Forschungsprojekt

Kritische Analyse der Erfolgsfaktoren von Bitcoin zur Verwendung in der Realwirtschaft

angefertigt an der Hochschule Harz
Fachbereich Wirtschaftswissenschaften
Studiengang F.A.C.T.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BC - Blockchain

BTC - Bitcoin (auch als informeller Währungscode genutzt)

DLT - Distributed Ledger Technology

PoW - Proof of Work

P2P - Peer-to-Peer

Nonce - Used only once

KW - Kryptowährungen

1 Einleitung

1.1 Relevanz des Themas

Damit ein Wirtschaftssystem arbeiten und Handel betreiben kann benötigt es damals wie heute ein Tauschmittel. Vor rund 3.500 Jahren bestanden die ersten Tauschmittel, die als Währung anerkannt wurden, aus kostbaren und seltenen Objekten. Überall auf der Welt entstanden verschiedene Tauschmittel: Wer in China eine Kuh kaufen wollte, konnte mit Kauri (seltenen weißen Muscheln) zahlen. In Afrika wurden Salzbarren, in Südamerika Kakaobohnen, auf den Fidschiinseln im Pazifik Walzähne, in Russland zu flachen Ziegeln gepresster Tee als Währung anerkannt. Im Laufe der Jahrhunderte wurde dieses Naturalgeld aufgrund der besseren Handel-, Transportierbarkeit und gleichen Beschaffenheit durch unser heutiges Münzgeld abgelöst.[1]

Am Anfang des 17. Jahrhunderts erwies sich das Transportieren von Edelmetallen als unpraktisch und barg Gefahren des Verlustes durch Diebstahl oder Raub. Deshalb gingen Banken dazu über für das eingelagerte Gold Schuldscheine in Form von Papier auszustellen. Dabei entsprach der Wert der Schuldscheine exakt dem Wert, die eine Person bei der Bank eingelagert hatte. Das grundlegende Vertrauen in das Bankensystem bildete dabei die Basis, um einen "wertlosen" Schuldschein aus Papier als Zahlungsmittel für das hinterlegte Gold anzuerkennen.[2] Die Golddeckung galt seitdem bis etwa 1914 weltweit. Aufgrund der Vorherrschaft des britischen Empire, war die Goldwährung international handelbar, akzeptiert und anerkannt. Eine Unze Gold entsprach dabei exakt 3 Pfund, 17 Shilling und 9 Pence, wodurch sich ein fester Wechselkurs ergab. Zudem änderte sich dieser Wert im Verlauf der Jahrhunderte nicht. Der Wert des Geldes resultierte somit aus der vorhanden Menge an Gold.[3] Damit sich eine Regierung an der Spitze behaupten kann braucht es zum Regieren die nötigen finanziellen Mittel um z.B. Kriege zu führen oder Konjunkturprogramme aufzulegen.

[1] Vgl.: o.V.: Harzsparkasse - Praktikum_Präsentation_JAV, S. 3.
[2] Vgl.: Borchert, M.: (2003), S.23.
[3] Vgl.: Müller, D.: (2010), S.51.

Die Regierungen bemerkten daher recht schnell, dass die Wahrscheinlichkeit das alle Gläubiger gleichzeitig ihre Schuldscheine einlösen sehr gering war. Aufgrund dieser Tatsache, wurde die Golddeckung zuerst verwässert und schließlich im Jahre 1971 mit der Abkopplung des US-Dollars vom Gold vollkommen aufgehoben.[4] Diese Abkopplung hatte eher politische anstelle von ökonomischen Gründen. Das Interesse von Regierungen ist primär eher ein Instrument zu besitzen, mit dem es möglich ist nach aktueller Interessenlage die Geldmenge und den Geldwert verändern zu können. Heutzutage wird dies als Geldpolitik bezeichnet. Alle weltweiten Währungen ob US-Dollar, Euro, britisches Pfund, chinesischer Renminbi oder russischer Rubel zählen heutzutage zu dem sogenannten Fiat-Geld.[5] Definiert ist Fiat-Geld als eine Währung ohne inneren bzw. festen Wert besitzt und wird nur durch gesetzliche Bestimmung als geltendes Zahlungsmittel festgelegt.[6] Diese Abkopplung vom Goldstandard führte dazu, dass in der Theorie somit unbegrenzt Geld aus dem quasi "nichts" durch die Regierungen geschaffen werden kann. Die Aufsicht über diesen Prozess haben die staatlichen Zentralbanken. De Facto hat eine Regierung weitestgehend alleinige Entscheidungsgewalt in Bezug auf die Schöpfung, Menge und Umlauf von Geld. Durch diese Maßnahmen wurde Geld das erste Mal in der Geschichte zentralisiert.[7] Womit die Hinterlegung und Deckung durch ein Edelmetall für alle Währungen nicht mehr garantiert ist. Am erkennbarsten und zugleich makabersten ist dies am Beispiel des US-Dollar ablesbar. Auf der aktuellen US-Dollar-Note steht nur noch ein Satz: "In God we trust".[8]

