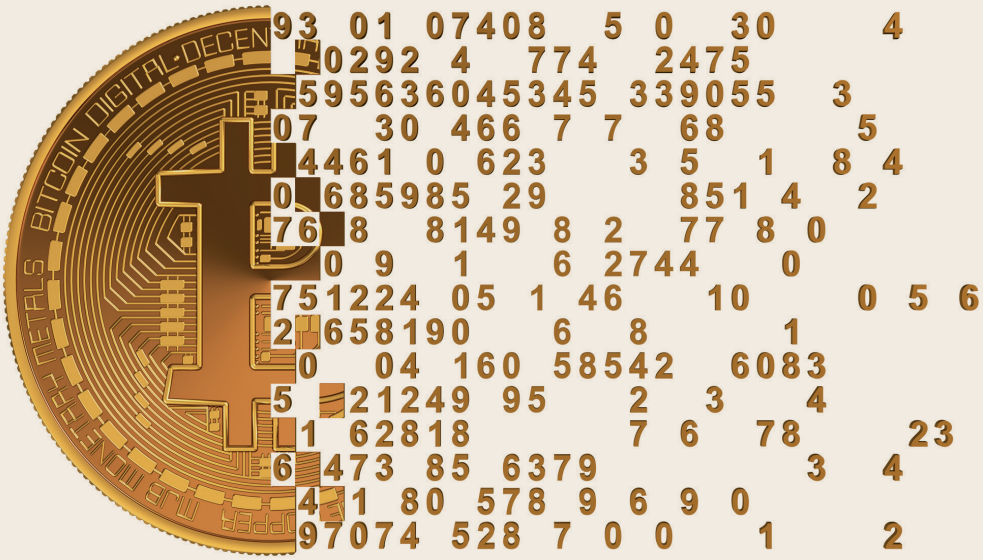
Dietmar Knapp



LEITFADEN

Kryptowährungen und ihre steuerlichen Auswirkungen

inkl technische, betriebswirtschaftliche und zivilrechtliche Aspekte

dbv

Autor:

Dietmar Knapp, MSc

Der Autor ist aufgrund seiner nationalen Berufsberechtigung auch in der Wirtschafts- und Steuerberatung für eine ausländische Kanzlei tätig. Aufgrund dieses Betätigungsfeldes konnte er sich ein fundiertes Wissen insbesondere im Bereich der Kryptowährungen aneignen.

1. Auflage
Juni 2018

ISBN: 978-3-7041-0710-7 (Print)
978-3-7041-2098-4 (E-Book)

dbv-Verlag – Fachverlag für Steuer- und Wirtschaftsrecht
8010 Graz, Geidorfgürtel 24, Tel (0316) 38 30 33; Fax (0316) 38 30 43
1070 Wien, Seidengasse 9, Tel (01) 796 35 62-24, Fax (01) 796 35 62-25
Internet: www.dbv.at, email: office@dbv.at

Copyright © 2018 by dbv-Verlag Graz, Wien

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sind vorbehalten.

Kein Teil des Werkes darf in irgendeiner Form ohne schriftliche Genehmigung des Verlages reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, wie zB Künstler/in, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Alle Angaben und externen Verlinkungen in diesem Buch erfolgen ohne Gewähr, eine Haftung des Autors und des Verlages ist ausgeschlossen. Stand der externen Verlinkungen: 27.6.2018

Druck und Herstellung
dbv-Druck-, Beratungs- und Verlagsgesellschaft mbH, Graz

Vorwort

Geld als Tausch- und Zahlungsmittel, Wertmesser und Recheneinheit, Wertaufbewahrungs- und Wertübertragungsmittel hat in den letzten Jahren durch unterschiedliche Umstände massiv an Vertrauen verloren. Viele Menschen glauben nicht mehr an den Wert des Geldes und befürchten, dass wieder Zeiten heranwachsen könnten, wo durch Hyperinflation die monetäre Kaufkraft rapide schwindet und Heere von Arbeitslosen den sozialen Frieden bedrohen könnten. Alles Fakten, die nicht ohne weiteres von der Hand zu weisen sind.

Inwiefern sich Kryptowährungen (Bitcoins & Co) als eine seriöse Alternative zu den bestehenden Geld- und Wertsystemen entwickeln könnten, lässt sich derzeit noch trefflich streiten. Die Volatilität, die im Moment die Charts von Bitcoin & Co wiederspiegeln, bürgen auch nicht gerade für jene Stabilität bzw Werterhaltung und bleiben das Vertrauen schuldig, das sich „Otto“ Normalverbraucher wünschen würde.

Was nun allein die Sicherheitsmerkmale einer Blockchain betrifft, ist diese Datenplattform viel weniger missbrauchsanfällig als die vergleichbaren Softwaresysteme vieler Banken. Es ist nicht ausgeschlossen bzw ist es denk- und nachvollziehbar, dass die heutigen Geld- und Wertetransfer-Systeme aus vorgenannten Gründen, durch andere – vor allem durch ein System, das mehr Vertrauen, mehr Sicherheit und Stabilität garantiert, also Mehrwerte für das gesamte Benutzerfeld (zB Bretton Woods System) generiert – ersetzt werden.

Jedenfalls kennzeichnen die Attribute einer Blockchain, wie **Vertrauen** (ohne zentralen Garanten), **Sicherheit** (Integrität/Missbrauchsschutz), **Transaktionsfähigkeit** (automatisiert), **Nachvollziehbarkeit** (Fälschungssicherheit) und **Auffindbarkeit** (Matching) Merkmale, die das Stärkenprofil dieser Softwaretechnik zum Vorschein bringt.

Dass sich auf Basis einer Blockchain-Technologie noch eine Vielzahl von anderen Datenverarbeitungs-Optionen ergeben (bspw Verrechnungs-, Buchhaltungs- und Personalverrechnungssysteme), steigert die Anwendungsbreite dieses Werkzeuges ganz erheblich. Speziell für Rechnungswesenberufe ergeben sich dadurch völlig neue Marktperspektiven/Weiterentwicklungschancen und für deren Zielgruppen ein wahres Füllhorn an neuen IT-Lösungsoptionen, mit den Vorzügen der Blockchaintechnik.

KR Mag Hans Kraft, MSc, MBA, CMC — Graz, im Juni 2018

Inhaltsverzeichnis

Seite

Vorwort 3

Kapitel 1 Einleitung

1.1 Einstiegsszenario: Blackout ... 9
1.2 Digitalisierung von Geld und Märkten ... 11
1.3 Zeit als Währung in der Zukunft ... 17

Kapitel 2 Technische Aspekte

2.1 Einführung in die Kryptografie ... 23
2.1.1 Geheimhaltung ... 24
2.1.2 Authentizität und Integrität ... 24
2.2 Transaktionslegitimität versus Transaktionskonsens ... 25
2.3 Kryptowährungsnutzung und Anonymität ... 31
2.4 Mining als Schöpfungsakt der Kryptowährung ... 32
2.5 Chancen und Risiken von Kryptowährungen ... 36

Kapitel 3 Volkswirtschaftliche Aspekte

3.1 Klassische Geldwirtschaft ... 44
3.1.1 Kryptowährischer Geldwirtschaftsansatz ... 49
3.2 Digitale Zahlungssysteme im Kontext mit Leistungsaustauschprozessen ... 51
3.3 Kryptowährung als quasi-anerkanntes Zahlungsmittel ... 55
3.3.1 Innovative Entwicklungen rund um die Blockchain-Technik ... 58

Kapitel 4 Mikroökonomische Aspekte in Bezug auf Kryptowährungen

4.1 Spieltheoretischer Ansatz ... 64

Kapitel 5 Betriebswirtschaftliche Aspekte

5.1 Buchhalterische Herausforderungen im Zusammenhang mit Kryptowährungen ... 74
5.1.1 Allgemeines zur Buchführung versus Kryptowährungen ... 74

Seite

5.1.2 Verbuchung von Kryptowährungen 76
5.1.3 Skontoverbuchung 86
5.1.4 Anzahlungsproblematik 88
5.1.5 Tauschproblematik 89
5.1.6 Privatbuchungen 90
5.1.7 Gebührenproblematik 92
5.1.8 Wechselproblematik 92
5.1.9 Arbeitsentgeltsproblematik 95
5.1.10 Freier Dienstnehmer 95
5.1.11 Forderungsausfall-Problematik 97
5.1.12 Crowdfunding 98
5.1.13 Bilanzierung von Kryptowährungen 98
5.1.13.1 Kostenrechnerische Ansätze für Kalkulationen mit Kryptowährungen . 100
5.1.13.2 Kennzahlenbezogene Überlegungen im Zusammenhang mit Kryptowährungen 101
5.1.13.3 Controlling-Prozessanpassung im Kontext mit Kryptowährungen 102
5.1.13.4 Strategische Unternehmensüberlegungen rund um Kryptowährungen 103
5.1.13.5 Risikomanagement 104

