Von der visuellen Symbolik zum Vertrauen schaffenden System der virtuellen Währung Bitcoin

Meropi Tzanetakis

1. Einleitung

Das traditionelle Zahlungswesen ist in Bewegung. Neben das staatlich kontrollierte Währungssystem, das in Form von Banknoten, Münzen und als Buchgeld (Giralgeld) existiert, traten mit der zunehmenden Verbreitung des World Wide Web und technologischen Entwicklungen virtuelle Währungen[1] (vW) zum Kauf und Verkauf von Waren und Dienstleistungen (ECB 2012). Derzeit existieren rund 500 unterschiedliche virtuelle Währungen, die sich hinsichtlich ihrer technischen Eigenschaften und Funktionalität unterscheiden (ECB 2015, S. 9). Daneben hat die zunehmende Erschließung des Internets für VerbraucherInnen in den letzten 20 Jahren auch elektronisches Geld (E-Geld) hervorgebracht, das als eine digitale Darstellung von Buchgeld von virtuellen Währungen zu unterscheiden ist. Weitläufig bekannt ist es als elektronische Geldbörse, elektronische Überweisung oder in Form von Prepaid-Karten (Schweizerische Eidgenossenschaft 2014, S. 7). Anders als bei virtuellen Währungen bleiben bei E-Geld die Rechnungseinheiten der jeweiligen Währung (z. B. Euro, US-Dollar) erhalten (ECB 2012, S. 16). Kurz gesagt, ein Euro in meiner Brieftasche bleibt auch im Internet bei einer Online-Überweisung ein Euro.

Unter einer vW kann eine digitale Darstellung von Wert verstanden werden, die von keiner staatlichen Institution ausgegeben wird und unter gewissen Umständen als Alternative zu Geld verwendet

[1] Die Begriffe „digitale Währung“ und „virtuelle Währung“ werden in diesem Beitrag alternierend für denselben Inhalt verwendet.

werden kann (ECB 2015, S. 25). Eine vW kann, abhängig von der Akzeptanz innerhalb der Community ihrer NutzerInnen, die wichtigsten Funktionen von herkömmlichem Geld erfüllen – die eines Zahlungsmittels, einer Recheneinheit und/oder eines Wertaufbewahrungsmittels (FATF 2014, S. 4). Sämtlichen vW ist jedoch gemein, dass sie bislang nicht als gesetzliches Zahlungsmittel zugelassen sind (ECB 2015, S. 24).

Der vorliegende Artikel wird sich schwerpunktmäßig mit der vW Bitcoin beschäftigen und hierbei der Frage nachgehen, welche symbolischen Darstellungsformen und physische Ausformungen von Bitcoin offline im Umlauf sind und wer dadurch angesprochen werden soll. Dazu werden eingangs virtuelle Währungen im Universum der Währungssysteme verortet. Im darauffolgenden Abschnitt wird auf grundlegende Charakteristika und die wirtschaftliche Bedeutung von Bitcoin eingegangen, um zu erläutern, wie diese vW im Gegensatz zu staatlich garantierten Währungen funktioniert. In einem nächsten Schritt werden Bitcoin-Symbole besprochen und Ausformungen des digitalen Codes als Münzen und Noten diskutiert. Darauf folgt eine Analyse, wie Bitcoin-Symbole durch vertrauensbildende Mechanismen zu einer steigenden Akzeptanz dieser vW beitragen sollen. Der Beitrag schließt mit einer Zusammenfassung der wichtigsten Erkenntnisse aus der Analyse und einem Ausblick auf mögliche zukünftige Entwicklungen von vW ab.

2. Einordnung virtueller Währungen

Die meisten vW existieren bislang als digitaler Code und haben keine physische Ausformung als Münzen oder Noten (Schweizerische Eidgenossenschaft 2014). Auf eine beispielhafte Ausnahme, Bitcoin, wird in den folgenden Kapiteln eingegangen werden. Die etwa 500 in Umlauf befindlichen vW können nach unterschiedli-

chen Gesichtspunkten kategorisiert werden. Eine Unterteilungsmöglichkeit richtet sich nach ihren Berührungspunkten mit gesetzlichen Zahlungsmitteln und der Möglichkeit, Waren und Dienstleistungen zu (ver-)kaufen (ECB 2012, S. 13 ff.).