Daher ist die existenzielle Voraussetzung einer jeden Währung, um als Zahlungsmittel anerkannt zu werden, immer das Vertrauen der Marktteilnehmer. Was passiert aber wenn das Vertrauen in die Währung oder "Gott" nicht mehr gegeben ist?

Bereits Henry Ford, Gründer der Ford Motor Company, erkannte diesen Zusammenhang indem er sagte:

"Würden die Menschen das Geldsystem verstehen, hätten wir eine Revolution noch vor morgen früh."[9]

[4] Vgl.: Wolff, E.: (2017), S.163.
[5] Vgl.: Polleit, T.: Gold ist die bessere Währung, 2017, 11.03.2020 [Online].
[6] Vgl.: o.V.: CAPinside - Was bitte sind FIAT-Währungen ?, 2018, 11.03.2020, [Online].
[7] Vgl.: Hosp, J.: (2017), S.33-36.
[8] Vgl. Müller, D.: (2010), S.54.

Der Impuls zum Hinterfragen und Umdenken kam allerdings erst mit der Finanzkrise in 2008 und der daraus resultierenden Weltwirtschaftskrise. Die Menschen wachten langsam auf und vertrauten dem althergebrachten Finanzwesen nicht mehr blindlings. Das Vertrauen der Menschen in das Bankensystem war durch die tiefgründigen Einschnitte im normalen Alltag tief erschüttert und sie fingen somit an das bestehende Finanzsystem zunehmend in Frage zu stellen und nach alternativen Lösungswegen zu suchen.[10]
Eine Lösung um sich von den zentralisierten Kontrollstellen abzukoppeln, sah bereits 1999 der angesehene Wirtschaftswissenschaftler Milton Friedmann in seinem legendären Interview, indem er sagte:

"I think that the Internet is going to be one of the major forces for reducing the role of the government. The one thing that's missing, but that will soon be developed, is a reliable e-cash."[11]

Bis zur Realisierung seiner Aussage vergingen allerdings noch knapp 10 Jahre. Erst durch die Möglichkeiten der Digitalisierung war es möglich ein System zu erschaffen, dass die Nachteile einer zentralisierten Währung abschaffen konnte ohne jedoch die Vorteile zu verlieren. Diese Adaption der Funktionen eines dezentralisierten Systems erlaubten es einer Währung, wie den Bitcoin und der zugrundliegenden Blockchain (BC) Technology als Gegenwicht zu den Fiat-Währungen seinen Platz im Finanzsystem zu finden.[12] Diese Dezentralisierung war der Schlüssel zum Durchbruch für Kryptowährungen (KW) um das existenzielle Vertrauen der Nutzer zu gewinnen.

Währungen, wie der Bitcoin die langfristig erfolgreich seien wollen, müssen daher aufgrund der hohen Relevanz des Themas einen geeigneten Weg finden zwischen der Akzeptanz in der Realwirtschaft und der Beibehaltung eines dezentralen Systems.

[9] Zitat von Henry Ford (*1947), amerikanischer Industrieller
[10] Vgl.: David Lee, K.: (2015), S.XXi.
[11] Zitat von Milton Friedman (*2006), US-amerikanischer Wirtschaftswissenschaftler
[12] Vgl.: Nguyen, L.: (2018), S.6.