Kapitel 6 Rechtliche Aspekte

6.1 Unionsrechtliche Aspekte im Zusammenhang mit dem Euro als gesetzliches Zahlungsmittel 107
6.2 Verfassungsrechtliche Aspekte im Zusammenhang mit Kryptowährungen ... 108
6.3 Strafrechtliche Aspekte zum Institut der Kryptowährungen 112
6.3.1 Betrugstatbestand gem § 146 StG 114
6.3.2 Urkundenfälschung gem § 223 StGB 115
6.3.3 Verfälschung besonders geschützter Urkunden gem § 237 StGB 117
6.3.4 Betrügerischer Datenmissbrauch gem § 148a StGB 117
6.3.5 Widerrechtlicher Zugriff auf ein Computersystem gem § 118a StGB 118
6.3.6 Verletzung des Telekommunikationsgeheimnisses gem § 119 StGB 118
6.3.7 Ketten- oder Pyramidenspiel gem § 168a StGB 119
6.3.8 Geldwäscherei gem § 165 StGB 120
6.3.9 Weitere Delikte des Strafgesetzbuches im Kontext mit Kryptowährungen 122

Seite

6.4 Finanzmarktaufsichtliche Aspekte im Spannungsfeld rund um Kryptowährungen ... 123
6.5 Zivilrechtliche Annahme einer Sache ... 126
6.6 Zivilrechtliche Annahme der Kryptowährung als immaterielles Recht ... 129
6.7 Rechtsgeschäfte in Kryptowährungen und ihre zivilrechtliche Zulässigkeit ... 131
6.8 Rechtsvergleiche mit der deutschen Rechtsordnung ... 137

Kapitel 7 Steuerliche Aspekte

7.1 Formalrechtliche Einordnung der Kryptowährung ... 140
7.2 Umsatzsteuerrechtliche Aspekte ... 141
7.2.1 Rechtsgrundlagenabgrenzung im Zusammenhang mit Kryptowährungen ... 141
7.2.2 Leistungsaustausch in und durch Kryptowährungen ... 143
7.2.3 Vorsteuerabzugsoptionen im Zusammenhang mit Kryptowährungen ... 146
7.2.4 Weiterführende umsatzsteuerrechtliche Aspekte im Zusammenhang mit Kryptowährungen ... 153
7.3 Ertragssteuerliche Aspekte ... 160
7.3.1 Einkünfte aus Spekulationsgeschäften gem § 31 EStG ... 162
7.3.2 Kryptowährung als Betriebsvermögen ... 167
7.3.3 Einkünfte aus Gewerbebetrieb gem § 23 EStG ... 169
7.3.4 Gewinnermittlung im betrieblichen Bereich ... 174
7.3.4.1 Pauschalierung gem § 17 EStG ... 174
7.3.4.2 Einnahmen-Ausgaben-Rechnung ... 177
7.3.4.3 Doppelte Buchhaltung nach Steuerrecht ... 180
7.3.4.4 Doppelte Buchhaltung nach Unternehmensrecht ... 183
7.3.4.5 Internationale Rechnungslegung ... 184
7.3.4.5.1 Bilanzielle Darstellung ... 188
7.3.4.5.2 Cash flow-Statement ... 189

Anhang

Abkürzungsverzeichnis ... 191
Glossarium ... 194
Quellenverzeichnis ... 206
Stichwortverzeichnis ... 209

Kapitel 1
Einleitung

Die Globalisierung der Märkte ist eine Tatsache. Es ist daher wenig verwunderlich, dass auch die damit verbundenen Transaktionen ein größeres Volumen annehmen. Das Geld der Investoren und Unternehmen kennt keine Grenzen. Es bewegt sich von einem Bankkonto zum anderen – meist digital, ohne real jemals in Erscheinung zu treten. Durch dieses Giralgeld können große Mengen an Geld weltweit rasch bewegt werden – die gesetzlichen Rahmenbedingungen für Investoren und Banken werden jährlich aufgrund der politischen Besorgnis rund um etwaige Terrorismusfinanzierungen strenger. Der **Homo oeconomicus** als rationaler Agent wird zum repräsentativen Nutzenmaximierer in der Spieltheorie rund um die Märkte. Diese Person fällt seine Entscheidungen aufgrund der Analysen zu den (neo-)klassischen Wirtschaftstheorien; es gilt für ihn das absolute Rationalprinzip. Im globalen Wettbewerb gilt dies auch für das klassische Geldsystem, um diesen staatlichen Regularien teilweise zu entkommen. Es wird nach einer lukrativen Alternative gesucht. Eine Option hierfür ist die Kryptowährung.

1.1 Einstiegsszenario: Blackout

„Stell dir vor, es geht das Licht aus, sag was würdest du dann tun … finster, finster!“

– Hans Lang/Erich Meder

Ein flächendeckendes Blackout als kompletter Stromausfall auf einem ganzen Kontinent – entweder ausgelöst durch eine Naturkatastrophe oder, perfider noch, durch einen Terroranschlag – wurde bisher in seiner Endkonsequenz nur bedingt von den öffentlichen Stellen oder wissenschaftlichen Institutionen untersucht. Niemand kann konkret die Folgen aus einem solchen massiven Störfall abschätzen, da die Kraftwerksbetreiber in Anbetracht des **Share-value-Drucks** nur bedingt ein Notsystem für ein paar Tage eingerichtet haben. Auch die öffentliche Hand, mit ihrem Auftrag zum Schutz der Gesundheit und des Lebens der Bevölkerung, verfügen bloß über Notfallsysteme, die zeitlich begrenzt nutzbar sind, da davon ausgegangen wird, dass allfällige Stromausfälle innerhalb weniger Stunden wieder behoben werden können. Deshalb sehen Unternehmen selbst nur eine rudimentäre oder keine Vorsorge für diesen Fall vor. Die Konsequenz besteht darin, dass die öffentliche Ordnung und das soziale Gefüge innerhalb kurzer Zeit zusammenbrechen – nichts geht mehr!

Ein solches Szenario ist möglich; weil ein großer Teil unserer Energieversorgung vom Strom abhängig ist, wobei die operativen Steuerungssysteme selbst – siehe bspw die angebotenen *Supervisory Control & Data Acquisition Systems (SCADA)* – in ihrer komplexen Konzeption anfällig sind. Es ist kein **ADV-System** sicher; das ist Tatsache. Ein ADV-System ist eine Abfolge von Prozessen, die teils auf elektronischen und teils auf operativen Arbeitsanweisungen basieren. Immer mehr elektronische Produkte helfen uns den Alltag zu meistern, ohne dass wir bedenken, dass diese

Geräte für ihr Funktionieren Strom benötigen – denken wir an das Mobiltelefon, den Computer, die Waschmaschine, den Kühlschrank etc; alles braucht Strom. Ohne elektronische Haushaltsgeräte ist das tägliche Leben äußerst mühsam – kein Wasser fließt, kein Licht geht an, keine Klospülung funktioniert mehr. Mit dem Ausfall vieler elektronischer Kommunikationsgeräte kann kaum mehr auf den eigenen Datenbestand – egal, wo er gesichert ist – zugegriffen werden.

Informationen und Daten bestimmen bereits heute unser Leben wesentlich, da sowohl wirtschaftliche als auch persönliche Entscheidungen oft auf dem schnellen Informationsrückgriff im **World Wide Web** beruhen. Weil bestimmte Ereignisse in der Öffentlichkeit der realen Welt oder im Internet des virtuellen Raums bekannt werden, können aus dieser gefilterten Informationsmenge jene Entscheidungen getroffen werden, die einem hoffen lassen, das Richtige getan zu haben. In diesem Zusammenhang gilt es festzuhalten, dass die Information aufgrund des Internets grundsätzlich mit einem Wert von Null anzunehmen ist, weshalb die monetäre Wirkung wegen der (fast) freien Zugänglichkeit entsprechend einzuschätzen ist.

