
- Mayer, T. (2021).** Die Vermessung des Unbekannten - Ein Essay über Geld und Gesellschaft in Zeiten radikaler Unsicherheit. FinanzBuch Verlag, München 2021. ISBN 978-3-95972-483-8
- McAfee / Center for Strategic and International Studies (CSIS) (2018).** Kurzfassung: Die wirtschaftlichen Folgen von Cyber-Kriminalität - keine Erleichterung in Sicht, Februar 2018. <https://www.mcafee.com/enterprise/de-de/assets/executive-summaries/es-economic-impact-cybercrime.pdf>. abgerufen am 24.11.2021
- Meyer, D. (2020).** Europäische Union und Währungsunion in der Dauerkrise - Analysen und Konzepte für einen Neuanfang. Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-27177-0. <https://doi.org/10.1007/978-3-658-27177-0>. abgerufen am 29.06.2021
- Michel, C (2017).** The United States of Anonymity. Kleptocracy Initiative, Hudson Institut. 03.11. 2017. <https://www.hudson.org/research/13981-the-united-states-of-anonymity>. abgerufen am 05.10.2021

- Michler, A.F. (2015).** Der Verzicht auf Bargeld löst keine ökonomischen Probleme. In: Thiele, C.-L./Niepelt, D./Krüger, M. (2015). Diskussion um das Bargeld: Hätte eine Abschaffung von Banknoten und Münzen wirklich Vorteile? In: *Ifo Schnelldienst*, vol. 68, no. 13, 2015, pp. 3–18, https://www.ifo.de/DocDL/ifosd_2015_13_1.pdf. abgerufen am 15.07.2021
- Mikl-Horke, G. (2011).** Geld – soziologische Interpretationen. In: Historische Soziologie – Sozioökonomie – Wirtschaftssoziologie. VS Verlag für Sozialwissenschaften.. pp. 188–209, https://doi.org/10.1007/978-3-531-92798-5_9. abgerufen am 24.06.2021
- Morscher, C. / Schlothmann, D. / Horsch, A. (2017):** Bargeld quo vadis?. Freiburger Arbeitspapiere, No. 2017/01, Technische Universität Bergakademie Freiberg, Fakultät für Wirtschaftswissenschaften, Freiberg, <http://nbn-resolving.de/urn:nbn:de:bsz:105-qucosa-224662>. abgerufen am 30.06.2021
- Müller, M. (2017).** Erfolgreich mit Geld und Risiko umgehen - Mit Finanzpsychologie bessere Finanzentscheidungen treffen, Springer-Verlag Berlin Heidelberg, 2. Auflage. <https://doi.org/10.1007/978-3-662-53165-5>. abgerufen am 27.07.2021
- Muth, M. (2021).** Nordkoreanische Hackergruppe - USA klagen "beste Bankräuber der Welt" an. Süddeutsche Zeitung:online, 18.02.2021. <https://www.sueddeutsche.de/digital/hacker-nordkorea-lazarus-us-justiz-1.5210297>. abgerufen am 31.01.2022
- Musto, C. (2022).** 12 Days of Cash: Christmas 2021 Series. CashEssentials:online, 07.01.2022. <https://cashesentials.org/12-days-of-cash-christmas-2021-series/>. abgerufen am 28.01.2022
- Nakamoto, S. (2008).** Bitcoin: A Peer-toPeer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>. abgerufen am 01.09.2021
- Nestler, N. (2017).** Kapitel 5: Geldwäsche, § 261 StGB. In: *Bank- und Kapitalmarktstrafrecht*, Springer Verlag, Berlin, Heidelberg. pp. 349–381. doi:10.1007/978-3-662-53959-0_5. https://doi.org/10.1007/978-3-662-53959-0_5. abgerufen am 19.05.2021
- Nickel, M. (2021).** Allgemeine Verständnisgrundlagen und Abgrenzung von Cum/Ex- und Cum/Cum-Geschäften. In: Die steuerstrafrechtliche Bewertung von Cum/Ex-Geschäften. Juridicum - Schriften zum Wirtschaftsstrafrecht, vol 5. Springer, Wiesbaden. https://doi.org/10.1007/978-3-658-35212-7_2. abgerufen am 10.01.2022
- Noack, H./Philipper, J. (2016).** Bargeld - abschaffen? oder erhalten! Ein Beitrag zur Diskussion um die Zukunft des Bargelds. <https://library.fes.de/pdf-files/managerkreis/12691.pdf>. abgerufen am 10.05.2021

- ntv (15.08.2021).** Kampf gegen Geldwäsche - Frankreich fordert neues Bargeld-Limit.