1.2 Zielsetzung der Arbeit und Forschungsfrage

Das Ziel des vorliegenden Forschungsprojektes ist es, die Erfolgsfaktoren für Verwendung von Bitcoins in der Realwirtschaft herauszuarbeiten, zu analysieren und herkömmlichen Währungen gegenüberzustellen.
Dafür ist das vorliegende Forschungsprojekt in 5 Hauptabschnitte gegliedert. Im ersten Abschnitt findet sich die Einleitung und die Relevanz für die Realwirtschaft wieder. Im zweiten Abschnitt erfolgt die theoretische Auseinandersetzung mit den klassischen Zahlungsmethoden und Geldcharakteristiken. Dabei werden die Hauptfunktionen und Eigenschaften herausgearbeitet. Anschließend wird in Kapitel 3 die Entstehung und Entwicklung des Bitcoins näher betrachtet. Dieser Grundlagenteil hat das Ziel ein Verständnis von digitalen Währungen, der BC Technologie und deren Funktionsweise zu erzeugen. Diese innovative Technologie ist der Treiber hinter den KW.
Nach eingehender Betrachtung der theoretischen und technischen Entwicklung befasst sich Kapitel 4 mit der Gegenüberstellung von klassischen und kryptischen Zahlungsmethoden in Form von Bitcoin und deren Verwendung in der Realwirtschaft. Die zentrale Forschungsfrage lautet daher:

- Welche Erfolgsfaktoren von Bitcoin können identifiziert werden und welche Anwendungsmöglichkeiten ergeben sich daraus in der Realwirtschaft?

Die einzelnen Erfolgsfaktoren werden hierbei mittels eines Chancen-/ Risikoanalyse herausgearbeitet und anschließend mit den in Kapitel 2 dargestellten Eigenschaften von Geld verglichen. Zudem soll anhand der Erfolgsfaktoren in Abschnitt 4.3.1 aufgezeigt werden, welche Branchen besonders stark von der Verwendung in der Realwirtschaft profitieren.
Die aus der Untersuchung gewonnen Erkenntnisse werden in Verbindung mit den theoretischen Kenntnissen verknüpft und abschließend in Kapitel 5 eruiert und kritisch gewürdigt.

1.3 Kritische Würdigung der Literatur

Das Thema der Forschung ist sehr aktuell, wodurch die zur Verfügung stehende Literatur nur in eingeschränkten Umfang zur Verfügung steht. Zurzeit existieren nur wenige wissenschaftliche Studien oder Ausarbeitungen. Diese Tendenz hat sich aufgrund des medialen Interesses an Bitcoins, aufgrund der massiven Kursanstiege, seitdem ersten erscheinen im Jahr 2008 stark gewandelt. Diese Aufmerksamkeit schlägt sich auch in der Zahl der Publikation von Fachartikeln in Zeitschriften wie z.B. Kryptomagazinen oder anderen Buchquellen durch.

Eine Vielzahl an Nachrichtenmeiden (z.B. F.A.Z., das Handelsblatt) publizieren eigene Fachartikel rund um das Thema Blockchain und Kryptowährungen. Des Weiteren bringen immer mehr Verlage darunter z.B. der Springer Verlag geeignete Buchquellen zur Literaturrecherche heraus. Zusätzlich werden Expertenblogs wie bspw. BTC-Echo zur Informationsgewinnung verwendet, welche sich mit aktuellen, hintergründigen Themen zur Blockchain Technologie und digitalen Währungen befassen.

Ein kritischer Aspekt bei der verwendeten Literatur ist stets die Aktualität. Bitcoins stellen hierbei eine sich schnell verändernde Thematik dar, wodurch Literatur aus dem Jahr 2015 nur noch teilweise als verlässlich in Bezug auf ihre Aussagekraft angesehen werden kann. Die Auswahl der verwendeten Quellen soll daher, trotz Einschränkungen, einen möglichst hohen Erkenntnisgewinn im Bezug zur Forschungsfrage ermöglichen.

Aufgrund der eher als übersichtlich zu bezeichnen (im Vergleich zu anderen wissenschaftlichen Themen) vorhandenen Literatur, folgt primär die Verwendung von aktuellen Quellen unter Hinzunahme alternativen Quellen wie z.B. den oben angeführten Expertenblogs. Wichtig hierbei ist es stets ein vernünftiges Maß an Aktualität der verwendeten Quelle und objektiver Sichtweise des Autors zu wahren. Dies ist unabdingbar um die Seriosität des Forschungsthemas zu wahren.