Das menschliche Zusammenleben wird durch das gesatzte Rechtsgefüge in seiner Ordnung bestimmt; hingegen muss das Internet als rechtsloser – also anarchistischer – Raum angesehen werden, zumal für die virtuelle Welt noch keine Rechtsordnung beschlossen wurde.

Wenn nichts mehr geht, geht alles – aufgrund einer globalen Katastrophe, gleich welchen Ursprungs – können die aufgebauten Strukturen zusammenbrechen, weshalb diese kaum mehr genutzt werden. Die öffentliche Sicherheit kann nicht mehr aufrechterhalten werden, sodass es zu einer Rückbesinnung zu den naturrechtlich akzentuierten Werten auf Basis der Ethik als wissenschaftlich-theoretische Reflexion über das gedeihliche Zusammenleben und das sittlich richtige Verhalten und die Moral als von der Gesamtheit einer Gruppe verinnerlichten Verhaltensregeln in Anwendung der ethischen Grundsätze kommt. Demgegenüber stehen Partikularinteressen einzelner Behörden, Firmen und schließlich auch Personen, da in der Krise diese Kreise ihren schnellen Vorteil zum Schaden des anderen suchen. So werden einfache handwerkliche Tätigkeiten für das Überleben wichtig, weshalb gerade in einer solchen Phase der Tausch als komplementäres Wirtschaftssystem an Bedeutung gewinnt. Als Währung wird die Zeit vereinbart, um seine Grundbedürfnisse sichern zu können. Das Gemeinsame wird über das Trennende gestellt, obwohl es auch Menschen geben wird, die diese Situation auszunutzen versuchen – entweder durch kriminelle Machenschaften oder (vorsätzlicher) Ausbeutung und/oder Benachteiligung anderer Menschen.

Für Kryptowährungen als eine im virtuellen Raum erzeugte und dort auch gehandelte Währung bedeutet ein Blackout eine absolute Instabilität. Weder ein Bestand noch ein Kurs, der sich aufgrund des Prinzips von Angebot und Nachfrage ergibt, ist und/oder bleibt nachverfolgbar, sodass es in einem solchen Extremfall zu einem gewichtigen Vertrauensverlust kommt, der eine Hyperinflation auslösen kann. Mit dem Verfall dieser nur im virtuellen Raum existierenden Werte, die von keinem realen Bankensystem hinterlegt sind, ist eine totale Auflösung dieser Währungsblase denkbar.

1.2 Digitalisierung von Geld und Märkten

Viele Jahre war Geld etwas Greifbares – das klassische Zug-um-Zug-Geschäft: Hier Ware, da Bargeld, verliert mit zunehmender Vernetzung der Wirtschaft an Bedeutung, weil Banknoten im größeren Umfang schwer und teuer in der Herstellung sind. Einfacher werden wirtschaftliche Transaktionen durch die Möglichkeit der Verbuchung von Buchgeld vollzogen. Durch eine simple Umbuchung von einem Bankkonto auf das andere werden monetäre Werte verschoben, ohne dass es zu einem realen Geldfluss kommt. Nur das reale Bargeld ist bei einem globalen Blackout existent und digitale Transaktionssysteme werden aufgrund der Unbenützbarkeit praktisch wertlos.

Damit dieses Transaktionssystem funktioniert, bedarf es des Vertrauens zu diesem Algorithmus. Begonnen hat es damit, dass reiche Menschen bargeldlos – nur ausgestattet mit einer Kreditkarte – die Welt bereisten. Das reale Vermögen wurde in einer Bank hinterlegt, und die reisende Person hatte bald weltweit Zugriff auf ihr Vermögen, indem für die Bezahlung von Waren und Dienstleistungen eine Abbuchung mittels Kreditkarte erfolgte. Anfangs wurden diese Transaktionen entweder per Scheckeinlösung oder mittels Telegrafenanweisungen direkt ans Kreditkartenunternehmen buchhalterisch dargestellt.

Heutzutage wird versucht, Zahlungen (wie etwa von *Square* verfolgt) über das Mobiltelefon rasch und digital abzuwickeln. Durch den Download einer App kann diese Bezahltechnik einfach benutzt werden – keine Geldbörse mehr, kein Geld abheben mehr! Die Idee für diesen Bezahldienst entstand, nachdem eine Zahlung per Kreditkarte aufgrund der fehlenden technischen Ausstattung fehlgeschlagen war. *Jack Dorsey* und *Jim McKelvey* wollten die Kreditkartentechnologie durch Nutzung der Mobilfunktechnik optimieren – *Square* als Plattform verfolgt eine alternative Bezahlstrategie für die User im Alltag. Schnell entwickelte sich der Mitbewerb – *Google Wallet, Apple Pay* oder *Stripe*. Für die Nutzung dieser Bezahlplattformen ist die Gebührenbelastung für die Kundschaft entscheidend. Nur durch kleine oder Pauschal-Gebühren, jedenfalls billiger als die Interchange-Gebühr der Kreditkartenunternehmen, kann dieses Geschäftsmodell Erfolg haben. Und es funktioniert – wer in Schweden mit Valuten bezahlt, ist ein Außenseiter. Mit dem Smartphone, auf dem eine App installiert wurde, wird am Kiosk das Eis und beim Bäcker das Baguette digital und bargeldlos bezahlt; dank Funk-Chip entfällt auch eine lästige Unterschrift oder eine Pin-Nummer. Niemand weiß derzeit genau, was passiert, wenn großflächig Mobiltelefone per digitalem Virus gehackt werden, sodass elektronische Abbuchungen passieren, obwohl kein Grundgeschäft in der realen Welt zugrunde liegt – wer kommt für den entstandenen Schaden auf und welche rechtlichen Konsequenzen können gegen den Übeltäter ins Feld geführt werden?

Aber die Digitalisierung schreitet nicht nur in Europa fort, denn die afrikanischen Volkswirtschaften setzen ebenfalls auf diesen Trend – Mobiltelefone sichern in Flüchtlingscamps den Kontakt zur Familie. Durch die Nutzung der digitalisierten Bezahlsysteme boomt die Wirtschaft – Transaktionen per Mobiltelefone sind schnell,

sicher und kostengünstig. Beispielsweise ist das *M-Pesa*-Programm zu nennen, das von einer kenianischen Mobilfunkfirma in Kooperation mit einem Kommunikationsunternehmen entwickelt wurde, um grundlegende Funktionen des Geldtransfers abwickeln zu können. Dadurch ergab sich die Möglichkeit eines bargeldlosen Zahlungsverkehrs mittels Mobiltelefone, ohne die Notwendigkeit ein reguläres Bankkonto eröffnen zu müssen. Die Inhaber von Tankstellen, Supermärkten, Straßenkioske oder Internetcafés agieren als *M-Pesa-Agents*, bei denen Ein- und Auszahlungen von Bargeld getätigt werden können, sodass es zu Gutschriften oder Belastungen des elektronisch geführten Kontos kommt; gleichzeitig wird der Besitzer des Mobiltelefons aktuell über den Stands seines Guthabens informiert. Grundgedanke dieser Entwicklung in Afrika ist es, die Korruption in den Griff zu bekommen. Digitalisiertes Geld soll Vertrauen schaffen, um einen direkten Zugriff von Vorgesetzten oder der herrschenden Klasse zu vermeiden. Natürlich kann jedes digitale System unterwandert werden, wenn die Oberschicht die Mittelschicht erpresst oder bedroht, um die Masse der Unterschicht zu betrügen.

Digitale Bezahlmethoden basieren auf dem Vertrauen der Nutzer – der Onlinehandel war anfangs von Misstrauen und Missverständnissen geprägt. Erste Erfolge in der Schaffung eines digitalisierten Vertrauens erzielte *Ebay* als ein Unternehmen, das anfangs als **Consumer-to-Consumer**-Marktplatz mit flohmarktähnlichem Charakter agierte, um sich in der Folge zu einer **Business-to-Consumer**-Plattform zu entwickeln. Die Grundidee von *Ebay* ist, jemanden zu helfen, mit einer anderen Person Handel zu treiben – dies bedingt einen Raum des gegenseitigen Vertrauens. Um eine solche Vertrauensbasis im Online-Handel aufbauen zu können, musste ein Algorithmus entwickelt werden, der Online-Vertrauen ermöglicht. Durch das gegenseitige Bewerten von Käufer und Verkäufer entsteht Transparenz, die durch den Plattformbetreiber überwacht wird. Meistens können Anbieter mit guten Gesamtbewertungen auf dieser Online-Handelsbühne reüssieren – es wird aufgrund des von Algorithmen generierten Vertrauens Handel betrieben. Diese Computerprogramme sind von Menschenhand erdacht und geschrieben, weshalb sie weder vor Eigenmanipulationen noch von Cyberattacken Dritter sicher sind – man muss eben vertrauen!