<https://www.n-tv.de/wirtschaft/Frankreich-fordert-neues-Bargeld-Limit-article22743789.html>. abgerufen am 15.08.2021
- ntv (15.02.2022).** Auch staatliche Banken betroffen - Kiew meldet Cyberattacke auf
 Ministerium. <https://www.n-tv.de/politik/Kiew-meldet-Cyberattacke-auf-Ministerium-article23129914.html>. abgerufen am 16.02.2022
- Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) (o.D.).** What
 is the CRS? . <https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/>.
 abgerufen am 05.01.2021
- Oser, J. (2021).** Wenn sich Polizisten Daten erschleichen. Süddeutsche Zeitung:online,
 21.02.2021. <https://www.sueddeutsche.de/bayern/bayern-polizisten-daten-abfrage-gruene-1.5212617>. abgerufen am 20.12.2021
- Oxford Committee for Famine Relief (OXFAM) (Oxforder Komitee zur Linderung von
 Hungersnot).** EU tax haven blacklist review - Oxfam analysis and background.
 05.02.2021. <https://oxfam.app.box.com/v/2021EUTaxHavensBrief>. abgerufen am
 30.04.2021
- Pahl, H. (2017).** Niklas Luhmann: Die Wirtschaft der Gesellschaft. In: Kraemer, K./ Brugger,
 F. (eds). Schlüsselwerke der Wirtschaftssoziologie. Wirtschaft + Gesellschaft. Springer
 VS, Wiesbaden. https://doi.org/10.1007/978-3-658-08184-3_18. abgerufen am 25.11.2021
- Pawlik, J. (2018).** Kryptocoin Diebstähle. Seminar Innovative Internet-Technologien und
 Mobilkommunikation. Lehrstuhl für Netzarchitekturen und Netzdienste . Fakultät für
 Informatik, Technische Universität München. doi: 10.2313/NET-2018-03-1_06.
https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2018-03-1/NET-2018-03-1_06.pdf.
 abgerufen am 19.05.2021
- Peters, M./Senn, M. (2021).** Der Finanzsektor ist zu groß - Warum ein aufgeblähter
 Finanzsektor der europäischen Wirtschaft und Gesellschaft schadet. Finanzwende
 Recherche. Berlin. Dezember 2021. [https://www.finanzwende-recherche.de/wp-
 content/uploads/2021/12/Report_Der-Finanzsektor-ist-zu-gross.pdf](https://www.finanzwende-recherche.de/wp-content/uploads/2021/12/Report_Der-Finanzsektor-ist-zu-gross.pdf). aberufen am
 27.01.2022
- President's Global Development Council (2015).** A call to action on financial inclusion. Kon-
 ferenzpapier des G20-Treffen 15.-16.11.2015. Belek-Antalya (Türkei).
[https://www.usaid.gov/sites/default/files/documents/9276/GDCRecommendationsOnFi-
 nancialInclusion11_2015.pdf](https://www.usaid.gov/sites/default/files/documents/9276/GDCRecommendationsOnFinancialInclusion11_2015.pdf). abgerufen am 23.01.2022

- Redaktion beck-aktuell (2020).** Bundesregierung will Kampf gegen Geldwäsche weiter verstärken. beck-aktuell:online. 20.01.2020.
<https://rsw.beck.de/aktuell/daily/meldung/detail/bundesregierung-will-kampf-gegen-geldwaesche-weiter-verstaerken>. abgerufen am 11.08.2021
- Rentzsch, F. (2017).** In Dänemark zeigt sich, was passiert, wenn der Immobilienmarkt außer Kontrolle gerät. Business Insider:online, 30.06.2017.