2 Klassische Zahlungmethoden

2.1 Definition von Geld, E-Geld und Währung

Die geschichtlichen Hintergründe zur Entstehung und Entwicklung von Geld wurden bereits bei der Relevanz des Themas in Abschnitt 1.1 verdeutlicht. Dieses Verständnis ist essenziell um die späteren Gegenüberstellungen von klassischen Zahlungsmethoden und Kryptowährungen hinsichtlich einer vollwertigen, anerkannten und möglichen Substituierbarkeit gesetzlicher Zahlungsmittel beurteilen zu können. Wie wird Geld allerdings im wirtschaftlichen Sinne definiert? Viele berühmte Ökonomen darunter auch Mankiw verwenden den Begriff des Geldes in einem sehr liberalen Sinne, wie die Aussage von Mankiw belegt:

" Money is the set of assets in economy that people regularly use to buy goods and services from each other".[13]

Die ökonomische Definition von Geld ist allgemein deutlich enger gefasst und besagt, Geld ist ein anerkanntes Tausch- und Zahlungsmittel, auf das sich eine Gesellschaft geeinigt hat. Handelt es sich bei diesem festgelegten Tausch-/ Zahlungsmittel um ein Mittel, dass auf Rechtswege festgelegt wurde, wird es als gesetzliches Zahlungsmittel anerkannt. Hierbei wird der Begriff der Währung verwendet.[14] Dahingegen wird eine virtuelle Währung definiert, als eine Darstellung von digitalen Werten, die nicht von einer zentralen gesetzlichen Stelle wie z.B. einer Zentralbank, einem Kreditinstitut oder einem anderen Geldinstitut herausgegeben wird. Alle virtuellen Währungen haben dahingehend gemein, dass sie festen mathematischen Regeln und Mechanismen folgen. Solange es als kein gesetzliches Zahlungsmittel gilt, leitet sich der Wert der virtuellen Währung ausschließlich aus dem Vertrauen der Benutzer in diese Währung ab.[15] Wichtig an dieser Stelle ist klar die Begriffe virtuelle Währung und E-Geld voneinander abzugrenzen.

[13] Vgl.: Mankiw, N.: (2008), S.324.
[14] Vgl.: o.V.: Gabler Wirtschaftslexikon - Definition: Was ist "Geld"?, o.J., 15.03.2020 [Online].
[15] Vgl.: o.V.: Gabler Wirtschaftslexikon - Virtuelle Währung, o.J.,15.03.2020 [Online]

Bei E-Geld (Elektronisches Geld) handelt es sich um die elektronische Repräsentation einer offiziellen Währung. Diese dient dem offiziellen Zahlungsverkehr in elektronischer Form. Diese als elektronisch, offizielle Variante einer Währung darf nicht mit Kryptowährungen wie Bitcoin verwechselt werden.[16] Die untenstehende Abbildung soll diese wesentliche Unterscheidung noch einmal verbildlichen.

Geld-Matrix			
Rechtsstatus	Unreguliert	bestimmte Arten von lokalen Währungen	**Kryptowährungen**
	Reguliert	Banknoten und Münzen	E-Geld
			Buchgeld
		Physisch	Digital
		Geldformat	

Abbildung 1 - Geld-Matrix[17]

Bitcoin kann somit als Währung gesehen werden, welche allerdings von keiner staatlichen Institution reglementiert ist. Darüber hinaus muss Geld drei Funktionen erfüllen um als Währung fungieren zu können: Die Funktion als Tauschmittel, die Rechenfunktion und die Wertspeicherfunktion.[18] Diese Funktionen werden in Abschnitt 2.2 weiter erläutert.

2.2 Funktionen von Geld

Geld im allgemein lässt sich als eine Art von Energie beschreiben. Dies entspricht zwar nicht der ökonomischen Definition, bringt aber das Konzept von Geld näher. Bei Geld handelt es sich um nichts anderes als ein Medium, dass einen bestimmten Wert speichert, ihn erhält um ihn später wieder auszugeben.[19]

[16] Vgl.: Wenger, T; Tokarski K.: (2020), S.252.
[17] Vgl.: Wenger, T; Tokarski K.: (2020), S.253.
[18] Vgl.: o.V.: Deutsche Bundesbank - Was ist Geld?, 2019, 15.03.2020 [Online].
[19] Vgl.: Hosp, J.: (2017), S.26.