Der nächste Entwicklungsschritt stellt die **Sharing Economy** dar, da alles in einen Markt verwandelt werden kann, sodass jede Person als (Klein-)Unternehmer tätig werden kann. Es entsteht ein **Peer-to-Peer**-Marktplatz aufgrund der mobilen Technologieplattformen und den daraus erhobenen Ortsdaten in Verbindung mit den Analysen aus den Verhaltensmustern der teilnehmenden Personen. Beispielsweise kann *Airbnb* als **Community**-Marktplatz für Buchung und Vermietung von Unterkünften genannt werden. Dieses Unternehmen verfügt über kein einziges Hotel, ist aber die größte Hotelkette, da es weltweit nicht voll ausgelasteten Wohnraum über seine Internet-Plattform anbietet.

BEISPIEL:

Aufgrund dieser Entwicklung wurde im Herbst 2017 im Steirischen Landtag als „Lex Airbnb et al“ eine Novelle zum Steiermärkischen Nächtigungs- und Ferienwohnungsabgabegesetz (StNFWAG, LGBl Nr 118/2017) beschlossen, in der nun die doppelte Meldepflicht durch Anbieter, wie bspw Airbnb, und Vermieter unter

nicht unwesentlicher Strafandrohung festgeschrieben ist. Zwecks Einhebung der Ortstaxen werden die Vermieter und ein allfällig involvierter Anbieter angehalten, die Daten der Mieter an die Gemeinde zu übermitteln. Strittig ist noch, ob die Vermittlungsplattformen selbst für die Einhebung der touristischen Gebühren zuständig sein sollen.

Das **Sharing Economy** nichts mit Teilen zu tun hat, wird von *Uber* bewiesen, da dieses Unternehmen als Dienstleister-Plattform rund um Reisen und Logistik weltweit agiert. Mitfahrgelegenheiten sollen das Verkehrsaufkommen drosseln, Zustellungen sollen mit einem Personentransport verbunden werden, wenn ein gleiches Ziel anzusteuern ist. Das Unternehmen selbst stellt gerne den Umweltaspekt seiner Aktivitäten in den Vordergrund, und es vergisst gerne die zivil- und arbeitsrechtlich ungelösten Probleme rund um die Personen, die die Fahrten durchführen.

BEISPIEL:

Ein *Uber*-Teilnehmer bucht eine Mitfahrt als Auftraggeber. Die *Uber*-Plattform als Betreiber stellt diese Information allfälligen *Uber*-Chauffeuren als Auftragnehmer über eine App zur Verfügung. Es entstehen in der Folge mehrschichtige Vertragsverhältnisse, die mit der nationalen Rechtsordnung nur schwer greifbar werden:

a) Vertrag zwischen Auftraggeber und Betreiber bezüglich Nutzung der Plattform zwecks Order einer Fuhrmöglichkeit;
b) Vertrag zwischen Auftraggeber und Auftragnehmer bezüglich der Fuhr- als Dienstleistung selbst, sodass diesbezüglich zu klären wäre, ob dadurch bereits eine wirtschaftliche und persönliche Abhängigkeit entstehen kann;
c) Vertrag zwischen Betreiber und Auftragnehmer bezüglich der Fuhrdienstleistungsanbietung auf der Plattform, sodass auch in diesem Falle zu prüfen wäre, ob nicht schon durch dieses Anbot des Betreibers an den Auftragnehmer seine Daten zu veröffentlichen eine wirtschaftliche und/oder persönliche Abhängigkeit entstehen kann; und ein
d) Vertrag zwischen Auftraggeber, Auftragnehmer und Betreiber einerseits und Anbietern von Kryptowährungen, da die Bezahlung in Zukunft auch im virtuellen Raum durch Belastung seiner elektronischen Geldbörse erfolgen kann.

Ausgehend von den dargestellten Vertragsverhältnissen, die ordnungsgemäß für eine bestimmte Dauer der Fuhrleistung gegen Entgelt abgeschlossen werden, stellt sich im Falle der Nichterbringung oder Schlechterbringung die Frage, wer zur Haftung und an welchem Ort herangezogen werden kann, da eine absolute Abwälzung des Unternehmerrisikos auf den Auftragnehmer nicht sozialadäquat erscheint. Es stellt sich zudem die Frage, was passiert, wenn das Entgelt elektronisch nicht umgebucht werden kann. Schließlich muss festgestellt werden, dass die offenen Fragen der Speicherung und Verarbeitung von personenbezogenen Daten bei diesem Geschäftsmodell im Kontext mit der Datenschutz-Grundverordnung (DSGVO, Verordnung der EU 2016/679 des Europäischen Parlaments und Rates vom 27.4.2016) nicht geklärt sind, weshalb sich wesentliche Nachteile für alle Beteiligten ergeben können.

Die Zukunft des digitalisierten Vertrauens wird zunehmend auf ein dezentrales Speichersystem mit permanenter Protokollführung basieren und jede teilnehmende Person kann für sich erkennen, dass ihre Daten korrekt verarbeitet und verspeichert wurden; wodurch die klassische monolithische Serverstruktur mit starrer Vernetzung zwecks Datenhaltung in den Hintergrund gedrängt werden wird. Digitales Geld braucht für die tägliche Akzeptanz ein tiefgehendes Vertrauen zum **Cyberraum**.

Bereits heute ist erkennbar, dass ungeschützte Computer, die ans Internet andocken, Gefahr laufen durch eine **Malware** Schaden zu nehmen – Software wird zur Waffe. Ärgerlich, wenn eine Schadsoftware in Form eines sich reproduzierenden Wurms die Datenbestände auf der eigenen Festplatte löscht; immer davon ausgehend, dass jederzeit auf eine funktionierende Datensicherung zurückgegriffen werden kann. Fatal wird dieses Szenario, wenn ein Computervirus Computernetze von Staaten oder öffentlichen Institutionen angreift, um Informationen auszuspionieren oder direkt Firmenspionage betreiben zu können. Durch die bekannten Diebstähle an geistigem Eigentum der letzten Jahre lässt sich ein Schaden von mehreren Milliarden Dollar abschätzen. Tatsache bleibt: Je mehr User online sind und je entwickelter die Hardware ist, die ans Internet angeschlossen werden, desto größer sind die Gefahren für **ADV**-technische Manipulationen. Es entsteht durch diese Vielzahl von Nutzern eine unvorstellbare Vielfalt an Optionen der Verwundbarkeit dieser Systeme – entweder isoliert betrachtet oder als Schwarmnetze. Gesellschaftspolitische Konflikte wurden oftmals kriegerisch durch Vernichtung von Menschen und Maschinen ausgetragen. Ein **Cyberkrieg** ist eine Konfliktform, die für die heutige Zeit von großer Relevanz ist. Weder die rechtlichen Rahmenbedingungen noch die technischen Entwicklungen können der Völkergemeinschaft eine Garantie der Sicherheit und der Gewaltlosigkeit abgeben – der Computer als **Cyberwaffe** ist überall und gegen jedermann sofort einsetzbar. Ländergrenzen werden zu unbedeutenden Landmarken im Internet, sodass ganze Bevölkerungsschichten durch **Cyber-Attacken** bedroht werden können. Wenn jeder jeden angreifen kann, wird der Diebstahl von virtuellen Beständen von Kryptowährungen nicht nur denkbar, sondern real – wer haftet dann wem gegenüber?