<https://www.businessinsider.de/wirtschaft/nullzinspolitik-daenischer-immobilienmarkt-geraet-ausser-kontrolle-2017-6/>. abgerufen am 17.05.2021
- Rieger, F. (2018).** Einführung einer Obergrenze für Bargeldtransaktionen – Rechtliche Grenzen und die Perspektive der Praxis. In: Lempp, J./Pitz, T./Sickmann J. (eds). Die Zukunft des Bargelds. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-21720-4_3. abgerufen am 10.05.2021
- Rogoff, K. S. (2016).** Der Fluch des Geldes - Warum unser Bargeld verschwinden wird. FinanzBuch Verlag München. ISBN 978-3-86248-882-7
- Rogoff, K.S. (2021).** Bitcoin - Ein Fluch schlimmer als Bargeld. Gastkommentar in Börse Online, 08.07.2021. <https://www.boerse-online.de/nachrichten/aktien/kenneth-rogoff-bitcoin-ein-fluch-schlimmer-als-bargeld-1030572202>. abgerufen am 10.09.2021
- Rohrbeck, F./Saleswski, C./Schröm, O. (2017).** Der doppelte Kubicki. Zeit Online, 16.11.2017. <https://www.zeit.de/2017/47/wofgang-kubicki-finanzminister-cum-ex-kritik>. abgerufen am 11.01.2022
- Salewski, C./Schröm, O., Strunz, B. (2020).** Hamburg verzichtet auf 47 Millionen Euro. tagesschau:online, 13.02.2020. <https://www.tagesschau.de/investigativ/panorama/cum-ex-skandal-warburg-bank-101.html>. abgerufen am 11.01.2022
- Sauerland, M./ Höhs, J. (2019):** Geld - Vom Sein zum Schein. Springer Fachmedien Wiesbaden, 2019, <https://doi.org/10.1007/978-3-658-26666-0>. abgerufen am 24.06.2021
- Schiller, K. (2019).** Was ist Blockchain? - Einfach und verständlich erklärt. Blockchainwelt. 27.01.2019. <https://blockchainwelt.de/blockchain-was-ist-das/>. abgerufen am 12.11.2021
- Schmidt, A. (2022).** Die Bargeldentwicklung in Berlin, Brandenburg und Mecklenburg-Vorpommern anhand von Zählraten der WSN Sicherheit und Service GmbH in den Jahren 2012 bis 2021. Internes Dokument der WSN Sicherheit und Service GmbH. 10.01.2022

- Schneider, F. (2009).** Die Finanzströme von organisierter Kriminalität und Terrorismus: Was wissen wir (nicht)?. *Vierteljahrshefte zur Wirtschaftsforschung*, vol. 78, no. 4, Duncker & Humblot GmbH, Oct. 2009, pp. 73–87, doi:10.3790/vjh.78.4.73. <http://ejournals.duncker-humblot.de/doi/abs/10.3790/vjh.78.4.73>. abgerufen am 05.07.2021
- Schneider, F. (2016).** Der Umfang der Geldwäsche in Deutschland und weltweit - einige Fakten und eine kritische Auseinandersetzung mit der Dunkelfeldstudie von Kai Bussmann. Sept. 2016, <https://geldwaesche-beauftragte.de/wp-content/uploads/2017/04/Der-Umfang-der-Geldwaesche-in-Deutschland-und-weltweit-Friedrich-Naumann-Stiftung.pdf>. abgerufen am 18.05.2021
- Schneider, F. (2017a).** Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism?. International Cash Conference 2017 - War on Cash: Is there a Future for Cash? 25 - 27 April 2017. Island of Mainau, Germany. Deutsche Bundesbank, Frankfurt am Main. <https://www.econstor.eu/bitstream/10419/162914/1/Schneider.pdf>. abgerufen am 05.07.2021
- Schneider, F. (2017b).** Schattenwirtschaft: Ursachen statt Bargeld bekämpfen. In: *Die Volkswirtschaft*, no. 8–9, 2017, pp. 21–24. https://stage.dievolkswirtschaft.ch/content/uploads/2017/07/09_Schneider_DE.pdf abgerufen am 30.06.2021