Die drei Hauptfunktionen wurden bereits in Kapitel 2.1 aufgeführt. Daraus resultieren gewisse Anforderungen, die ein Objekt oder Medium erfüllen muss um als Geld anerkannt zu werden. Im folgenden Abschnitt sollen die drei Hauptkriterien näher betrachtet werde:

Die **Tauschfunktion** ist der eigentliche Kern des Geldes. Sie dient der Aufgabe als Tausch- und Zahlungsmittel. Vor Einführung von Geld konnten Waren ausschließlich auf direkten Wege gehandelt werden. Dies wurde als Naturalwirtschaft bezeichnet. Grundvoraussetzung ist stets, dass eine Situation entsteht in der zwei Marktteilnehmer gleichzeitig die Güter der Gegenpartei nachfragen. Zudem müssten die Marktsubjekte sich im jeweiligen Tauschverhältnis auf einen geeigneten Wert einigen.[20] Existiert allerdings ein vereinheitlichtes Gut, welches von allen Marktteilnehmern gleichermaßen akzeptiert wird, so kann jede Transaktion über dieses Gut abgewickelt werden. In unserer heutigen Wirtschaftswelt stellt Geld dieses Gut dar und vereinfacht somit den Handel aller zu transferierenden Wirtschaftsgüter.[21] Der Gut zu Gut Handel ist durch Geld abkömmlich geworden.

Die Funktion der **Recheneinheit** ermöglicht es den Wert aller Güter oder Dienstleistungen in einer gleichbleibenden Bezugsgröße darzustellen und die Objekte untereinander vergleichbar zu machen. Statt die dynamischen Tauschverhältnisse zwischen zu tauschenden Objekten einprägen und anpassen zu müssen, schafft Geld einen universellen Bemessungsmaßstab. Dies sorgt für mehr Objektivität und Transparenz auf dem Markt. Such- und Transaktionskosten können dadurch reduziert werden und die Handelbarkeit wird erleichtert.

Die Funktion des **Wertspeichers** bedeutet, dass Waren oder Dienstleistungen nicht immer unmittelbar gegeneinander ausgetauscht werden müssen. Der Verkauf von Waren und Dienstleistungen kann zeitlich auseinanderliegen und ermöglicht die zurückgehaltene Kaufkraft zu sparen und später zu verwenden.

[20] Vgl.: Schär, F.; Berentsen, A.: (2017), S.12 f.
[21] Vgl.: Niessner, M.: (2017), S.11.

Dies erlaubt eine bessere Planbarkeit und Absicherung gegen plötzlich auftretende Investitionen. Zudem ermöglicht dieser Effekt größere Rücklagen zu bilden um später höhere Investitionen am Markt tätigen zu können.[22]
Neben dem klassischen Sparen existieren weitere Investitionsmöglichkeiten, wie z.B. Wertpapiere, Edelmetalle oder Immobilien, die sich auch als Wertspeicher eignen. Zudem generieren diese Anlagealternativen i.d.R. einen Mehrwert in Form von Dividenden oder Zinserträgen. Allerdings überwiegt hierbei der hohe Liquiditätsgrad bei Geld gegenüber solchen Anlageklassen.[23]

2.3 Eigenschaften von Geld

Um die in Abschnitt 2.2. beschrieben Hauptfunktionen erfüllen zu können bedarf es sieben Eigenschaften. Diese lauten: Geldeinheiten müssen haltbar, transferierbar, homogen, verifizierbar sowie ein Mindestmaß an Wertstabilität aufweisen können. Zudem muss gewährleistet sein, dass die Anzahl der sich im Umlauf befindlichen Geldeinheiten strikt reglementiert ist.

- **Haltbarkeit:** Um als Wertspeicher fungieren zu können ist unabdingbar ein gewisses Maß an Haltbarkeit vorauszusetzen. Dadurch eignen sich weder empfindliche noch kurzlebige Güter als langfristige Aufbewahrungsmittel. Die Haltbarkeit muss über einen längeren Zeitraum gegeben sein, damit Geld seine Kaufkraft beibehält.
- **Transferierbarkeit:** Ein Gut muss ohne größere Hürden und Kosten von einem Marktteilnehmer auf den anderen transferierbar sein und bleiben. Dies drückt sich in der Liquidität aus.
- **Teilbarkeit:** Grundvoraussetzung um gegen beliebig heterogene Güter getauscht werden zu können ist es, dass die Geldeinheiten teilbar oder bereits in entsprechend kleinen Einheiten zur Verfügung stehen.

[22] Vgl.: Vgl.: Schär, F.; Berentsen, A.: (2017), S.15 f.
[23] Vgl.: Jarchow, H.: (2010), S.3.