Beispiel:

Sehr lang wurden Banküberfälle durch Gewaltanwendung gegen Mensch und Leben durchgeführt, indem Bankräuber in die Bank eindrangen, die Anwesenden bedrohten und schließlich versuchten, mit dem erbeuteten Geld zu fliehen; der Dieb wird durch die Gewaltanwendung zum Räuber, da er den der Bank gehörenden Besitzstand an Geld gewaltsam bricht, um es in der Folge widerrechtlich in sein Gewahrsam zu bringen. Verwirklicht er als Täter das Delikt – er ist grundsätzlich eindeutig identifizierbar. Heutzutage erfolgt der Diebstahl auf Byte-Ebene, denn durch sorglos aufbewahrte Passwörter dringt der Täter in das Computersystem der Bank ein, wählt Konten und lässt das Giralgeld elektronisch auf ein Konto seiner Wahl abbuchen und nach seinem Willen umbuchen, sodass es sehr schwierig wird, ihn als Täter auszuforschen. Noch komplexer wird es, ihn strafrechtlich zu verfolgen, da ihm ad personam erst die Tat nachgewiesen werden muss – übrigens welche? War es ein Cyber-Banküberfall oder war es ein Angriff auf einen

Staat, denn der Cyberangriff auf Konten einer Bank auf dem staatlichen Territorium kann transformativ auch einen volkswirtschaftlichen Schaden bedingen. Wird noch das Kalkül einer Kryptowährung einbezogen, wird die rechtliche Dimension zur Verfolgung mit Verurteilung um ein Vielfaches komplexer.

Cybersicherheit ist eine der weltweit schnell wachsenden Industrien, weil sich nicht nur Unternehmen, sondern auch Staaten – teils militärisch – gegen feindliche **Cyber-Operationen** wappnen müssen. Dies bedingt eine Komplexität, sodass sich daraus eine Dominanz für bestimmte Unternehmen ergeben kann, die zu einer gewollten Überwachungsdichte der Bevölkerung unter Aushebelung der Menschenrechte führen wird. Die Sammlung von Daten wird zum unternehmerischen Machterhalt genutzt, obwohl es streng genommen Daten eines jeden einzelnen Menschen sind, auf die nur er ein persönliches Recht hat.

Beispiel:

Die derzeitige Infrastruktur von Banken beruht auf einer veralteten Technologie, sodass in den nächsten Jahren massive Investitionen mit gleichzeitigem Personalabbau notwendig sind. Fintech-Unternehmen erklären den Banken, dass sie ein großes Hauptbuch sind, in dem festgehalten wird, wie viel Geld den Bankkunden gehört und wie viel Geld ihnen die Bankkunden schulden. Der Zugriff auf Daten seitens der Bank und seitens der Kundschaft ist derzeit zwar möglich, jedoch weiß keiner von beiden, was der andere zu bieten hat. Es geht in erster Linie um die Daten, die aufzubereiten sind, damit einerseits die Bonitätseinschätzung transparent wird und andererseits das Rating des Kunden in Echtzeit einsehbar ist. In zweiter Linie kann von der Bank den Kunden entgeltbare Dienstleistungen wie bspw Haushaltsrechnung, Finanzierungsplanung oder Investitionsberechnungen, angeboten werden, die sodann für ein Ansuchen betreffend die Gewährung von Förderungen oder als Abschluss für das Finanzamt genutzt werden können, weil die Bank über alle relevanten Daten verfügt. Diese Datenmengen sind demnach strategisch als Unternehmenswert und operativ als Rentabilitätsmaßstab zu schützen, sodass diese Cyber-Integrität von Dritten zugekauft werden muss. Daraus ergibt sich eine Einschränkung des Rechts auf den eigenen Datenbestand. Wenn nun Bestände an Kryptowährungen im Cyber-Raum überwiegend anonym gekauft und verkauft werden können, muss für die Massentauglichkeit ein Cyber-Sicherheitssystem angeboten werden, das den einzelnen User überzeugt und ein entsprechendes Vertrauen auslöst.

Schließlich ist an die Nutzung der Sozialen Netze zu denken, da dort eine virtuelle Persönlichkeit geschaffen wird, die niemals sterben kann. Ein Löschungsvorgang der eigenen Daten im Netz hat immer zur Folge, dass Datenrestbestände bei Dritten gespeichert bleiben. Der virtuelle Fußabdruck ist mit seiner Verspeicherung im Netz endgültig. Wenn oftmals seitens der Banken und/oder staatlichen Institutionen ins Treffen geführt wird, dass die Nutzung von Kryptowährungen verschiedene Formen von Terrorismusfinanzierung Vorschub leisten, dann sind solche Argumente nur für

die Öffentlichkeit gedacht, da jede Umbuchung einer Kryptowährung im Netz aufscheint, womit ein Rückschluss unter Beobachtung der Sozialen Systemnetzumwelt möglich wird. Dies gilt auch für das **Darknet**, zumal bestimmte Prozeduren die Offenlegung von persönlichen Daten bedingen – einmal verspeichert, bleiben sie auch für Dritte auffindbar.

Wohin die Reise gehen kann, bespricht *Cecila Skingsley* als Vizegouverneurin der schwedischen Zentralbank, wenn sie meint, dass zukünftig das schwedische Bargeld durch Nutzung einer *E-Krone* als digitale Währung neben dem Giralgeld entfallen können würde. Es könnte zu einer entsprechenden Verminderung der Gebühren kommen, die derzeit noch von den Kreditkartenfirmen für ihren Aufwand verrechnet werden, weil entweder mit wiederaufladbaren Kreditkarten, die von der *Riksbank* ausgegeben werden, oder mit dem Mobiltelefon bezahlt wird. Nebeneffekt dieser Einführung sollte die Verhinderung von nicht deklarierten Einnahmen aus betrieblichen und/oder privaten Geschäften sein, weil es kein Bargeld mehr in Schweden geben wird. Umgesetzt soll dieses System über eine abgewandelte Blockchain werden, da es personenbezogene Kontendaten nicht jedermann zugänglich zu machen gilt, weshalb neben dem bisherigen Verschlüsselungssystem auch eine Kombination mit einer App-Funktion als Code-Entsperrung Platz greifen soll. Sämtliche Bankverträge sollten auf dieser Datenbanktechnologie der Verspeicherung aufbauen, um eine transparente Dokumentation auch für die schwedische Finanzverwaltung entstehen zu lassen. Weil diese Technologie auch die **Smart-Contracts**-Entwicklung fördert, indem sämtliche bankrelevanten Geschäfte über standardisierte Eingabemasken erfolgen, die im Hintergrund einen zivilrechtlichen Vertrag generieren, kommt es für die Banken zu wesentlichen Einsparungspotenzialen, die sie nutzen können. Juristische und fiskal- sowie geldpolitische Schwierigkeiten sind zu klären, insbesondere welche Garantie über den innewohnenden Wert dieser virtuellen Währung – mit Einführung der **E-Krone** als digitale Währung vom Staat – abgegeben werden muss, weil die *Riksbank* diese Kryptowährung selbst emittiert.

Demgegenüber plant *Putin* für Russland laut seinem Kommunikationsminister *Nikiforows* über die russische Zentralbank einen **KryptoRuble** auszugeben, sodass es zu einer Untersagung Dritter für einen Miningprozess käme, weil diese **Cyber-Devise** als staatliches Instrument – hergestellt von der Behörde – der Bürgerschaft zur Verfügung stehen würde. Ein allfälliger Kursgewinn bei Umtausch der digitalen Kryptowährung in Rubel wäre einkommensteuerpflichtig; gleich wie der Ankauf von KryptoRuble, wenn nicht lückenlos die Historie des Geldes nachgewiesen werden kann. Das russische Finanzministerium will noch entscheiden, ob es sich beim KryptoRuble um virtuelles Geld oder um digitales Vermögen handelt, sodass aufgrund all dieser Unwägbarkeiten wie etwa zentrale Ausgabe und Überwachung, Verbot des Miningprozesses, Kursgewinnbesteuerung sowie Besteuerung bei nur glaubhaft gemachtem Geldursprung, und unklare Klassifizierung durch das russische Finanzministerium, es sehr schwer sein wird, Akzeptanz in der Cyber-Gemeinde für diese digitale Kryptowährung zu schaffen.

Obskur wird die Entwicklung rund um die Bezeichnung **Coin**, wenn bspw die Firma Kodak ihre neue Bildarchivierungsplattform **KodakCoin** nennt, worauf der Aktienkurs der besagten Firma steigt, weil die marktteilnehmenden Personen fälschlicherweise angenommen haben, dass Kodak nun ein Geschäft rund um Kryptowährungen beginnen will. Tatsächlich soll KodakCoin eine Möglichkeit bieten, unerlaubte Nutzung geschützter Bilder im Netz zu verfolgen und zu stoppen.

