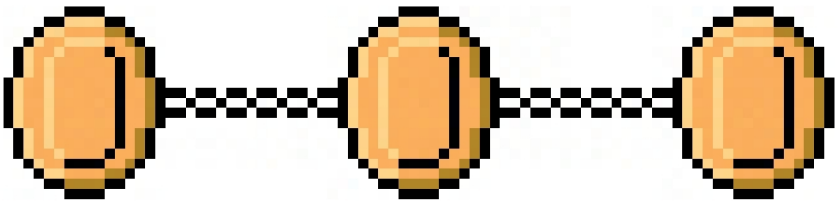
Aleksander Berentsen | Fabian Schär

Bitcoin, Blockchain und Kryptoassets

Eine umfassende Einführung



Universität Basel

Aleksander Berentsen | Fabian Schär

Bitcoin, Blockchain und Kryptoassets

Erste Auflage

Universität Basel

Bibliografische Informationen der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Das vorliegende Buch ist Teil der Dissertationsschrift von Fabian Schär. Grosse Teile des Buches wurden alleine durch Fabian Schär verfasst. Dies gilt insbesondere für die Kapitel 2, 3, 4, 5, 7 und 8. Kapitel 1 und 6 wurden von Fabian Schär und Aleksander Berentsen gemeinsam verfasst.

Herstellung und Verlag:
BoD - Books on Demand, Norderstedt

Finanziert durch den Förderverein des Wirtschaftswissenschaftlichen Zentrums der Universität Basel

ISBN: 978-3-7431-8272-1

1. Auflage vom 15. Januar 2017

Vorwort

Kryptowährungen haben in den letzten Jahren eine erstaunliche Entwicklung erfahren und geniessen insbesondere seit der Einführung von Bitcoin im Jahre 2009 eine hohe Publizität. Dies gilt ebenso für weniger bekannte Kryptowährungen wie Ethereum, Ripple oder Litecoin.

Für Schlagzeilen sorgten anfänglich neben den Vorkommnissen um die Bitcoin-Tauschbörse Mt. Gox und der für illegale Aktivitäten vorteilhaften Anonymität von Transaktionen insbesondere die grossen Wertschwankungen der Kryptowährung Bitcoin (BTC). Lag der Wert eines BTC im Frühjahr 2012 noch bei rund 5 USD, kletterte er am 4. Dezember 2013 auf den bisherigen Höchststand von 1'145 USD. Auch im Jahr 2016 hat sich der Kurs von 434 auf 960 USD mehr als verdoppelt. Obschon Bitcoin deswegen nach wie vor primär als Transaktions- und nicht als Wertaufbewahrungsmittel eingesetzt wird, ist das Vertrauen in Bitcoin gestiegen. Verschiedene Akteure akzeptieren inzwischen Bitcoin und andere Kryptowährungen als Zahlungsmittel oder nehmen Einlagen in Bitcoin entgegen. Mit der Stadt Zug bietet seit 2016 auch die öffentliche Hand Zahlungsmöglichkeiten in Bitcoin an. Dass Kryptowährungen damit in ein reiferes Stadium gekommen sind, zeigt sich überdies daran, dass es mittlerweile wie bei anderen wichtigen Währungen auch derivative Kontrakte auf Bitcoin und Ethereum gibt.

Zum Vertrauen beigetragen hat der anfänglich kritisch wahrgenommene Umstand der dezentralen Schöpfung der Währung. Das Geld wird nicht durch Zentralbanken geschaffen, sondern durch einen Algorithmus. Technische Voraussetzung des Systems ist die *Blockchain*, in welcher sämtliche bisherigen Transaktionen lückenlos und an vielen Orten gleichzeitig abgespeichert werden. Gerade diese Architektur einer Vielzahl weltweit abgespeicherter Kopien der Datenbank

verleiht dem System ein hohes Mass an Stabilität und einen Schutz gegenüber Manipulationen und einem Systemausfall.

Trotz der Publizität ist die bisherige wirtschaftliche Bedeutung von Kryptowährungen indessen noch relativ gering: Die Marktkapitalisierung der mit Abstand wichtigsten Kryptowährung Bitcoin lag Anfang 2017 bei lediglich rund 14.5 Mrd. USD, was derjenigen eines grösseren kotierten Unternehmens entspricht. Interessant ist jedoch, dass das technische Kernstück, die Blockchain, zunehmend für weitere Anwendungen im Internet eingesetzt wird. Im Mai 2016 wurde ein DAO (decentralized autonomous organization) Fund auf Basis der Blockchain-Technologie lanciert, bei welchem Investitionsentscheidungen dezentral durch die Investorencommunity getroffen werden. Weitere Anwendungen entstehen zunehmend im Rahmen von Smart Contracts, welche die Nutzung von Software, Musik, Filmen, softwaregesteuerten Gütern wie Fahrzeugen und Sicherheitstechnik abhängig von Zahlungen oder anderen Voraussetzungen machen. Bei Immaterialgütern sowie in Bereichen, wo entsprechende staatliche Institutionen fehlen, bietet die Blockchain-Technologie damit neue Möglichkeiten zur Sicherung von Eigentumsrechten.

Gleichwohl gibt es noch zahlreiche Unklarheiten und offene Fragen: In rechtlicher Hinsicht betreffen diese die Legalität von Transaktionen sowie die Zulässigkeit der Schöpfung von Geld durch Private. Unklar ist ausserdem, wie mit virtuellen DAOs, welche keinen rechtlichen Sitz haben, umgegangen werden soll. Auch die Anonymität von Transaktionen wird im Zuge der Terrorismusbekämpfung und der Erhebung von Steuern zunehmend als problematisch angesehen. Für die Besteuerung erweist sich zudem die hohe Kursvolatilität als Herausforderung, weshalb möglicherweise andere Verfahren zur Berechnung der Steuerwerte erforderlich werden als sie gegenwärtig für Fremdwährungen zum Einsatz gelangen.

In konzeptioneller Hinsicht wird der vom Wirtschaftswachstum losgelöste Prozess zur Schaffung von Bitcoins kritisiert, da die Marktkapitalisierung nicht mit dem Wirtschaftswachstum einhergeht. Die Rate der Ausweitung beträgt aktuell lediglich rund 75 Bitcoin pro Stunde.

Ferner gibt es für die *Miner* hohe technische Voraussetzungen, da das Eigentum an Bitcoins durch das System erfasst sein muss und die Miner Daten sicherstellen müssen, um die Historie jeder Transaktion und der entsprechenden *Blocks* lückenlos zu erfassen.

Vor diesem Hintergrund vermittelt das vorliegende Buch erstmalig eine umfassende und systematische Einführung in das Wesen und die Dynamik von Kryptowährungen und Kryptoassets. Zunächst werden die Grundlagen des Geldes und die Charakteristika von Kryptowährungen besprochen. Der spezielle Fokus liegt hierbei auf der Kryptowährung Bitcoin und der Blockchain als deren technische Grundlage. Der zweite Teil widmet sich der Funktionsweise des Netzwerks, der Sicherheit und der Verschlüsselungstechnik sowie dem Mining. Im dritten Teil analysieren die Autoren die Eignung von Bitcoin als Tauschmittel, Wertspeicher und Recheneinheit sowie weitere nicht-monetäre Anwendungen. Die Ausführungen schliessen mit einem Praxisleitfaden.

Das Buch knüpft damit an die aktuelle Diskussion zu Kryptowährungen an und stellt den Bogen von der geldtheoretischen Basis über die technischen Grundlagen bis hin zu weiteren Anwendungsmöglichkeiten her. Die Autoren vermitteln auf verständliche und zugleich detaillierte Weise ein komplexes und anspruchsvolles Thema. Besonders gelungen gerade für das Studium sind die Aufgaben zur Vertiefung des Stoffes. Es freut mich daher sehr, dass dieses Buch nun der Leserschaft zugänglich ist, und ich bin überzeugt, dass es dazu beiträgt, ein profundes Verständnis dieses spannenden Gebiets und der inskünftig noch viel wichtiger werdenden Technologie zu vermitteln.