- **Homogenität**: Geldeinheiten die exakt den gleichen Nennwert zueinander aufweisen, müssen konvertibel zueinander sein.
- **Verifizierbarkeit:** Geldeinheiten müssen so gestaltet werden können, dass sie gegenüber Missbrauch (Fälschung) immun sind.[24]
- **Wertstabilität:** Der Ausschluss von Volatilitäten um eine stabile Geldeinheit zu gewährleisten.
- **Seltenheit**: Die limitierte Verfügbarkeit des Angebotes ist die Basis zur Verwendung dieses Gutes als Tauschmittel. Gebe es keine Seltenheit, gäbe es auch kein ökonomischer Grund damit Handel zu betreiben.[25]

[24] Vgl.: Botvinnikova, J.: (2019), S.6.
[25] Vgl.: Schär, F.; Berentsen, A.: (2017), S.17.

3 Bitcoin
3.1 Technische Grundlagen
3.1.1 Entstehung der Blockchain

Kryptowährungen und die damit verbundene Blockchain sind kein gänzlich neues Konzept. Die ersten Ideen entstanden bereits Anfang der 1990er Jahre. Bereits 1983 entwickelte der amerikanische Kryptograph David Chaun eine verschlüsselte, elektronische und anonyme Währung namens "ecash". Später wurde das Programm dann in die Währung "Digicash" umbenannt. Mittels Digicash sollte sich anonym Geld von Banken abheben lassen.[26]

Der nächste Schritt zur Realisierung einer Kryptowährung war die wissentschaftliche Arbeit mit dem Thema Cryptographically linking blocks in an append-only data structure von Stuart Haber und Scott Stornetta im Jahr 1991.[27] Sie legten mit ihrer wissenschaftlichen Arbeit über eine Blockchain den Grundstein für die weitere Entwicklung von Kryptowährungen. In ihrer Arbeit beschrieben sie die Möglichkeit kryptografische Blöcke in einer Datenstruktur so anzulegen, dass die Blöcke ausschließlich neue Einträge entgegennehmen ohne alte Einträge zu verändern oder zu löschen. Diese Entwicklung ist bis heute das zentrale Element hinter der Blockchain Technologie.[28]

Der nächste große Schritt in der Entwicklung hin zu einer digitalen Währung war die Erfindung von "bit gold" durch Nick Szabo im Jahr 1998. Bit gold wählte damals als erste digitale Währung den Proof-of-Work Algorithmus, wodurch das Ziel verfolgt werden sollte eine dezentrale, elektronische Währung, die nicht von Staaten oder Zentralbanken kontrolliert wurde, zu erschaffen. Bei Transaktionen von herkömmlichen Währungen waren bis dato immer die Finanzinstitute involviert. Szabo wollte dies ändern, so dass es möglich sein sollte Transaktionen anonym, ohne die Beteiligung fremder Dritter durchzuführen.[29]

[26] Vgl.: Schneider, T.: (2017), S.5.
[27] Vgl.: Dr. Beyer, C.: Blockchain Before Bitcoin: A History, 2018, 15.04.2020 [Online].
[28] Vgl.: Cueni, S.: (2019), S.5.
[29] Vgl.: o.V.: 6 Gründe arum dieser nebulöse Computerwissenschaftler wohl Bitcoin erfunden hat, 2018, 15.04.2020 [Online].

Das gravierende Problem war zu dieser Zeit allerdings die des Double Spending. Double Spending bedeutet hierbei, dass etwas doppelt ausgegeben wird. Bei den entwickelten Kryptowährungen handelt es sich ja um nichts Anderes als geschrieben Code abgespeichert auf einer Festplatte. Diesem Code stand zu diesem Zeitpunkt allerdings kein physisches Gut gegenüber.[30]

Dadurch war es möglich die digitale Währung künstlich zu erhöhen. Dieses Problem ist vergleichbar mit einem Foto auf einem PC. Es ist möglich dieses Bild an eine Person A schicken, gleichzeitig aber auch einfach zu kopieren und an Person B zu schicken. Damit entsteht die Möglichkeit sich selber neue Kryptowährungen zu erstellen, womit eine Währung auf dieser Basis unbrauchbar ist.[31]