Der kurzfristige Absturz der Kryptowährung **bitcoin** ist einerseits auf eine spekulative Blasenwirkung am Markt, auch wegen der Gier nach „schnellem Geld des kleinen Mannes“, und andererseits wegen der enormen Energiekosten für die Generierung neuer **Tokens** zurückzuführen, weil die benötigte Rechenleistung überproportional steigt. Nach der *Gaußschen* Kurventheorie gilt, dass nach dem Sättigungsgrad jener Kostenteil beginnt, der wesentlich höher ist, als dies von der Wertentwicklung am Markt durch Kauf und Verkauf abgebildet werden kann.

1.3 Zeit als Währung in der Zukunft

Ausgehend vom Neoliberalismus als Doktrin der unkontrollierten Märkte bei minimalen Staatseingriff, bei dem der Wohlstand dadurch entsteht, dass die teilnehmenden Personen im Rahmen des Eigennutzes ihre Interessen so verfolgen, dass ihre Teilnahme am Markt vom eigenen Vorteil bestimmt wird, weil eben der staatliche Eingriff nur rudimentär ist. Die sich daraus ergebende Ungleichheit ist gewollt, da sie für das Aufrechterhalten des Systems notwendig ist. Der Postkapitalismus bedingt, dass die Informationstechnologie den erforderlichen Arbeitsaufwand der Beschäftigten grundsätzlich verringert. Die Grenzen zwischen entgeltlich orientierter Arbeit und zu finanzierender Freizeit sind nicht mehr starr, weshalb sich die Beziehung zwischen der zu erbringenden Arbeit und dem daraus resultierenden Einkommen gelockert hat. Die Information als Gut ist im **Cyber-Raum** im Überfluss vorhanden, ohne dem Diktat der Knappheit zu folgen, sodass sie den Markt um die Fähigkeit einer real-sozialgewichtigen Preisfestlegung bringt. Die kollaborative Allmende-Produktion als Peer-Produktion im Cyber-Raum bewirkt eine Entwicklung von einem Markt, der ohne Managementhierarchie und ohne Entgeltsanspruch agiert, bspw wird Wikipedia von sehr vielen Freiwilligen gratis erzeugt, wodurch Enzyklopädie-Verlage vom Markt verdrängt wurden. Unter Bezugnahme auf das Maschinenfragment von *Marx*, das von der These ausgeht, dass in einer (globalen) Wirtschaft, in der die von Menschenhand geschaffenen Dinge im Sinne des zivilrechtlichen Begriffs der Sache einen Großteil der Produktions- und Dienstleistungsarbeit leisten und die Arbeit von Menschen nur mehr in der Gestaltung, Steuerung, Überwachung und Wartung dieser Dinge wie bspw Maschinen reduziert wird, muss das in diesen Dingen gespeicherte Wissen ein gesellschaftliches sein.

Beispiel:

Die kommerzielle Softwareentwicklung unter Verwendung einer Programmiersprache zwecks Erstellung einer Steuerung (bspw in der Produktion) bedingt, dass für den Prozess der Schnittstellenanpassung auf Informationen zurückgegriffen

wird, deren Code von Dritten erstellt wurde. Weder der Programmierer der Produktionssteuerung, noch das Unternehmen, das den Programmierer beauftragt hat, ist Eigentümer aller verwendeten Codes, sodass dieses Wissen gesellschaftlich ist. Die Entwicklung der Software basiert auf dem Wissen und der Erfahrung Dritter, die der Gesellschaft im Netz zur Verfügung gestellt wird, damit die geplante Steuerung der Produktionsanlage erstellt werden kann. Die Kreativität und das eingesetzte Wissen des Programmierers in Relation zum bereitgestellten Softwareentwicklungsumfeld sind dadurch minimal, obwohl diese Faktoren zur Mehrung des gesellschaftlichen Wissens beitragen. Komplexer wird die Sachlage, wenn lernfähige Micro-Programme Routinen selbständig ausführen. Damit tragen sie zur Wissensmehrung autonom bei, sodass dieser Prozess nur dadurch wahrgenommen wird, weil der programmierende Mensch auf diese Routinen aus Vereinfachungsgründen zurückgreift.

Wenn Wissen eine entscheidende Produktionskraft ist, kann eine Produktionssteigerung kaum durch Verlängerung der Arbeitszeit, sondern durch nicht-monetäre Anreizsysteme entstehen. Längere Arbeitstage sind energieaufwendiger und mit der Beschleunigung der Arbeitsabläufe wird bald an die Grenzen der menschlichen Geschicklichkeit und Belastbarkeit gestoßen. Die Mehrung von Wissen bedingt ein kreativ-gesellschaftliches Umfeld, damit der Einzelne seine Erkenntnisse in der kritischen Diskussion mit Dritten austauschen und seine Entwicklungen verbessern kann. Aus dieser Theorie wird geschlossen, dass der auf diesem Wissen beruhende Kapitalismus nicht mit einem Preismechanismus funktionieren kann, indem der Wert eines Guts vom Wert der für seine Erzeugung benötigten Inputs an Produktionskraft abhängt. Bei einem auf Wissen beruhenden Kapitalismus kommt es zu einem logischen Widerspruch zwischen den Produktionskräften, bestehend aus Maschinenarbeit und Arbeitskraft, und den gesellschaftlichen Beziehungen in einem wirtschaftlichen Austausch. Heute keimt der Informationskapitalismus, da Daten und Information wesentlich die globalen Märkte beherrschen, sodass unter strenger Konsequenz der Anwendung des Maschinenfragments es zu einer Verringerung der Arbeitszeit auf ein Minimum kommen muss. Sozialadäquat wäre das gesamte akkumulierte Wissen der Gesellschaft so einzusetzen, um aus dem gesellschaftlich produzierten Wissen eine Menge an freier Zeit für die Menschen entstehen zu lassen – es kommt nach *Drucker* zur „gebildeten universellen Person“. Die geschaffene Produktion ist am Markt anzubieten und das vom Angebot-Annehmer eingesetzte Geld schafft den Wertausgleich. Dieser monetäre Wertausgleich ist nicht sofort real, da er auf einer virtuell geschaffenen Währung basiert, sodass er auch Teil des gesellschaftlichen produzierten Wissens wird. Durch den Einsatz von Kryptowährungen kommt es zu einer konsequenten Weiterverfolgung dieser Theorie – Geld als Währung tritt in den Hintergrund und Zeit als Währung wird immer wichtiger.

„*In Time – Deine Zeit läuft ab*“ – ein Sciencefiction-Film von *Andrew Niccol* zeichnet ein gesellschaftspolitisches Bild in einer Zukunft, bei dem die Lebenszeit als einzig akzeptierte Währung für die Bezahlung von Waren und Leistungen angenommen wird. Durch Genmanipulation ist das Lebensalter aufgrund der Überbevölkerung

beschränkt, sodass der Tod durch Erreichen eines bestimmten Lebensalters vorherbestimmt ist. Dieser Film als Kritik am herrschenden Jugendwahn und gesellschaftspolitischen Sozialdarwinismus-Mahnung zeigt das menschliche Verhalten in Extremsituationen aufgrund der sozialen Fehlentwicklungen auf, sodass damit das Erkennen der eigenen Zeiteinteilung in Frage gestellt wird. Zeit ist für die arbeitende Gesellschaft sekundär, da sie sich dem selbstverherrlichenden Ego unterzuordnen hat – „*Ich muss*" ist die vorherrschende Prämisse, ohne auf gesellschaftspolitischer Ebene wahrzunehmen, dass sich die Produktionsvoraussetzungen wesentlich verändert haben. Das eingesetzte Wissen wird täglich durch neue Erkenntnisse gemehrt und Produktionsprozesse können ständig optimiert werden. Anstatt diese Entwicklung anzunehmen, in dem der Mensch seine Freizeit ausweitet, wird über die Verlängerung der Arbeitszeit diskutiert, wohl wissend, dass jedes Wachstum beschränkt ist. Die eigene Zeit ist das höchste Gut, zumal sie gleichzeitig verhandelbare Ware und selbstredend Währung darstellt. Die Schaffung von Kryptowährungen entkoppelt viele realwirtschaftliche Prozesse vom Leben, da diese nur im Cyber-Raum aufgrund der menschlichen Kreativität und des ökonomischen Überlebenswillens des Menschen stattfinden kann.

Kreativität, Erfindungskraft und globales Wissen tragen wesentlich zur derzeitigen Produktionsweise bei, sodass daraus der kognitive Kapitalismus abgeleitet wird. Die immaterielle Arbeit schafft in seiner gesamten menschlichen Bandbreite eine Wissensökonomie, die eine „neue" Ordnung in der Gesellschaft entstehen lässt. Es kommt zu einer Transformation von Wissen zur Ware. Dieser Theorie folgend ist die Kryptowährung eine logische Weiterentwicklung dieses eingeleiteten Prozesses und das Geld aus der Realwelt wird in den virtuellen Raum des optionalen Seins gezogen.