Basel, 9. Januar 2017
Prof. Dr. Pascal Gantenbein

Inhaltsverzeichnis

Was ist Bitcoin?

Selbst wenn man sich bereits seit geraumer Zeit mit dem Thema Bitcoin auseinandersetzt, muss man immer wieder erstaunt feststellen, wie schwierig sich das Konzept in Worte fassen lässt. Die grundsätzlich einfache Frage "Was ist Bitcoin?" eröffnet ein ganzes Spektrum möglicher Erklärungsansätze, von denen jedoch keiner wirklich angebracht zu sein scheint. Reduziert man das Konzept auf triviale und rein monetäre Schlagworte, wie etwa *digitales Bargeld*, entstehen falsche Erwartungen und Assoziationen. Es werden unhaltbare Vergleiche mit Kreditkarten, Buchgeld oder E-Banking Lösungen gezogen und Bitcoin wird als uninteressant und irrelevant eingestuft. Versucht man dagegen der Komplexität und Innovationskraft von Bitcoin gerecht zu werden, setzt man ein hohes Mass an Wissensdurst, Geduld und interdisziplinärem Vorwissen voraus (Abbildung 1).

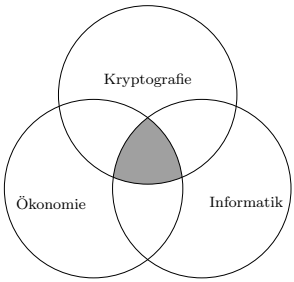


Abbildung 1: Interdisziplinarität von Bitcoin

Das Gegenüber muss gewillt und in der Lage sein, abstrakten Argumenten aus den Disziplinen der Ökonomie, Kryptografie und Informatik folgen und diese verknüpfen zu können. Dies führt mitunter zu grossen Verständnisproblemen.

Erschwerend hinzu kommt die Tatsache, dass Bitcoin keiner Entität unterstellt ist. Die Technologie gehört keiner Person und keinem Unternehmen. Sie wird durch keine einzelne Partei kontrolliert. Bitcoin ist vielmehr ein autonomes Konstrukt mit einer Vielzahl verschiedener Anspruchsgruppen, die das System durch komplexe Interaktionen und Anreizstrukturen prägen.

Durch diese Unabhängigkeit ermöglicht die Technologie erstmals die Abbildung von virtuellem Eigentum, ohne dass dafür eine zentrale Instanz notwendig ist. Was unspektakulär klingen mag, entspricht einem enormen technologischen Durchbruch. Vor Bitcoin konnte ein Konsens über den Zustand virtueller Besitzstände ausschliesslich über die Zentralisierung eines Registers sichergestellt werden. In zentralisierten Systemen wird eine Instanz exklusiv mit Registerführungsrechten ausgestattet. Durch diese Rechte hat eine solche Instanz die Fähigkeit das Register zu manipulieren und Vermögensansprüche beliebig zu verändern. Besteht die Möglichkeit, dass die zentrale Instanz auf irgendeine Weise korrumpierbar oder Ausfällen und Angriffen durch Dritte ausgesetzt ist, wird dies zu erheblichen Problemen führen und die Glaubwürdigkeit des Systems untergraben. Die dezentrale Natur des Bitcoin-Systems macht es immun gegenüber vieler dieser Probleme.

Ferner ist Bitcoin eine Art Grundgerüst, welches das Fundament für eine Vielzahl neuartiger Applikationen bildet. Analog der TCP/IP Technologie, welche oberflächlich betrachtet lediglich einer Standardisierung in der Kommunikation gleichkommt, unsere Lebensweise durch das Internet aber dennoch spürbar verändert hat, ist auch die Innovationskraft von Bitcoin nur dann erfassbar, wenn man die Möglichkeiten weiterer Anwendungen berücksichtigt.

Die Bitcoin-Technologie kann zur Darstellung von Eigentum und Zuständen im weitesten Sinne verwendet werden. Immer wenn es um die dezentrale Verwaltung von Anspruchsrechten an einem knappen Gut geht, oder aber ein bestimmter Zustand festgehalten und öffentlich bezeugt werden soll, bildet Bitcoin eine

valide Technologie-Grundlage. Virtuelle Ansprüche auf Grundstücke, Giralgeld und Unternehmensanteile sind dabei genauso denkbar, wie Ansprüche auf Briefmarken, Domainnamen oder auf eine eigens für das System geschaffene Geldeinheit mit dem Namen *Bitcoin*. Letztere bildet die native Recheneinheit im Bitcoin Register.

Da die Ursprünge von Bitcoin in der monetären Anwendung liegen, haben wir uns dazu entschieden, unsere Analyse aus dieser Perspektive zu beginnen. Wir konzentrieren uns im ersten Kapitel auf den monetär-theoretischen Kontext und schaffen damit die Grundlage, um die Motivation hinter dem Konstrukt *Bitcoin* verstehen zu können. In Kapitel 2 beginnen wir dann die eigentliche Analyse des Bitcoin-Systems. Das Kapitel dient als Grobüberblick und vermittelt ein solides Grundwissen, welches in den späteren Kapiteln vertieft wird. Die beiden Kapitel bilden den ersten Teil des Buches, der als eine allgemeine Einführung gedacht ist. Er soll Einsteiger langsam an das Thema heranführen und die benötigten Grundlagen schaffen.

Der zweite Teil des Buches besteht aus den Kapiteln 3-5. Hierbei handelt es sich um die wohl anspruchsvollsten Kapitel des Buches, welche sich vorwiegend mit der Funktionsweise und den technischen Aspekten des Systems beschäftigen. Kapitel 3 analysiert die Transaktionsfähigkeit, also die Art und Weise der Kommunikation, insbesondere in Hinblick auf Transaktionen, die zur Übertragung von Eigentumsrechten verwendet werden. Zu diesem Zweck werden wir den Aufbau und die Eigenheiten des Bitcoin-Netzwerks analysieren. Kapitel 4 widmet sich der Transaktionslegitimität. Es wird veranschaulicht wie Transaktionen zur Übertragung von Eigentumsrechten auf ihre Korrektheit überprüft werden können und inwiefern jede Person des Netzwerks selbstständig die Rechtmässigkeit einer Zahlung feststellen kann. Das Kapitel zeigt das Konzept der Pseudonyme und beinhaltet eine Einführung in die asymmetrische Kryptografie basierend auf elliptischen Kurven. In Kapitel 5 wird der Transaktionskonsens abgehandelt. Es wird aufgezeigt inwiefern die Netzwerkteilnehmer sich auf einen einzigen Registerzustand der Eigentumsrechte einigen können.

Teil 3 des Buches umfasst die Kapitel 6-8 und widmet sich spezifischen Fragestellungen und weiterführenden Applikationen. In Kapitel 6 greifen wir einige

Punkte aus dem ersten Kapitel wieder auf und versuchen eine Antwort auf die Frage zu finden, ob Bitcoin die monetären Funktionen erfüllen kann und somit in die Kategorie einer Geldeinheit fällt. In Kapitel 7 beschäftigen wir uns mit alternativen Applikationen der Bitcoin-Technologie. Wir zeigen verschiedene Möglichkeiten zum Einsatz der Blockchain. Dieses Kapitel soll einem Ausblick über mögliche Anwendungsfälle abseits des rein monetären Bereichs dienen. Das achte und letzte Kapitel umfasst einen Praxisleitfaden, der interessierte Personen an den Gebrauch der Bitcoin Einheit heranführt und ihnen den Einstieg in die Welt der Kryptowährungen erleichtern soll.