Durch Platzen der Immobilienblase in Amerika und der dadurch ausgelösten globalen Finanzkrise wurde das Vertrauen in zentrale Intermediäre stark erschüttert. Ab diesem Zeitpunkt war für jeden offensichtlich das zentralisierte Systeme nicht zu Einhundert Prozent fehlerfrei und vertrauenswürdig sind.[32]

Zeitgleich im Jahr 2008 beschrieb ein Pseudonym namens Satoshi Nakamoto die Lösung des Double Spending Problems in seinem legendären Whitepapter "Bitcoin: A Peer-to-Peer Electronic Cas System". Bis heute ist die eindeutige Identität des Erstellers nicht zweifelsfrei geklärt. Zu dem Pseudonym existieren zahlreiche Theorien - es handle sich um eine Einzelperson, eine Gruppe oder sogar um das CIA.
In dem Artikel stellt Nakamoto das Konzept einer Blockchain und der darauf befindlichen Kryptowährung Bitcoin erstmalig vor. Die Blockchain agiert hierbei als eine Art verteilte Buchhaltung. Diese verteilte Buchhaltung zeichnet dabei jede Transaktion transparent im Hintergrund mit auf und schließt Double Spending damit vollkommen aus. Diese revolutionäre Idee erlaubte es im dezentralen Transaktionssystem Zahlungen vorzunehmen, ohne das eine dritte Partei als zentraler Institution zum Einsatz kommt.

[30] Vgl.: Hosp, J.: (2017), S.40.
[31] Vgl.: Schneider, T.: (2018), S.6.
[32] Vgl.: Wenger, T. et al.: (2020), S.249.

Daher bietet die Blockchain nicht nur eine Verwendung für Geld sondern eröffnet mannigfaltige Verwendungsmöglichkeiten. Sie ist das ideale Werkzeug, wann immer etwas übertragen und dokumentiert werden soll wie z.B. im Kunstbereich, in der Medizin, bei Behörden, im Energiehandel, bei Immobilien etc.[33]

3.1.2 Blockchain Technologie

Die Blockchain Technologie ist die Grundlage zur Existenz einer dezentralen Währung. Die Technologie verzeichnet dabei jede Transaktion und speichert diese in Blöcken. Alle Transaktionen werden dabei mit einem Zeitstempel versehen. Kryptische Verfahren wie der Proof-of-Work Mechanismus in Kombination mit einer SHA-256 Verschlüsselungstechnik sichern die Transaktionen dabei ab. Anschließend werde diese Blöcke wieder aneinandergereiht, woraus der englische Begriff "blockchain" auf Deutsch Blockkette folgt.[34] Sie wird von keiner zentralen Institution oder Staat besessen oder kontrolliert. Bei der Blockchain handelt es sich daher um ein webbasiertes, dezentral verteiltes Kontenbuch[35]

Diese Beschreibung ist eine von vielen Definitionen, die versuchen diese hochkomplexe Technologie hinter der Blockchain in verkürzter Form darzustellen. Blockchains sind somit im Grunde eine alternative Lösung zu den althergebrachten intermediären Transaktionssystemen, die als Voraussetzung eine vertrauenswürdige Drittpartei benötigen. Wichtig hierbei ist zu vermerken, dass es sich bei der Blockchain um ein Transaktionssystem und bei dem Bitcoin um eine Geldeinheit handelt. Bitcoin wird eher als eine Applikation, die auf der Blockchain beruht verstanden.

[33] Vgl.: Thelen, F.: (2018), S:242.
[34] Vgl.: Schneider, T.: (2018), S.7.
[35] Vgl.: Polleit, T.: Gold ist die bessere Währung, 2017, 11.03.2020 [Online].

Durch Ablösung der zentralen Instanz zwischen den Transaktionsparteien wird die Systemarchitektur weg von einer zentralen hin zu einer verteilten (dezentralen) Architektur verändert. Dezentrale Systeme, wie die Blockchain, verfügen dabei nicht mehr über einen zentralen Knotenpunkt sondern alle Knotenpunkte kommunizieren direkt miteinander. Diese Technologie nennt sich Distributed Ledger Technologie (DLT). Oft werden in der Literatur die DLT und die Blockchain synonym miteinander verwendet.
Eigentlich handelt es sich bei der Blockchain allerdings um eine mögliche Darstellung eines Transaktionssystems die auf der DLT beruht. Zum einfacheren Verständnis sollen in dieser Arbeit die Begriffe synonym verwendet werden.[36]