Alternativ wird heute gerne der Tausch als Option für die Installierung eines alternativ-regionalen Wirtschaftssystems zum Thema gemacht. Die nationale Währung eines Landes oder eines Staatenbundes verliert zunehmend an Vertrauen in der Bevölkerung und Regionalwährungen entstehen, weil die Menschen, die in dieser Region leben, den Wert der Produktion selbst festlegen wollen. Entweder weil die Preisentwicklung nicht mit den Realeinkommen in keinem „gefühlten" stimmigen Verhältnis mehr ist oder weil im Internet abrufbare Informationen den Schluss zulassen, dass die nationale Währung keine staatliche Deckung mehr innehat, sodass sie seitens dieser Bevölkerungskreise nur mehr als Spielgeld angesehen wird. In diesem Spannungsfeld ist zwischen dem klassischen Kapitalismus und **Peer-Produktionen** als divergierende Systeme zu unterscheiden, die derzeit noch parallel existieren und sich stärken. Nach *Rifkin* kommt es durch das vernetzte Kommunikationsverhalten mit gezielter (Internet-)Datennutzung zu einer berechenbaren Kostensenkung, womit eine damit einhergehende Effizienzsteigerung die Folge ist. Das Cyber-Netzwerk trägt dazu bei, die Grenzkosten im Sinne von Zusatzkosten physischer Güter und Dienstleistungen auf dieselbe Art zu senken wie „copy and paste" die Kosten von Informationsgütern senkt. Durch die Teilnahme jedes Menschen und Gegenstandes an einem intelligenten Netzwerk kommt es zur Teilhabe mit exponentieller Wirkung nach außen. Diese Theorie nimmt an, dass die Zusatzkosten von Energie und materiellen Gütern durch den Allmende-Einsatz auf ähnliche Art sinken werden, wie das

Internet dies bei digitalen Produkten bewirkt. Die Frage nach dem Schutz des geistigen Eigentums bleibt bei dieser Annahme unbeantwortet. Für den Kryptowährungsbereich kann eine inflationäre Entwicklung durch ein unüberschaubares Angebot von Kryptowährungen dazu führen, dass die Grenzkosten zur Schaffung dieser Kryptowährungen gegen Null gehen müssten. Wer die Entwicklung auf diesem Markt kennt, weiß, dass dies deshalb unvorstellbar ist, da die notwendige Rechenleistung und der damit verbundene Energieverbrauch wesentliche Einflussfaktoren für diesen Bereich sind.

In diesem Zusammenhang ist auf die Entwicklung im Bereich des **Crowdsourcing** bzw **Crowdworking** Bezug zu nehmen, weil es eine Arbeitsform als eine interaktive Leistungserbringung darstellt, die kollaborativ oder wettbewerbsorientiert organisiert sein kann. In einem solchen System agieren eine große Anzahl von extrinsisch oder intrinsisch motivierten Akteuren als **Prosumenten** mit unterschiedlichem Wissensstand unter Verwendung von moderner Informations- und Kommunikationssysteme. Leistungsobjekt sind entweder Produkte oder Dienstleistungen mit unterschiedlichen Innovationsgrad, die durch Nutzung des (Schwarm-)Netzwerks der Partizipierenden als teilweise Auftragnehmer reaktiv durch externe Anstöße oder proaktiv durch selbständiges Identifizieren von (Bedarfs-)Lücken entwickelt werden. Ökonomisch kommt es zu einer strategischen Auslagerung einer üblicherweise von Erwerbstätigen entgeltlich zu erbringender Leistung, durch einen gezielten Aufruf an eine Masse von unbekannten Personen, die das Internet nutzt, um daraus direkt wirtschaftliche oder frei verwertbare Vorteile zu erzielen. Die Entgeltlichkeit tritt bei diesem unternehmerischen Agieren oft in den Hintergrund. Beispielsweise wenn die erbrachten Leistungen nicht abgenommen werden, weil sie nicht den Vorstellungen des Unternehmers als Auftraggeber entsprechen. Kritisch ist diese Entwicklung zu sehen, wenn das Unternehmen versucht, kostenlos oder listig zu diversen Vorschlägen durch die im Schwarm agierenden Prosumenten zu verwandten Themen zu bekommen, um zukünftige und innovative Entwicklungen unter der eigenen Urheberschaft anzustoßen. Der Vorteil dieser Entwicklung besteht darin, dass aufgrund der Einbeziehung der Kundschaft am Produktionsprozess eine gezielte Umsetzung der Vorstellung der Kundschaft gegeben ist. Die Kritik am **Crowdworking** wird nachvollziehbar, wenn Unternehmen anfangs unbezahlte und freiwillige Mitarbeit an einem Projekt annehmen, um die entgeltlichen Arbeitsleistungen in **Microjobs,** ohne umfassende soziale Absicherung in einem Schattenarbeitsmarkt, auszulagern. Ein weiterer Kritikpunkt sind die Schöpfungsrechte, da bisher rechtlich keine klare Aussage besteht, wem diese zustehen – dem Unternehmen als Auftraggeber oder dem Prosumenten als geistigen Schöpfer. Diese aufgeworfenen Probleme werden durch die Schaffung von Kryptowährungen durchwegs verstärkt, da durch die Zerteilung von Projekten, abgegolten mit Kryptowährungseinheiten und aufgeteilt in kleine Aufgaben, es zukünftig leichter sein wird, all diese Prozesse schneller und kostengünstiger – ohne Rücksichtnahme auf die sozialen Standards in der realen Welt – zu realisieren. Das Konzept eines **Social Forecasting** als betriebswirtschaftliche Methode rund um Vorhersagen über zukünftige Ereignisse aus dem kollektiven Wissen einer Gruppe in virtuellen Prognosebörsen könnte als Basis für eine angemessene Entlohnung des

Crowdsourcing-Prozesses genutzt werden, zumal diese auch in einer expandierenden Kryptowährung mit einem geringen Einstiegskurs erfolgen könnte.

Die **Generation Y** ist grundsätzlich sehr gut ausgebildet und zeichnet sich durch einen technikaffinen Lebensstil aus, weil sie mehrheitlich mit dem Internet und der mobilen Kommunikation aufgewachsen ist. Die Arbeit wird eher teamorientiert gesehen. Ziel der Arbeit ist die Freude an ihr und nicht Status oder Prestige, weshalb der Gedanke der **Work-Life-Balance** im Vordergrund steht. Dieser Wertewandel wird durch offene Nutzung von Kryptowährungen fortgesetzt. Diese Menschen sind im Umgang mit Krisen trainiert und die Improvisation gehört zur Lebensplanung per se, sodass die Freizeit dazu genutzt wird, mit Teilnehmern aus den Sozialen Netzwerken zu kommunizieren. Berufliche Unabhängigkeit bedingt ein lebenslanges Lernen, sodass diese Generation auch eine Entgeltlichkeit für ihre Mühen in Form von Kryptowährungen mit Entwicklungspotenzial akzeptiert.

Kapitel 2
Technische Aspekte

Ein **Bit** als kleinste binäre Einheit in der Digitaltechnik kann nur zwei Zustände annehmen – entweder Null oder Eins. Eine binäre Folge von acht Bit als Datenpäckchen ergibt die Maßeinheit **Byte**, die in der Informatik Standard ist. Der historische Ansatz geht davon aus, dass ein Byte als eine bestimmte Anzahl von Bit dazu verwendet wurde, um einzelne Schriftzeichen zu codieren. Das Byte diente als kleinstes adressierbares Element in vielen Rechenarchitekturen. Das Wort Bit ist ein Schachtelwort, bestehend aus den englischen Wörtern ***bi**nary* und *digi**t***; hingegen ist der Begriff Byte als Kunstwort zu sehen, und es wird als Standardeinheit für Speicherkapazitäten und Datenmengen verwendet. Für Datenspeicher mit binärer Adressierung ergeben sich die Speicherkapazitäten von 2^n Byte, also in Form von Zweierpotenzen.