Das Buch richtet sich an Studierende und Personen aus der Akademie und Praxis, die sich gerne mit dem Thema vertraut machen möchten. Es werden die Grundlagen aller drei relevanten Disziplinen aufgearbeitet, wodurch ein umfassendes Verständnis der Technologie möglich wird. Nebst dem Lauftext ist das Buch mit vielen Anmerkungen versehen, die dem Leser, mittels Beispielen und weiterführenden Hinweisen, einen vertieften Einblick in die jeweilige Thematik bieten. Zudem wird das Buch durch Repetitionsaufgaben abgerundet, die am Ende eines jeden Kapitels gefunden werden können und eine selbstständige Überprüfung des Wissens ermöglichen. Darüber hinaus lohnt sich ein Blick auf die Webseite `www.blockchainbuch.de`, auf welcher ergänzendes Material bereitsteht.

Wir möchten uns an dieser Stelle ganz herzlich beim Förderverein des Wirtschaftswissenschaftlichen Zentrums der Universität Basel, für die finanzielle Unterstützung dieses Projekts, bedanken. Es freut uns, dass das Thema als ausdrückliches Wunschthema genannt und mit grossem Interesse verfolgt wurde. Ferner hoffen wir mit diesem Buch einen wertvollen Beitrag zur Aufarbeitung dieses komplexen Themas geleistet und eine Grundlage geschaffen zu haben, die vielen interessierten Personen aus Privatwirtschaft, Politik und Akademie den Einstieg einfacher machen wird.

Weiterer Dank gilt den folgenden Personen sowie all jenen, die uns im Entstehungsprozess dieses Buches unterstützt und begleitet haben.

Pascal Gantenbein, Brigitte Guggisberg, Raphael Mani, Matthias Mohler, Remo Nyffenegger, Edith Schär, Michèle Schnider und Joachim Setlik.

Teil I

Einführung

1 Monetär-theoretischer Kontext

Bitcoin wurde mit dem Ziel entwickelt, eine neuartige Geldeinheit zu schaffen. Wie wir im Verlaufe dieses Buches aufzeigen, gehen die möglichen Verwendungszwecke der Bitcoin-Technologie deutlich über jene einer Geldeinheit hinaus. Das Verständnis der Besonderheiten der Bitcoin-Technologie setzt jedoch eine gewisse Vertrautheit mit den Wurzeln von Bitcoin und somit mit dem Thema Geld voraus.

In der modernen Geldtheorie wird Geld als *Gedächtnis* beschrieben.[110] Der Ursprung dieser Definition beruht auf der Beobachtung, dass Menschen sich tagtäglich zahlreiche Gefälligkeiten erweisen, für die keine unmittelbare Gegenleistung erfolgt. Solche "Geschenke" werden beispielsweise innerhalb der Familie, unter Freunden oder am Arbeitsplatz unter Kollegen ausgetauscht. Das Ausüben von Hausarbeiten in den eigenen vier Wänden, die Übernahme der ungeliebten Aufgabe im Büro oder die Einladung zum nächsten Abendessen unter Freunden sind nur einige Beispiele. Tagtäglich gehen wir dutzende solcher *Gift-Giving* Beziehungen ein.[1]

Das Charakteristische an diesen Beziehungen ist, dass alle Beteiligten ihre eigene Buchhaltung der aktuellen Schuldverhältnisse führen. Die Buchhaltung wird nicht schriftlich festgehalten. Sie wird vielmehr unterbewusst im Gedächtnis der Teilnehmer geführt. Nichtsdestotrotz hat jeder Teilnehmer eine grobe Vorstellung darüber, ob der Austausch von Geschenken und Gefälligkeiten ungefähr ausgeglichen ist.

[1] Diese einleitende Diskussion über den Zusammenhang zwischen *Gift-Giving* Beziehungen, Geld und Bitcoin findet sich in ähnlicher Form auch in Berentsen (2017) [20].

Werden die Hausarbeiten immer von derselben Person erledigt, ohne dass die profitierende Person eine andere Aufgabe übernimmt, wird dies zu Diskussionen in der Beziehung führen. Muss im Büro immer dieselbe Person die ungeliebten Arbeiten des Teams übernehmen, wird dies ebenfalls für Diskussionsstoff sorgen. Sind die Einladungen zum Abendessen in einer Freundschaft sehr einseitig verteilt, wird die eingeladene Person als geizig wahrgenommen und die Freundschaft auf die Probe gestellt.

Damit ein solches System des *Gift-Giving* funktionieren kann, braucht es einen Konsensmechanismus. Die Einigung erfolgt in der Regel indem die Beteiligten miteinander sprechen und Unstimmigkeiten untereinander klären. Dabei kann es natürlich auch zu Reibereien kommen. Kann kein Konsens hergestellt werden, droht der Ausschluss aus der Beziehung.

In der Praxis sehen wir, dass der Austausch von Gefälligkeiten dann gut funktioniert, wenn sich die Teilnehmer gut kennen und die Gruppengrösse klein ist. In grösseren Gruppen funktioniert das System nicht mehr, weil es schwierig wird, einen Konsens herzustellen. Zudem finden viele Tauschbeziehungen in modernen Gesellschaften zwischen Menschen statt, welche sich überhaupt nicht kennen und sich mit grosser Wahrscheinlichkeit nie mehr begegnen werden. In solchen Gruppen wird das *Gift-Giving* durch den Austausch von Geld ersetzt. Geld übernimmt die Rolle des Gedächtnisses in komplexen Gesellschaften mit komplizierten Tauschbeziehungen. Geld führt Buch über den globalen Austausch von Gefälligkeiten. Geld ist Gedächtnis.

Ein Zahlungssystem besteht aus Regeln, welche bestimmen, wie Geld repräsentiert wird, wie es hergestellt wird und wie die Übertragung von Eigentum an den Geldeinheiten vonstattengeht. Um besser zu verstehen, wie das Bitcoin-System funktioniert, lohnt es sich, einen kurzen Blick auf klassische Zahlungssysteme zu werfen.

Beginnen wir mit dem Bargeld, also Münzen und Banknoten. Münzen und Banknoten sind physische Objekte. Das hat den grossen Vorteil, dass die Eigentumsverhältnisse immer klar definiert sind. Das Eigentum an einer Banknote oder Münze wird beim Bezahlen vom Käufer an den Verkäufer eines Gutes übertra-

gen. Dies ermöglicht den Handel zwischen Menschen, die sich nicht kennen bzw. anonym sind. Zudem ist es nicht möglich, mit der gleichen Geldeinheit mehrere Käufe zu tätigen, es braucht also keine Drittpartei, welche kontrollieren muss, ob der Käufer der rechtmässige Eigentümer der Geldeinheit ist.

Bargeld hat aber den grossen Nachteil, dass es die physische Nähe zwischen Käufer und Verkäufer voraussetzt. Die Einschränkung ist gerade mit dem Aufkommen des Internets augenfällig geworden. Zudem ist das Halten von grösseren Summen von Bargeld aus Sicherheits- und Kostengründen unattraktiv. Aus diesen Gründen ist schon bald die Idee entstanden, physisches Bargeld durch digitales Geld zu ersetzen. Im Internet würde der Käufer eine digitale Münze in Form einer Textdatei an den Verkäufer übermitteln. Das Problem dieser Idee ist, dass sich eine digitale Münze beliebig oft kopieren lässt. Dadurch könnte ein Käufer dieselbe digitale Münze an mehrere Verkäufer senden oder gar weitere Kopien für sich selbst behalten.