- Schwartz, M./Dapp, T.F./Beck, G.W./Khussainova, A. (2017).** Deutschlands Banken schalten bei Filialschließungen einen Gang höher - Herkulesaufgabe Digitalisierung. Fokus Volkswirtschaft Nr. 181, 08.10.2017, KfW Research. <https://www.kfw.de/Über-die-KfW/Service/Download-Center/Konzernthemen/Research/Fokus-Volkswirtschaft/>. abgerufen am 28.01.2022
- Schweigert, T. (2021a).** Offshore Konto eröffnen. <https://schweigertconsulting.com/offshore-konto-eroeffnen>. abgerufen am 02.01.2022
- Schweigert, T. (2021b).** Offshore Firma. <https://schweigertconsulting.com/offshore-firma/>. abgerufen am 02.01.2022
- Seibel, K. (2022).** Konten, Depots, Schließfächer – Finanzämter sind so neugierig wie nie. Welt:Online, 21.01.2022. <https://www.welt.de/wirtschaft/article236371973/Konten-Depots-Schliessfaecher-Finanzaeemter-sind-so-neugierig-wie-nie.html>. abgerufen am 21.01.2022

- Siller, M./Schrag, M./Althammer, P. et al. (2021).** Wirecard: Chronologie eines Finanzskandals. BR24:online, 20.04.2021.
<https://www.br.de/nachrichten/wirtschaft/aufstieg-und-fall-die-chronologie-zum-wirecard-fall,SCku91R>. abgerufen am 09.01.2022
- Sinn, H.-W. (2021).** Die wundersame Geldvermehrung - Staatsverschuldung, Negativzinsen, Inflation. Verlag Herder GmbH, Freiburg im Breisgau 2021. ISBN 978-3-451-82580-4
- Stirnemann, S. (2018).** Grundlagen und Theorie – eine Einführung. In: Der Mensch als Risikofaktor bei Wirtschaftskriminalität. Springer Gabler, Wiesbaden.
https://doi.org/10.1007/978-3-658-20813-4_1. abgerufen am 19.05.2021
- SophosLabs/Sophos Managed Threat Response/Sophos Raid Response/SophosAI (2021).** Sophos 2022 Threat Report - Interrelated threats target an interdependent world. Abingdon (UK). <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2022-threat-report.pdf>. abgerufen am 06.12.2021
- Soska, K. / Christin, N. (2015).** Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. Proceedings of the 24th USENIX Security Symposium. 12-14.08.2015. Washington D.C.. S. 33-48. ISBN 978-1-939133-11-3.
<https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska>. abgerufen am 07.12.2021
- Stede, C. / BTC-Echo (2021).** 69.000 BTC weg - AfriCrypt wird milliardenschwerer Exit-Scam vorgeworfen. BTC-Echo:online, 24.06.2021.
<https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska>. abgerufen am 08.09.2021
- Steinmann, T. (2020a).** Wie die Ermittler die Wirecard-Chefs vom Haken ließen. Capital:online, 18.11.2020. https://www.capital.de/wirtschaft-politik/erste-razzia-bei-wirecard-schon-lange-vor-der-pleite?article_onepage=true. abgerufen am 09.01.2022
- Steinmann, T. (2020b).** BaFin machten mehr Wirecard-Geschäfte als bekannt. Capital:online, 08.10.2020. <https://www.capital.de/wirtschaft-politik/staatsanwaelte-ermittelten-schon-frueh-gegen-wirecard>. abgerufen am 09.01.2022
- Steinmann, T. (2020c).** Staatsanwälte ermittelten schon früh gegen Wirecard. Capital:online, 03.11.2020. <https://www.capital.de/wirtschaft-politik/bafin-mitarbeiter-machten-mehr-wirecard-geschaefte-als-bekannt>. abgerufen am 09.01.2022

- Svensson, M. (2021).** Dirty Money Exploits Weakness to Enter : A Narrative Literature Review on the Challenges of Combatting Money Laundering (Dissertation).