Digitale Kryptowährungen bauen auf den vorerwähnten Einheiten auf. Jedoch sind sie in ihrer Komplexität interdisziplinär zu sehen. Diese Mehrschichtigkeit geht als Schnittmenge aus der Kryptografie, der Ökonomie und Informatik hervor. Grundsätzlich sind Kryptowährungen keiner Entität unterstellt. Kryptowährungen sind als ein autonomes Konstrukt zwecks Bedienung der Anspruchsgruppenerwartungen zu sehen, das ein System prägt, das auf komplexer Interaktion und Anreizstrukturen beruht. Durch die gezielte Unabhängigkeit ist es möglich, virtuelles Eigentum nachvollziehbar abzubilden. Demgegenüber steht die klassische Registerzentralisierung, um einen Konsens über den Zustand von virtuellen Besitzzuständen darzustellen, weil in einem solchen zentralistischen System eine Instanz eingeschaltet ist, die exklusiv mit Registerführungsrechten ausgestattet ist. Durch diese Ausschließlichkeitsrechte für diese anerkannte Verwaltungsstelle im digitalen System besteht die Gefahr einer willentlichen oder unabsichtlichen Veränderung von der Instanz selbst oder durch eine Einflussnahme von außen durch Dritte. Die dezentrale autonome Struktur von Kryptowährungen als System schließt die vorgenannten Probleme großteils aus. Kryptowährungen sind jetzt schon als eine Art Grundgerüst zu sehen. Die Entwicklung als Quasi-Zahlungsoption dient als Fundament für eine Vielzahl neuartiger Applikationen; denkbar bspw ist die Darstellung des virtuellen Eigentums als valide Technologie-Grundlage durch die native Recheneinheit im jeweils geschaffenen Kryptowährungsregister.

Das Einsatzgebiet von digitalen Verrechnungssystemen ist mannigfaltig, da sehr viele Gegenstände, die im täglichen Leben genutzt werden, mit Mikroprozessoren ausgestattet sind, sodass sie untereinander vernetzt werden können. Die Nutzung und Verwaltung erfolgt über *Smart Contracts* als Computerprotokolle, die sowohl Verträge darstellen oder überprüfen können als auch die Verhandlung oder Abwicklung des Vertrags technisch unterstützen sollen, wodurch die Schriftform sekundär oder hinfällig wird. Diese virtuellen Protokolle verfügen über klar definierte Benutzerschnittstellen, sodass sie die Logik vertraglicher Regelungen technisch abbilden können.

BEISPIEL:

Smart Contracts als Computerprotokolle können bspw in der digitalen Rechteverwaltung die abgeschlossenen Copyright-Lizenzen transparent abbilden; oder im Finanzbereich können die getätigten Transaktionen eindeutig und nachvollziehbar dargestellt werden, weil sie das Design von E-Commerce-Protokollen mit einem hoch entwickelten Vertragsrecht verbinden.

Durch das ständige Abgleichen, Speichern und Weitergeben von Daten zwischen den Maschinen kann die Nutzung überwacht werden, sodass nutzungsabhängige und in *Realtime* vereinbarte Zahlungen für deren Nutzung vereinbart und von der elektronisch eingerichteten Brieftasche (**Wallet**) abgebucht werden können. Durch intelligente Verwendung von Kryptotransaktionssystemen ist die Bezahlung solcher Kleinstbeträge keine große Herausforderung und die Algorithmen der genutzten *Smart Contracts* können die mit ihnen verbundenen Gegenstände automatisch steuern, weshalb bspw Nachbestellung selbständig vom System in die Wege geleitet werden – diese Vernetzung der Gerätschaften wird auch *Internet of Things* (**IoT**) genannt.

2.1 Einführung in die Kryptografie

Klärend wird festgehalten, dass die Abgrenzung zur **Steganografie** darin besteht, dass dieses Verfahren den Kommunikationskanal verbirgt; hingegen die **Kryptografie** die Nachricht verschlüsselt. Für digitale Währungen werden zweckgebunden die Techniken der Kryptografie genutzt.

Klassische Computeranwendungen der Kryptografie basieren auf **symmetrischen Verschlüsselungsverfahren**, indem zwischen den Benutzern ein gemeinsamer, aber Dritten gegenüber geheimer Schlüssel (k) vereinbart wird. Dieses Schlüsselsystem wird zur Ver- und Entschlüsselung der Nachricht verwendet. Der Schlüssel wird sodann in der Kommunikation wechselseitig genützt. Die Schwachstelle dieses kryptografischen Systems besteht darin, dass die Benutzer von Anwendungen diesen über einen sicheren Kommunikationskanal fixieren müssen, sodass es lediglich zu einer zeitlich orientierten Verschiebung der Sicherheitsanforderungen an den Kommunikationskanal kommt.

$$k = 0$$

Asymmetrische Verschlüsselungsverfahren heben die vorerwähnte Einschränkung auf. Sie ermöglichen einen initialen Schlüsseltausch über Kommunikationskanäle, die potentiell unsicher sind. Schließlich können sie abgehört werden. Statt eines gemeinsam vereinbarten Schlüssels erstellt jeder Benutzer sein eigenes und persönliches Schlüsselpaar, bestehend aus einem privaten Schlüssel (k_p) und einem öffentlichen Schlüssel ($k_{\ddot{o}}$). Der öffentliche wird offengelegt; hingegen ist der private immer geheimzuhalten. Die Genialität dieses Schlüsselpaars basiert darauf, dass der öffentliche aus dem dazugehörig privaten Schlüssel aufgrund der mathematischen Eigenschaften abgeleitet werden kann; im Gegensatz dazu der öffentliche nicht zur Herleitung des privaten Schlüssels taugt. Der öffentliche Schlüssel wird als Produkt errech-

net, indem ein allgemein bekannter Basispunkt (G) einer elliptischen Kurve mit dem zuvor gewählten privaten Schlüssel multipliziert wird:

$$k_{Ö} = k_p \text{ x } G$$

Eine weitere Eigenschaft eines solchen Schlüsselpaares besteht darin, dass eine Nachricht, die mit dem einen Schlüssel codiert wird, mit dem anderen Schlüssel decodiert werden kann. Einerseits wird dadurch die Geheimhaltung zwischen Schlüsseleigentümer und Dritten und andererseits die Integrität und Authentizität der Nachricht gewährleistet.

2.1.1 Geheimhaltung

Jeder Dritte kann den öffentlichen Schlüssel eines Benutzers dazu nutzen, eine Nachricht zu verschlüsseln. Da aber zur Entschlüsselung der zugehörige private Schlüssel benötigt wird, ist der Besitzer des Schlüsselpaares der einzige Benutzer, der diese Nachricht entschlüsseln kann.

BEISPIEL:

Werden bspw sensible Informationen zu einer Person mit einem öffentlichen Schlüssel durch ein Unternehmen verschlüsselt, sollte dadurch sichergestellt sein, dass nur dieses Unternehmen auf diese Daten der Person einsehen kann.

2.1.2 Authentizität und Integrität

Wird von einem Benutzer eine Nachricht mit dem eigenen persönlichen Schlüssel codiert, kann die Information von jedem anderen Benutzer aufgrund des öffentlichen Schlüssels mit der Sicherheit, dass diese Nachricht vom Inhaber des privaten Schlüssels erstellt wurde, entschlüsselt werden. Das stellt die Prinzipien der Authentizität aufgrund der Nachrichtenerstellung durch den Besitzer des öffentlichen Schlüssels, der auf seinem privaten aufbaut, und der Integrität aufgrund der Verhinderung der nachträglichen Anpassung, sicher. Die Unterscheidung zwischen Inhaber und Besitzer erscheint aufgrund der möglichen Manipulation in der realen Welt als angebracht, weshalb auch der Begriff des Eigentümers aufgrund der grundsätzlich anonymen Nutzung im virtuellen Raum nicht verwendet wird.

In der **Bitcoin**-Technologie wird ein asymmetrisches Kryptoverfahren, basierend auf elliptischen Kurven, angewandt. Im Gegensatz dazu wird in der klassischen Kryptografie das Augenmerk auf die Fokussierung mittels Primzahlenzerlegung und Finden von diskreten Logarithmen gelegt. Eine Primzahlenzerlegung besteht aus einer Darstellung einer natürlichen Zahl als Produkt aus Primzahlen, die in der Folge als Primfaktoren bezeichnet werden:

$$N(=^{M}\Sigma_{k}=1e_{k}).$$

Als diskreter Logarithmus wird ein ganzzahliger verstanden:

$$a^x \equiv m \bmod p$$