Das Problem der Kopien wird in der Literatur als *Double Spend* bezeichnet. Es existieren zwei Lösungen. Die erste Lösung besteht darin, dass eine zentrale Instanz damit beauftragt wird, alle elektronischen Zahlungen zu überprüfen. Dazu gehört im Speziellen die Überprüfung, dass ein Käufer der rechtmässige Besitzer der zur Zahlung verwendeten Guthaben ist. Durch das Monopolrecht an der Buchführung entsteht per Konstruktion ein unanfechtbarer Konsens. Die zweite Lösung entspricht dem Bitcoin-System, mit dem das Problem der *Double Spends* ohne eine zentrale Instanz gelöst werden kann.

Das in der Schweiz dominante Zahlungssystem beruht auf der ersten Lösung. Elektronisches Geld wird in der Schweiz *Buchgeld* oder *Giralgeld* genannt. Giralgeld ist virtuelles Geld, da es nicht in physischer Form vorkommt. Es wird durch Geschäftsbanken geschaffen, welche gleichzeitig auch die Buchführung übernehmen. Giralgeld ist ein wichtiges Zahlungsmittel, da Zahlungen heutzutage mehrheitlich elektronisch mittels Überweisung vom Konto des Käufers zum Konto des Verkäufers ausgeführt werden. Banken sind dabei für die korrekte Buchführung verantwortlich und müssen verhindern, dass ein Kunde sein elektronisches Geld mehrfach verwenden kann. Das System basiert also auf zentralen Instanzen.

Im Gegensatz dazu ist das Bitcoin-System nicht auf zentralen Instanzen aufgestützt. Jeder Teilnehmer dieses Systems kann seine eigene Buchhaltung führen. In den individuellen Buchhaltungen werden die Eigentumsrechte an allen existierenden Bitcoin Einheiten festgehalten. Damit dies funktioniert und die verschiedenen Register im Einklang sind, gibt es einen Mechanismus, der zu einem Konsens führt - ganz ähnlich wie dies beim Austausch von Gefälligkeiten innerhalb der Familie, unter Freunden oder Kollegen der Fall war. Im Unterschied zu den einfachen und subjektiven Konsensregeln beim *Gift-Giving*, garantiert das Bitcoin-System aber einen objektiven und global skalierbaren Konsens, so dass zu jedem Zeitpunkt eine Einigung über die Eigentumsverhältnisse aller Bitcoin Einheiten erzielt werden kann.

Bitcoin übernimmt also ebenfalls die Rolle des Gedächtnisses in komplexen Gesellschaften, benötigt dafür aber keine zentrale Instanz, die dieses Gedächtnis verwaltet.

Basierend auf diesem Grundgedanken erarbeiten wir im vorliegenden Kapitel die monetär-theoretischen Grundlagen und die Relevanz und Bedeutung von Bitcoin. Wir erörtern die allgemeine ökonomische Existenzberechtigung und die Funktionen von Geldeinheiten, analysieren deren Wertbestandteile und unterscheiden verschiedene Ausprägungen hinsichtlich ihrer Grundeigenschaften und Kontrollstrukturen. Dabei betrachten wir die Repräsentation, die Übertragbarkeit sowie die Schöpfung neuer Geldeinheiten und zeigen in welchen Bereichen traditionelle Geldsysteme an ihre Grenzen stossen und das Bitcoin-System neue Möglichkeiten eröffnet.

1.1 Entstehung einer Geldeinheit

Die klassische Theorie von Carl Menger[134] beschreibt die Entstehung einer Geldeinheit als einen Prozess, bei dem ein Gut mit einer hohen Marktpräsenz automatisch zum dominanten Tauschmittel wird. Die gesellschaftliche Koordination erfordert keine formale Entscheidungsfindung oder legislativen Beschlüsse, sondern kann durch die bereits präsente Nachfrage induziert werden. Weiter hält

Menger fest, dass die Dominanz eines Tauschmittels selbstverstärkend wirkt, da jeder Verkäufer ungern Güter mit einer tieferen Marktfähigkeit (Liquidität) in Zahlung nehmen wird.[2] Bei der Akzeptanz handelt es sich damit um eine klassische positive Externalität. Je mehr Marktteilnehmer ein bestimmtes Tauschmittel verwenden, desto höher ist der aus der Verwendung dieses Tauschmittels resultierende Nutzen.

Tatsächlich ist davon auszugehen, dass frühe Geldeinheiten auf diese Art entstanden sind. In unterschiedlichen Regionen und Zeitepochen wurden verschiedenste Güter und Abstraktionen als Geldeinheiten verwendet. Viele dieser frühen Vertreter haben gemein, dass sie entweder als Grundnahrungsmittel oder als (zeremonielle) Schmuckstücke dienten, wodurch ein stetiger Nachfragestrom gesichert schien.[133] Steine, Nutztiere, Walfischzähne, Muscheln, Federn und zahlreiche andere Gegenstände gehören zu einer beispielhaften Aufzählung, die keinerlei Anspruch auf Vollständigkeit erhebt.[12]

1.2 Funktionen einer Geldeinheit

Geldeinheiten erfüllen drei Funktionen (analog Abbildung 2). Als *Tauschmittel* führen sie zu einer Effizienzsteigerung im Handel und optimieren die Allokation von Gütern und Dienstleistungen. In der Funktion als *Recheneinheit* bilden sie eine universelle Referenz und erleichtern den wertmässigen Vergleich von Gütern und Dienstleistungen. Als *Wertspeicher* ermöglichen Geldeinheiten das Sparen. Die Funktionen werden nachfolgend ausführlich beschrieben.

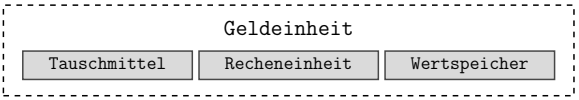


Abbildung 2: Funktionen von Geldeinheiten

[2] Der Literaturstrang basierend auf Kiyotaki und Wright (1993)[109] modelliert diesen Prozess und bildet somit einen guten Anknüpfpunkt für tiefer gehende Recherchen.

1.2.1 Tauschmittel

Tauschmittel sind unabdingbar für die Funktion einer modernen, durch weitgehende Arbeitsteilung gezeichneten Volkswirtschaft. Die Wirtschaftssubjekte sind spezialisiert und produzieren lediglich einen kleinen Teil der zum Leben notwendigen Güter selbst. Eine solche Spezialisierung ist nur möglich, wenn die restlichen Waren im Tauschhandel erworben werden können, wodurch eine arbeitsteilige Wirtschaft zwingend eine Tauschwirtschaft voraussetzt.

In einer Ökonomie ohne Geldeinheiten können Waren und Dienstleistungen ausschliesslich im direkten Austausch gehandelt werden.[3] Eine Person die einen Laib Brot besitzt, stattdessen aber lieber einen Krug Milch konsumieren möchte, müsste folglich erst eine Person finden, die einen Krug Milch besitzt und eine exakt gegensätzliche Präferenzlage aufweist. Nur dann wären beide Parteien gewillt und befähigt den Handel einzugehen. Eine einfache Übereinstimmung reicht dabei nicht aus. Ein erfolgreiches Tauschgeschäft kommt nur dann zustande, wenn die eine Partei hat, was die andere will und gleichzeitig will, was die andere hat. Durch diese, in der Fachliteratur als *doppelte Übereinstimmung der Bedürfnisse* bekannte, Problematik wird das Auffinden eines geeigneten Tauschpartners schwierig.[44] [145]

Hinzu kommt die eskalierende Zahl der möglichen Tauschpaare. Bei einer beliebigen Zahl n verschiedener Güter und Dienstleistungen, existieren $\frac{n(n-1)}{2}$ unterschiedliche Tauschpaare. In Ökonomien mit einer sehr überschaubaren Anzahl verschiedener Güter und Dienstleistungen mag der direkte Tauschhandel nur geringe Nachteile aufweisen. Wird das Wirtschaftssystem aber komplexer, so besteht es aus Milliarden von Subjekten, Gütern und Dienstleistungen. Die Suche nach geeigneten Tauschpartnern (beziehungsweise eines spezifischen Tauschpaars) zieht dann erhebliche Kosten nach sich.