<http://urn.kb.se/resolve?urn=urn:nbn:se:mau:diva-44818>. abgerufen am 24.08.2021
- Sveriges Riksbank (2019).** Payments in Sweden 2019. Stockholm.
<https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-in-sweden-2019/>. abgerufen am 06.07.2021
- tagesschau (2021).** Bargeldobergrenze gegen Geldwäsche. tagesschau:online, 20.07.2021.
<https://www.tagesschau.de/wirtschaft/verbraucher/bargeld-obergrenze-bargeldobergrenze-geldwaesche-eu-kommission-101.html>. abgerufen am 11.08.2021
- Tagesspiegel (2021).** Viel Wirbel um Mails von Scholz' Privataccount. Tagesspiegel:online, 22.04.2021. <https://www.tagesspiegel.de/politik/untersuchungsausschuss-zum-wirecard-skandal-viel-wirbel-um-mails-von-scholz-privataccount/27121956.html>. abgerufen am 09.01.2022
- Tax Justice Network (2020a).** Financial Secrecy Index - 2020 Results.
<https://fsi.taxjustice.net/en/introduction/fsi-results>. abgerufen am 05.01.2022
- Tax Justice Network (2020b).** Financial Secrecy Index 2020 - Narrative Report on United States of America. <https://fsi.taxjustice.net/PDF/UnitedStates.pdf>. abgerufen am 05.01.2022
- Thiele, C.-L. (2017).** Bargeld hat Zukunft! - Vielfältige Vorteile von Noten und Münzen für eine Zukunft von Bargeld. *Der Bank Blog*, 10 May 2017. <https://www.der-bank-blog.de/bargeld-hat-zukunft/trends/26648/>. abgerufen am 29.06.2021
- Thiele, C.-L./Niepelt, D./Krüger, M. (2015).** Diskussion um das Bargeld: Hätte eine Abschaffung von Banknoten und Münzen wirklich Vorteile? . In: *Ifo Schnelldienst*, vol. 68, no. 13, 2015, pp. 3–18, <https://www.ifo.de/publikationen/2015/aufsatz-zeitschrift/diskussion-um-das-bargeld-haette-eine-abschaffung-von>. abgerufen am 15.07.2021
- Thiele, S. (2017).** *Dirty Money – Wie schmutzig ist unser Geld?* | *Mikrobenzirkus*, 23.10.2017, <https://mikrobenzirkus.com/2017/10/23/dirty-money-wie-schmutzig-ist-unser-geld/>. abgerufen am 17.07.2021
- Thielmann, M. (2021).** Die größten Cyberangriffe - Ein kurzer Rückblick auf 2021. DsiN-Blog - Der IT Sicherheitsblog für den Mittelstand. <https://www.dsin-blog.de/2021/08/04/die-groessten-cyberangriffe-ein-kurzer-rueckblick-auf-2021/>. abgerufen am 03.12.2021

- Transparency International Duetschland (2021).** Geldwäschebekämpfung in Deutschland - Problem, Lösungsvorschläge und Beispielsfälle.
https://www.transparency.de/fileadmin/Redaktion/Publikationen/2021/Studie_Geldwa__sc he-in-Deutschland_210706.pdf. abgerufen am 06.10.2021
- Tzanetakis, M. (2019).** Digitalisierung von illegalen Märkten. In: Feustel, R./ Schmidt-Semisch, H./ Bröckling U. (eds). Handbuch Drogen in sozial- und kulturwissenschaftlicher Perspektive. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-22138-6_33. abgerufen am 10.05.2021
- van Wegberg, R./Oerlemans, J.-J./van Deventer, O. (2018).** Bitcoin money laundering: mixed results? - An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, Vol. 25 No. 2, pp. 419-435.