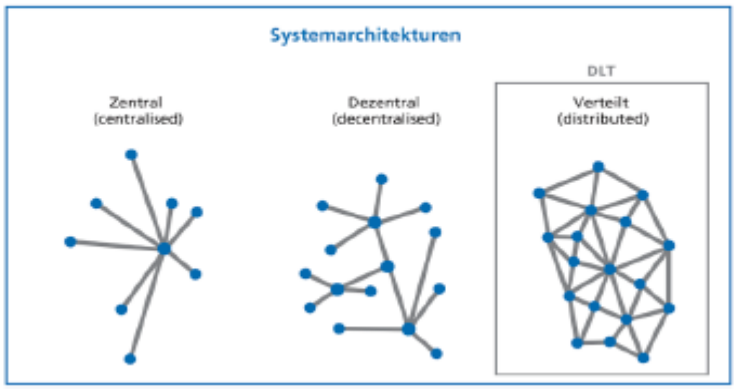

Abbildung 2 - Systemarchitekturen

Die Dezentralität ist bei der Blockchain der entscheidende Faktor. Dafür benutzt die Blockchain ein Peer-to-Peer (P2P) Netzwerk. Unter P2P wird verstanden, dass alle Teilnehmer gleichberechtigt sind. Jeder Teilnehmer besitzt somit alle bzw. einen Teil der Daten der Transaktionskette. Im Fall von Bitcoin speichert jeder Teilnehmer die komplette Transaktionskette auf seinem eigenen Computer ab. Momentan nimmt dies 312 GB in Anspruch, Tendenz steigend. Für die weitere Betrachtung soll die Bitcoin Blockchain als Grundlage dienen. Die einzelnen Peers kommunizieren online über einen Bitcoin-Client.[37]

[36] Vgl.: Egloff, P.; Turnes, E.: (2019), S.29.
[37] Nakamoto, S.: (2008), S.3 f.

Dabei werden die Ressourcen unter den einzelnen Peers aufgeteilt. Jeder Peer ist in der Lage Kryptowährungen zu jeder Zeit, standortunabhängig und vollkommen anonym zu kaufen oder zu verkaufen. Damit ist jeder Anbieter zeitgleich Anbieter und Nachfrager. Es erfolgt keine Bonitätsprüfung seitens einer zentralen Institution. Die Prüfung wird durch eine Verifizierung durch alle Peers selbstständig übernommen. Die Information der Übertragung (Kauf bzw. Verkauf von BTC) wird an alle Peers als Nachricht im dezentralen Netzwerk weitergeleitet. Solange bis allen Peers die Information zur Verfügung steht. Dies ist notwendig, damit alle Netzwerkteilnehmer stets eine aktualisierte Version der Blockchain besitzen.[38]

Diese Datenblöcke (Blocks) werden dezentral abgelegt und fest mit einer Kette (Chain) verbunden.[39] Die Verbindung wird mittels eines Codes, einen sogenannten Hash herbeigeführt. Eine Hashfunktion ist eine mathematische Funktion, die in der Kryptographie verwendet wird. Diese mathematische Funktion erlaubt es beliebig lange Zeichenketten mittels vorher festgelegter Größe in neue Zeichenketten zu transformieren. Diese neue Art von Zeichenketten werden als Hashwerte genannt. Die Blockchain nutzt hierfür den SHA-256 Algorithmus. SHA-256 erlaubt es Zahlungsinformationen, wie Betrag, Sender; Empfänger in 64 (Hash) Zeichen herunterzurechnen.[40]

Hashwerte sind wesentlicher Kern im Blockchain-System. Neben der verschlüsselten Übermittlung von Teilen der Transaktionsnachricht, sorgen sie dafür das ein Verkäufer von Bitcoin den anderen Netzwerkteilnehmern seine Bitcoins überweisen kann, ohne das fremde Dritte Zugriff auf seine Bitcoins erlangen oder diese stehlen könnten. Damit garantieren die Hashwerte eine Manipulationssicherheit und sorgen für die Integrität im Blockchain Netzwerk.[41]

[38] Vgl.: Brühl, V.: (2017), S.135 ff.
[39] Vgl.: Thelen, F.: (2018), S.240.
[40] Vgl.: Clement, R.; Schreiber, D.: (2016), S.330.
[41] Vgl.: Nakamoto, S.: (2008), S. 2 f.