Existiert hingegen ein dominantes Gut, welches vom Kollektiv allgemein akzeptiert wird, können sämtliche Geschäfte über dieses zur Geldeinheit gewordene

[3] Sollte ein etabliertes Vertrauensverhältnis bestehen und die (Geschäfts-)Beziehung eine gewisse Nachhaltigkeit aufweisen, stellt die Vergabe von Krediten eine mögliche Alternative dar. Gegenseitige Gefälligkeiten werden auf Kreditbasis vergeben, im Verlaufe der Zeit aufgerechnet und dadurch bereinigt.[85]

Gut abgewickelt werden. Alle erwünschten Güter und Dienstleistungen können dann gegen Einheiten des Tauschmittels erworben und Überschüssige für Einheiten des Tauschmittels veräussert werden. Die Existenz eines allgemein akzeptierten Tauschmittels, also einer Geldeinheit, separiert das Problem der doppelten Übereinstimmung der Bedürfnisse in zwei unabhängige Geschäfte: (An-)Kauf und Verkauf. Insofern reicht eine einfache Übereinstimmung, wobei die relevanten Tauschpaare schlagartig um den Faktor n reduziert werden, so dass lediglich $n - 1$ potentielle Paare übrig bleiben.

Die Person aus unserem Beispiel, welche Brot gegen Milch tauschen möchte, kann nun das Brot für Geldeinheiten veräussern. Mit den erhaltenen Geldeinheiten kann sie anschliessend den Krug Milch von einer beliebigen Drittperson erwerben. Die Existenz der Geldeinheit reduziert folglich die Komplexität des Problems.

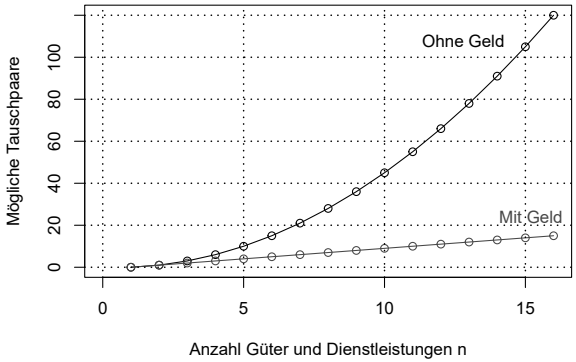


Abbildung 3: Anzahl der Tauschpaare mit und ohne Geldeinheiten

Abbildung 3 zeigt den Unterschied bezüglich der Anzahl an möglichen Tauschpaaren in Ökonomien mit und ohne Geldeinheiten (Tauschmittel). Das Diagramm veranschaulicht, wie die Zahl der potentiellen Tauschpaare selbst bei einer

geringen Gütermenge eskaliert und wie die Differenz der möglichen Tauschpaare von monetären und nicht-monetären Ökonomien mit zunehmender Komplexität grösser wird.[4]

1.2.2 Recheneinheit

Eine Recheneinheit ermöglicht den Wert aller Güter und Dienstleistungen in Einheiten derselben Bezugsgrösse auszudrücken und auf diese Weise vergleichbar zu machen. Dadurch wird die Informationsmenge, welche eine umfassende Marktübersicht erfordert, erheblich geringer. Anstatt sich die jeweiligen Tauschverhältnisse von $\frac{n(n-1)}{2}$ Tauschpaaren einprägen und dynamisch anpassen zu müssen, schaffen Geldeinheiten eine universelle Referenz zur Bewertung unterschiedlicher Leistungen. Denn wird der Preis aller Güter und Dienstleistungen in Geldeinheiten ausgedrückt, genügt ein einziger Geld-Gegenwert pro Gut (also $n-1$). Diese Erleichterung sorgt für mehr Transparenz auf dem Markt und reduziert dadurch die Such- und Transaktionskosten der Handelstätigkeit.

Meist vereinen Geldeinheiten die Funktion des Tauschmittels mit jener der Recheneinheit. Grundsätzlich lassen sich die beiden Funktionen aber ohne weiteres trennen (siehe Anmerkung 1.1).

[4] Eine zunehmende ökonomische Spezialisierung und Vielfalt erhöht die Komplexität des Tauschhandels und die damit einhergehenden Transaktionskosten. Höhere Transaktionskosten führen wiederum zu einem grösseren Einsparungspotential und begünstigen den Siegeszug eines allgemein akzeptierten Tauschmittels. Umgekehrt-relational kann argumentiert werden, dass ein allgemein akzeptiertes Tauschmittel die ökonomische Spezialisierung vorantrieb oder gar erst ermöglicht hat. Obwohl die Richtung einer kausalen Abhängigkeit der beiden Ereignisse nicht klar auszumachen ist, steht fest, dass die beiden ökonomischen Grundpfeiler eng miteinander verknüpft sind und in einer positiv korrelativen Beziehung stehen.[120]

Anmerkung 1.1

Ausgelagerte Recheneinheit

In den meisten Ökonomien übernehmen Geldeinheiten die Funktion der Recheneinheit. Geldeinheiten müssen diese Funktion jedoch nicht zwingend erfüllen. Tatsächlich zeigen einige historische Beispiele, dass die Funktion vollständig von der eigentlichen Geldeinheit losgelöst und stattdessen eine alternative Recheneinheit genutzt werden kann.

Im Mittelalter hat die Vielfalt verschiedener Münzen und die ständige Veränderungen von deren Edelmetallgehalt[a] dazu geführt, dass zumeist in den Standardeinheiten Pfund, Schilling und Pence gerechnet wurde, wobei ein Pfund 20 Schilling bzw. 240 Pence entsprach. Dadurch war es möglich, einen universellen Preis zu verwenden und Wertveränderungen spezifischer Münzen, ohne Anpassung der ausgewiesenen Warenpreise zu berücksichtigen.[112]

Auch heutzutage existieren noch Beispiele, bei denen die Funktion der Recheneinheit von der Geldeinheit abgespalten wurde. Die *Unidad De Fomento* in Chile (CLF) ist ein inflationsbereinigter nationaler Preisindex, der tagesaktuell gegenüber der Landeswährung (Peso) bestimmt und veröffentlicht wird. Die Ladenpreise in Chile werden primär in CLF ausgedrückt und sollten daher unabhängig vom Wertverlauf des Pesos stabil bleiben. Dadurch können administrative Kosten von Preisanpassungen (*Menükosten*) verhindert werden, während lediglich ein einziger Wechselkurs hinzu kommt.[111]

[a] Münzen wurden gefeilt, geknipst und Metalle durch Säurebäder abgelöst. Gelegentlich wurden Münzen gar von offizieller Seite rückbeordert und mit einem geringeren Edelmetallgehalt geprägt.

1.2.3 Wertspeicher

Die Wertspeicherfunktion ermöglicht das Sparen. Konkret bedeutet Sparen, dass Geld nicht unmittelbar gegen Güter und Dienstleistungen getauscht werden muss. Stattdessen können Geldeinheiten beiseite gelegt und ihre Kaufkraft zu einem

späteren Zeitpunkt ausgeübt werden. Dies erlaubt eine Konsumglättung und eine Absicherung gegen unerwartete Auslagen. Zudem ermöglichen derartige Rücklagen grössere Investitionen.

Ein Tauschmittel ist immer auch ein Wertaufbewahrungsmittel. Umgekehrt gibt es viele Wertaufbewahrungsmittel (Vermögensanlagen), welche nicht als liquides Tauschmittel verwendet werden.