<https://doi.org/10.1108/JFC-11-2016-0067>. abgerufen am 01.09.2021
- Verbraucherzentrale Bundesverband (2021).** Bargeld - Verfügbarkeit und Nutzung - Befragungen aus Dezember 2019 und Oktober 2021. Verbraucherzentrale Bundesverband e.V., 23.12.2021. https://www.vzbv.de/sites/default/files/2021-12/2021-12-03_Chartbericht%20Bargeld_3.0.pdf. abgerufen am 28.01.2022
- Verbraucherzentrale Bundesverband (2022).** Weiteres Gericht kippt Verwahrenngelte auf Girokonten - vzbv klagt erfolgreich gegen Preisklausel der Volksbank Rhein-Lippe. Verbraucherzentrale Bundesverband e.V., 26.01.2022. <https://www.vzbv.de/urteile/weiteres-gericht-kippt-verwahrenngelte-auf-girokonten>. abgerufen am 30.01.2022
- Vriesekoop, F./Russel C./Alvarez-Mayorga, B. et al. (2010).** Dirty money: an investigation into the hygiene status of some of the world's currencies as obtained from food outlets. *Foodborne Pathog Dis.* 2010 Dec; 7(12):1497-502. doi: 10.1089/fpd.2010.0606. Epub 2010 Aug 12. PMID: 20704502. <https://pubmed.ncbi.nlm.nih.gov/20704502/>. abgerufen am 17.07.2021
- Wahlers, K. (2013).** Das Hawala-Finanzsystem. In: Die rechtliche und ökonomische Struktur von Zahlungssystemen inner- und außerhalb des Bankensystems. Bibliothek des Bank- und Kapitalmarktrechts, vol 2. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37390-9_5. abgerufen am 21.07.2021
- Waidmann, L. (2021).** Die Top 5 Privacy-Kryptowährungen, die man kennen muss. *BTC-Echo:online*, 20.02.2021. <https://www.btc-echo.de/news/die-top-5-privacy-kryptowaehrungen-die-man-kennen-muss-112235/>. abgerufen am 08.12.2021

- Warneke, M. (2021).** Rundschreiben Nr. 4/2021 Steuerzahlergedenktag und Einkommensbelastungsquote 2021. 13 July 2021, https://www.steuerzahler.de/fileadmin/user_upload/DSi_Schriften/DSi_Rundschreiben/RS_04-2021_Steuerzahlergedenktag.pdf. abgerufen am 24.07.2021
- Wohlmann, M. (2020).** Kryptowährungen – Top oder Flop?. In: Rebeggiani/Wilke/Wohlmann. Megatrends aus Sicht der Volkswirtschaftslehre. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-30129-3_16. abgerufen am 10.05.2021
- World Economic Forum (o.D.).** Our Partners. <https://www.weforum.org/partners#search>. abgerufen am 02.02.2022
- World Economic Forum (2018).** The Known Traveller - Unlocking the potential of digital identity for secure and seamless travel. Januar 2018. Genf (CH). <https://cn.weforum.org/reports/the-known-traveller-unlocking-the-potential-of-digital-identity-for-secure-and-seamless-travel>. abgerufen am 16.01.2022
- World Health Organization (2020).** World Health Organization (WHO) Western Pacific auf Twitter: "FACT: The risk of being infected with the new #coronavirus by touching coins, banknotes, credit cards and other objects, is very low". <https://t.co/BOuqHUDjwL> #COVID19 #KnowtheFacts <https://t.co/>. <https://twitter.com/WHOWPRO/status/1229947064093593600/photo/1>. abgerufen am 19.05.2021
- Zeit Online (2021).** Cyberkriminalität - Verdachtsfälle von Geldwäsche mit Kryptowährungen nehmen stark zu. Zeit:Online, 02.09.2021. <https://www.zeit.de/wirtschaft/2021-09/geldwaesche-kryptowaehrungen-zunahme-cyberkriminalitaet-europa>. abgerufen am 24.12.2021
- Zitlmann, R. (2017).** Psychologie der Superreichen: Das verborgene Wissen der Vermögenselite. FinanzBuch Verlag. https://www.buecher.de/shop/werbung/psychologie-der-superreichen-ebook-pdf/zitlmann-rainer/products_products/detail/prod_id/47038099/. abgerufen am 27.07.2021

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt.

Alexander Schmidt, Neverin, 22.02.2022