1.3 Monetäre Grundeigenschaften

Um die drei Funktionen aus Abschnitt 1.2 erfüllen zu können, sollten Geldeinheiten haltbar, transferierbar, teilbar, homogen und verifizierbar sein sowie eine gewisse Wertstabilität aufweisen. Des Weiteren muss die Zahl der sich im Umlauf befindlichen Einheiten zwingend einer Beschränkung unterliegen. Abhängig von diesen sieben Grundeigenschaften können die drei Funktionen aus Abschnitt 1.2 unterschiedlich gut erfüllt werden.

Haltbarkeit. Die Verwendung als *Tauschmittel* und *Wertspeicher* bedingt Haltbarkeit. Verderbliche oder empfindliche Güter eignen sich weder als langfristige Anlage, noch für den Tauschhandel. Dasselbe gilt auch für Güter, die nur schwer gelagert werden können und dabei hohe Kosten verursachen.

Transferierbarkeit. Damit ein Gut als *Tauschmittel* in Frage kommt, muss die Übertragung der Eigentumsrechte ohne grössere Hürden und Kosten möglich sein.[5] Auch für die Funktion als *Wertspeicher* ist die Transferierbarkeit von Bedeutung, da eine Wertanlage nur dann Sinn macht, wenn sie zu einem späteren Zeitpunkt wieder liquidiert werden kann.

Teilbarkeit. Die Funktion als *Tauschmittel* setzt voraus, dass die Geldeinheit (oder ein Bruchteil davon) gegen beliebige Güter und Dienstleistungen eingetauscht werden kann. Folglich muss Geld entweder teilbar sein oder in entsprechend kleinen Stückelungen zur Verfügung stehen.[6]

[5] Im Falle einer physischen Geldeinheit umfasst dies die örtliche Beweglichkeit des Objekts.
[6] Das Problem der Nicht-Teilbarkeit wird modelliert in Berentsen und Rocheteau (2002).[22]

Homogenität. Geldeinheiten (mit demselben Nennwert) müssen homogen, also untereinander vertret- beziehungsweise austauschbar, sein. Nicht-homogene Güter weisen Unterschiede (Heterogenität) auf und erfordern bei jedem Tauschhandel eine individuelle Bewertung, die hohe Transaktionskosten zur Folge hat und den eigentlichen Zweck eines *Tauschmittels* verfehlt. Wein wäre beispielsweise eine schlechte Wahl, da die Qualitätsunterschiede immens und die Flaschen somit nicht homogen sind.

Verifizierbarkeit. Sowohl die Funktion des *Tauschmittels* als auch jene des *Wertspeichers* setzen voraus, dass die Authentizität der Einheiten verifiziert und eine Fälschung identifiziert werden kann.

Wertstabilität. *Wertspeicher* und *Recheneinheit* bauen auf eine gewisse Stabilität der Kaufkraft des Gutes. Insofern darf keine übermässige Volatilität beziehungsweise auseinanderdriftende Entwicklung von Angebot und Nachfrage bestehen. Güter mit hohen saisonalen und zufallsbedingten Angebotsschwankungen (beispielsweise Agrarprodukte) sind wenig geeignet.

Seltenheit. Ein beschränktes Vorkommen limitiert das Angebot des Gutes und ist die Grundlage für dessen Verwendung als *Tauschmittel*. Kommt ein Gut in unbeschränkter Menge vor, gibt es keinen Grund dieses zu handeln. Das Ausbleiben der Handelstätigkeit untergräbt auch dessen Funktion als *Wertspeicher*.

1.4 Monetärer Gegenwert

Der Wert von Geldeinheiten basiert auf verschiedenen Grundlagen. Konkret entsteht der Marktwert durch eine Kombination von Fundamentalwert, Zahlungsversprechen und einer Liquiditäts- und Spekulationsprämie (siehe Tabelle 1).

Der *Fundamentalwert* umfasst den stofflichen Eigenwert des Objekts. Er entspringt dem Nutzen, der aus dem Konsum oder dem Besitz der Ware resultiert, und ist in keiner Weise von der monetären Funktion des Gutes abhängig.

Zahlungsversprechen sind Wertkomponenten, die nicht stofflich an die Geldeinheit gebunden sind. Im Unterschied zum Fundamentalwert unterliegt dieser Wertbestandteil einem Emittentenrisiko. Kann oder will die garantierende Instanz eine Verbindlichkeit nicht erfüllen, entfällt dieser Wertbestandteil komplett.

Liquiditäts- und Spekulationsprämien werden oftmals unter dem Begriff Blasenkomponente zusammengefasst. Im Wesentlichen handelt es sich um zwei Optionen: Die Option auf den flexiblen Tausch der Geldeinheit in beliebige Güter und Dienstleistungen (Liquiditätswert) und die Option auf Gewinn bei einem allfälligen Wertanstieg (Spekulationswert). Beide Optionen haben einen gewissen Wert, der sich zumeist positiv auf den Marktwert der Geldeinheit auswirken wird.

	Fundamentalwert
+	Zahlungsversprechen
+	Liquiditäts- und Spekulationsprämie
=	Marktwert der Geldeinheit

Tabelle 1: Wertbestandteile einer Geldeinheit

Diese drei Wertbestandteile bilden die Basis für verschiedene Typen von Geldeinheiten analog Tabelle 2. Abhängig von der Kombination der Bestandteile des Marktwertes können Geldeinheiten den Kategorien Warengeld, Kreditgeld und Fiatgeld zugeordnet werden.

	Fundamental	Versprechen	Prämie
Warengeld	+		(+)
Kreditgeld		+	(+)
Fiatgeld			+

Tabelle 2: Geldtypen nach Wertbestandteilen

1.4.1 Warengeld

Warengeld hat einen stofflichen Fundamentalwert und kann eine Liquiditäts- und Spekulationsprämie enthalten. Durch diese Zusatzkomponente kann der Marktwert über dem Fundamentalwert liegen. Der Fundamentalwert bildet dabei die tiefstmögliche Wertschwelle, die selbst dann nicht unterschritten werden kann, wenn die Ware ihre Funktion als Geldeinheit verliert. Denn auch in diesem Fall könnte das Gut noch als Ware verwendet, beziehungsweise konsumiert oder in den Produktionsprozess eingebunden werden.

Einige Beispiele von Warengeld umfassen Muschelgeld in Afrika und China, Ringe und Schmuckstücke in Neu-Guinea und im Süd-Pazifik, Kleidergeld (Pelze) in Nordamerika und Metallgeld in vielen anderen Regionen der Welt. Auch Vieh und Grundnahrungsmittel wurden häufig als Warengeld verwendet.

1.4.2 Kreditgeld

Kreditgeld ist ein Zahlungsversprechen und besitzt keinen Fundamentalwert. In der Regel ist es ein Stück Papier oder ein digitaler Eintrag welcher besagt, dass der Emittent zu einem bestimmten, in der Zukunft liegenden Zeitpunkt eine Zahlung tätigen wird. In der englischen Sprache wird ein solches Zahlungsversprechen IOU ("I owe you" dt. "Ich schulde dir/Ihnen") genannt.

Grundsätzlich können Zahlungsversprechen beliebige Formen annehmen. Zum Beispiel: "ich schulde Person x eine Kuh auf den 1. Juli 2090" oder "ich schulde Person x eine Schlittenfahrt auf den 30. Januar 2020". Zumeist wird die Verbindlichkeit aber in der jeweiligen Landeswährung ausgedrückt.

Für den Marktwert eines Zahlungsversprechens spielt das Ausfallrisiko eine wesentliche Rolle. Insofern muss die Reputation des Emittenten berücksichtigt werden, so dass ein Versprechen über die Auslieferung einer Unze Gold von Person A, einen komplett anderen Marktwert aufweisen kann, als dasselbe Versprechen von Person B.

Zahlungsversprechen werden dann zu Geld, wenn sie allgemein akzeptiert und in Zahlung genommen werden. Hat ein Emittent einen besonders guten Ruf, können seine Zahlungsversprechen frei zirkulieren.

Anmerkung 1.2

Ursprünge des Papiergeldes

Frühe Vertreter des Papiergeldes entsprachen solchen Zahlungsversprechen, da sie durch reale Gegenwerte (in der Regel Gold) besichert waren. Sie beinhalteten das Versprechen auf Konvertierbarkeit in eine zuvor festgehaltene Edelmetallmenge.[a] Der Kreditcharakter dieser Scheine wird insbesondere dann klar, wenn man deren Herkunft betrachtet. Die ersten Geldscheine entstanden in China während der Tang Dynastie (618-907 nach Christus) als eine von privater Seite ausgestellte Kreditvereinbarung. Abhängig von Reputation und Bonität des ausstellenden Schuldners konnte dieses Papier zirkulieren und als monetäres Substitut für die gängigen *Kai Yuan* Bronzemünzen-Ketten dienen.[35]

[a] Beziehungsweise in andere Waren.

Kreditgeld ist nicht auf die Anknüpfung realer Gegenwerte beschränkt. Zahlungsversprechen über die Auslieferung von Fiatgeld sind nicht bloss denkbar sondern geläufig. Giralgeld ist grundsätzlich nichts anderes als ein bankenseitiges Versprechen, das Geld zu jeder Zeit (auf Sicht) in gesetzliche (Fiat-) Zahlungsmittel einzutauschen.

Analog allen anderen Geldtypen kann auch Kreditgeld eine zusätzliche Liquiditäts- und Spekulationsprämie beinhalten. Die Liquiditätsprämie kann dazu führen, dass der Marktwert von Kreditgeld grösser ist, als der Marktwert der angeknüpften Verbindlichkeit.

1.4.3 Fiatgeld

Der Ausdruck Fiatgeld hat seinen Ursprung im lateinischen *Fiat-Lux* (es werde Licht). Er verbildlicht die Tatsache, dass Fiatgeld weder über einen Fundamentalwert verfügt, noch ein Zahlungsversprechen beinhaltet und somit gewissermassen aus dem Nichts entsteht (es werde Geld). Tatsächlich stellt die Liquiditäts- und Spekulationsprämie die einzige Wertkomponente dar. Der Marktwert von Fiatgeld basiert ausschliesslich auf Zukunftserwartungen und kann bei einem Wegfall der monetären Funktion auf null fallen.

Landeswährungen, wie der US Dollar, der Euro oder der Schweizer Franken, gehören in die Kategorie des Fiatgeldes. Die Geldscheine können weder konsumiert noch in einen Produktionsprozess eingebunden werden und sind nicht durch Gold oder andere fundamental wertvolle Güter besichert. Die Wertstabilität wird einzig und allein durch die Zentralbanken garantiert, welche die jeweilige Geldeinheit exklusiv emittieren und den gesetzlichen Auftrag haben, diese stabil zu halten.

In der Schweiz und vielen anderen Ländern sind Banknoten, und in einem gewissen Umfang auch Münzen, gesetzliche Zahlungsmittel. In Artikel 3 des *Bundesgesetzes über die Währung und die Zahlungsmittel* wird ein Annahmezwang festgehalten, mit der Konsequenz, dass Einheiten der Landeswährung stets zur Tilgung ausstehender Schulden verwendet werden können.[175] Diese gesetzliche Grundlage sichert einen gewissen Nachfragestrom und begünstigt die Liquiditäts- und Spekulationsprämie der Geldeinheit. Des Weiteren kann die staatliche Stütze stabilisierend auf eine grundsätzlich sehr volatile Geldkategorie einwirken.

Fiatgeld ist ein relativ junges Phänomen. Bis in die 1970er Jahre hatte das Papiergeld in den meisten Ländern eine implizite oder explizite Golddeckung und somit eine angeknüpfte Verbindlichkeit (Kreditgeld). Durch den Wegfall dieser Verbindlichkeit und den vernachlässigbaren stofflichen Eigenwert eines Papierscheines entstand die Kategorie der ungedeckten Fiatgelder.[7]

[7] Wie wir später sehen werden gehört auch Bitcoin in diese Kategorie. Eine ausführliche Abhandlung der Frage weshalb Bitcoin als Fiatgeld bezeichnet werden muss, folgt in Anmerkung 2.6 auf Seite 80.

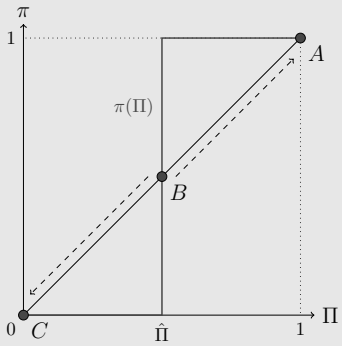
Anmerkung 1.3

Akzeptanz einer Fiatgeldeinheit als Koordinationsspiel

Fiatgeldeinheiten verfügen weder über einen Fundamentalwert, noch weisen sie angeknüpfte Verbindlichkeiten auf. Ihr Wert basiert ausschliesslich auf den Erwartungen hinsichtlich der zukünftigen Akzeptanz und Absatzfähigkeit (Liquiditäts- und Spekulationsprämie).

Je höher die Wahrscheinlichkeit, auf einen anderen Marktteilnehmer zu treffen, der die Fiatgeldeinheit in Zahlung nehmen wird, desto eher ist eine Person gewillt, ihrerseits eine solche Geldeinheit zu akzeptieren.

Dieser Sachverhalt wird in der folgenden Grafik veranschaulicht. Angenommen Π repräsentiert die Wahrscheinlichkeit, dass ein zukünftiger Tauschpartner die Geldeinheit in Zahlung nehmen wird und π ist unsere eigene Akzeptanzwahrscheinlichkeit. Die Funktion $\pi = \pi(\Pi)$ stellt dabei unsere beste Antwort auf eine gegebene Erwartung bezüglich der Ausprägung von Π dar.



Jeder Schnittpunkt von $\pi(\Pi)$ mit der 45° Linie entspricht einem Nash Gleichgewicht. Es gibt exakt drei solche Nash Gleichgewichte: A, B und C. Die beiden äusseren Gleichgewichte repräsentieren Situationen in denen nie-

mand (C) oder aber alle (A) Marktteilnehmer bereit sind, die Geldeinheit zu akzeptieren. Ein drittes Gleichgewicht (B) entsteht bei einem Schwellenwert $\hat{\Pi}$. Oberhalb dieses Wertes agieren selbstverstärkende Kräfte, welche die Ökonomie in das monetäre Gleichgewicht bringen. Liegt die Wahrscheinlichkeit unterhalb von $\hat{\Pi}$, wird die Akzeptanz dahinschwinden und schliesslich vollständig verloren gehen. Situationen mit diesen Charakteristiken werden in der Mikroökonomie (genauer Spieltheorie) auch als Koordinationsspiele bezeichnet.[19]

1.5 Monetäre Kontrollstrukturen

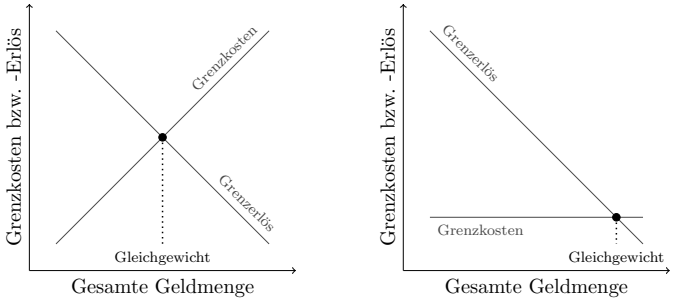
Geldeinheiten weisen unterschiedliche Kontrollstrukturen auf, welche grob in drei Dimensionen eingefangen werden können: *Schöpfung*, *Repräsentation* und *Transaktionsabwicklung*.

Die Schöpfung beschreibt die Art und Weise wie neue Geldeinheiten des jeweiligen Typs erstellt werden können. Dies hat wichtige Implikationen für die Geldmengensteuerung und somit auch für die Seltenheit und den Wert der entsprechenden Einheit. Die Repräsentation zeigt, ob der Wert einer Geldeinheit an ein physisches Objekt gebunden ist oder lediglich als virtuelle Abstraktion gehandelt wird. Die Transaktionsabwicklung beschreibt, ob die Übertragung einer Geldeinheit autonom und dezentral durchgeführt werden kann oder ob diese der Verarbeitung durch eine zentrale Instanz bedarf.

1.5.1 Geldschöpfung

Geldeinheiten müssen mengenmässig beschränkt werden, so dass sie eine gewisse *Seltenheit* aufweisen. Wäre eine Geldeinheit in uneingeschränktem Masse verfügbar, würde für diese Geldeinheit keine Zahlungsbereitschaft bestehen und der Gegenwert auf ein Minimum sinken. Die Seltenheit wird normalerweise über den Geldschöpfungsprozess erreicht, welcher entweder kompetitiv oder monopolisiert erfolgen kann.

Bei der kompetitiven Schöpfung kann jedes Wirtschaftssubjekt neue Geldeinheiten erstellen. Jedes Individuum wird selbstständig und aus purem Eigeninteresse abwägen, ob eine neue Geldeinheit die aus der Produktion entstehenden Kosten rechtfertigt. Ein Wirtschaftssubjekt hat einen Anreiz neue Geldeinheiten herzustellen, bis die Produktionskosten einer weiteren Geldeinheit (Grenzkosten) dem derzeitigen Marktpreis dieser Geldeinheit (Grenzerlös) entsprechen - in anderen Worten: Die Herstellung wird fortgeführt, solange der Herstellungsprozess einen positiven Ertrag abwirft.



(a) Steigende Grenzkosten (b) Konstante Grenzkosten

Abbildung 4: Kompetitive Geldschöpfung

Eine kompetitive Schöpfung bedingt eine technologische Limitierung, welche den Schöpfungsprozess in ein Gleichgewicht bringt. Abbildung 4a stellt diesen Zusammenhang schematisch dar und visualisiert das Gleichgewicht, welches sich am Schnittpunkt von Grenzkosten und Grenzerlös befindet. Die negative Steigung der Grenzerlöskurve ist darauf zurückzuführen, dass eine grössere Gesamtmenge (bei gleichbleibender Nachfrage), zu einem geringeren Marktwert der Geldeinheit führt und somit den Grenzerlös mindert. Die positive Steigung der Grenzkosten basiert auf der Annahme, dass die Herstellung der Geldeinheiten bestimmter Ressourcen oder Produktionsfaktoren bedarf, welche zunehmend seltener und somit kostspieliger werden. Dadurch steigen die Kosten für die Produktion einer weiteren Einheit mit der Ausdehnung der Geldmenge an.

Ein klassisches Beispiel der kompetitiven Schöpfung stellt das Schürfen von Gold dar. Grundsätzlich kann jedes Individuum diese Tätigkeit ausüben und neues Gold in den Umlauf bringen. Individuen werden dieser Beschäftigung aber nur solange nachgehen, wie sich die Anstrengungen bezahlt machen. Je mehr Gold bereits geschürft wurde, desto schwieriger und somit kostenintensiver wird dieser Prozess. Gleichzeitig führt eine Ausdehnung des Angebots - ceteris paribus - zu sinkenden Goldpreisen, so dass mit jeder weiteren Einheit Gold die Grenzkosten zu- und der Grenzerlös abnehmen werden. Ab einer bestimmten Menge übersteigen die Grenzkosten der Produktion einer weiteren Goldeinheit den Gegenwert dieser Goldeinheit, so dass die Schöpfung eingestellt wird.

Tiefe, konstante Grenzkosten analog Abbildung 4b führen hingegen dazu, dass grosse Mengen der Geldeinheit geschöpft werden. Sind die Grenzkosten gar komplett vernachlässigbar (Fiatgeld), haben Individuen solange einen Anreiz neue Geldeinheiten zu schöpfen, bis der Marktpreis dieser Geldeinheiten auf 0 fällt.

Um dies zu verhindern, muss in solchen Fällen eine künstliche Limitierung erfolgen, indem das Schöpfungsrecht restringiert oder monopolisiert wird. Normalerweise wird eine (halb-)staatliche Institution mit der Aufgabe betraut, exklusiv die nationale Währung auszugeben und zu verwalten. Es besteht aber auch die Möglichkeit, dieses Monopolrecht zu privatisieren.[21] Durch die Exklusivität der Schöpfung können die Herstellungskosten der Geldeinheiten unter dem aktuellen Marktpreis gehalten werden, da keine anderen Akteure existieren, welche ihrerseits in die Produktion eingreifen und Seigniorage-Erträge abschöpfen könnten.

Die monopolisierte Schöpfung wird in Abbildung 5 schematisch dargestellt. Der geldschöpfende Monopolist kann frei über die Menge und den theoretischen Marktpreis der Geldeinheit verfügen. Es ist ihm möglich, selbst bei tiefen, konstanten Grenzkosten, die Schöpfung freiwillig so zu beschränken, dass eine Geldeinheit mit einem positiven Gegenwert entsteht.

Als anschauliches Beispiel der monopolisierten Schöpfung bietet sich die Produktion des physischen Schweizer Frankens an. Die Schweizerische Nationalbank hat die exklusive Berechtigung zur Herstellung der Banknoten und ist dadurch im Besitz eines Schöpfungsmonopols. Die Herstellungskosten einer Banknote betra-

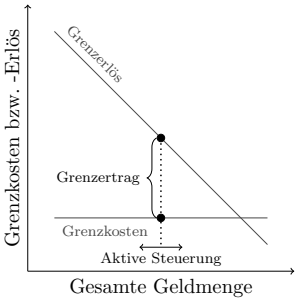


Abbildung 5: Monopolisierte Schöpfung mit konstanten Grenzkosten

gen durchschnittlich 30 Rappen.[38] Der Kostenvorteil der monopolisierten Geldschöpfung ist somit enorm. Im Falle des Einhundert Franken Geldscheins müssen lediglich 0.3% des realen Wertes des Tauschmittels für dessen Produktion aufgewendet werden. Bei der kompetitiven Schöpfung würde der Markt aufgrund dieser Tatsache solange mit Geldscheinen geflutet werden, bis der Wert eines Scheines bei den Kosten der Produktion läge, was einem Kostenpunkt von 100% des angestrebten Tauschmittel-Gegenwertes entsprechen würde. Es müssten also weitaus mehr Ressourcen für die Bereitstellung eines gegebenen Gegenwertes an Tauschmitteln aufgegeben werden. Gesellschaftlich betrachtet führt dies zu einer ineffizienten Allokation von Ressourcen und einer gewissen Effizienzüberlegenheit des monopolisierten Schöpfungsprozesses.[8]

Anmerkung 1.4

Relative Produktionskosten von Geldeinheiten

In der nachfolgenden Tabelle stellen wir beispielhaft die Kosten der Geldschöpfung des Schweizer Frankens dar. Die Daten umfassen die Kosten für die Entwicklung und die Produktion und gehen auf eine Auskunft des Bundesrates von 2013 zurück.[38] Die erste Tabellenspalte zeigt die Stückelung in CHF,

[8] Bitcoin steht häufig in der Kritik für seine Anwendung der kompetitiven Schöpfung. Siehe dazu Anmerkung 5.1 auf Seite 213.