Ein erster Typus (ECB 2012, S. 13) hat praktisch keine Verbindung zu einer Offline-Ökonomie. Diese sogenannten geschlossenen vW kommen vor allem innerhalb von Computerspielen zum Einsatz. Die vW kann online gesammelt werden, wobei zur Nutzung des Spiels eine Einschreibgebühr vorgesehen ist. Mit der vW können wiederum virtuelle Waren und Dienstleistungen innerhalb der diesbezüglichen Online-Community erworben werden. Dabei war ursprünglich nicht vorgesehen, dass dieser Typus vW in der physischen Welt gehandelt wird. Ein Beispiel für die aktuelle Entwicklung ist World of Warcraft (WoW)-Gold. Bei dem Online-Rollenspiel können mittels WoW-Gold z. B. Ausrüstungsgegenstände erworben werden. Die SpielerInnen haben die Möglichkeit, durch das Lösen von Aufgaben WoW-Gold zu sammeln bzw. im eigenen Auktionshaus mit anderen Spielern zu handeln. Der Kauf und Verkauf von WoW-Gold außerhalb des Spiels ist verboten und wird mit der Sperrung des Accounts durch den Hersteller geahndet. Nichtsdestotrotz hat sich ein illegaler Markt entwickelt, auf dem die vW gegen ein gesetzliches Zahlungsmittel ge- und verkauft werden kann.

Den zweiten Typus (ECB 2012, S. 14 f.) stellt einseitig handelbare vW dar. Sie kann mit realer Währung zu einem bestimmten Wechselkurs erworben werden, jedoch nicht mehr in diese zurückgewechselt werden. Mit vW dieses Typs wird es den NutzerInnen ermöglicht, online und offline Waren und Dienstleistungen zu kaufen. Als Beispiel sind Nintendo Points zu nennen. KundInnen können diese vW online mittels Kreditkarte beim Hersteller oder als Nintendo Points Card im Einzelhandel erstehen, um sie im Nintendo Shop gegen Spiele und Anwendungen einzutauschen.

Ein dritter Typus (ECB 2012, S. 14 f.) sind vW, die sowohl in reale Währung getauscht als auch umgekehrt zu bestimmten Wechselkursen von dieser eingetauscht werden können. Wie beim zweiten Typ auch, können mit vW des dritten Typs sowohl in der Offline- als auch in der Online-Ökonomie Waren und Dienstleistungen gekauft werden, wie im Folgenden gezeigt wird. Ein Beispiel sind Bitcoins. Zu Wechselkursen, die über Angebot und Nachfrage gebildet werden, können NutzerInnen Bitcoins in traditionelle Währungen wechseln und vice versa. Bei sämtlichen Online- und Offline-HändlerInnen, die diese vW als Zahlungsmittel akzeptieren, können Waren und Dienstleistungen gekauft werden. Im Gegensatz zu anderen vW haben Bitcoins keine zentrale Ausgabestelle, sie werden dezentral geschöpft.

Nachdem bisher drei Typen von virtuellen Währungen unterschieden worden sind, wird im nächsten Abschnitt auf grundlegende Wirkungsmechanismen von Bitcoin als Vertreter des dritten Typs eingegangen.

3. Bedeutung und Funktionsweisen von Bitcoin

Bei Bitcoin (BTC) handelt es sich um eine der bekanntesten und am weitesten verbreiteten virtuellen Währungen, wie auch die Darstellung in Abbildung 1 verdeutlicht. Demnach verbucht BTC mit einer Marktkapitalisierung (Anzahl der BTCs mal Wechselkurs) von 2,7 Milliarden US-Dollar etwa 80 % des Gesamtwertes sämtlicher Kryptowährungen[2]. Durch die breite Medienberichterstattung ist sie ins Bewusstsein der interessierten Öffentlichkeit vorgedrungen, gleichzeitig steigt die Anzahl von Händlern und

[2] Unter Kryptowährung wird eine vW verstanden, die mathematische Verschlüsselungsmechanismen zur Sicherung der Vertraulichkeit und Integrität sowie für die Authentifizierung von Informationen verwendet. http://wirtschaftslexikon.gabler.de/Definition/kryptographie.html [Zugriff am 30.03.2015].

Dienstleistern, die Bitcoin als Zahlungsmittel akzeptieren (Schweizerische Eidgenossenschaft 2014, S. 4). Dennoch ist BTC gesamtwirtschaftlich gesehen nicht sehr bedeutend, wie eine vergleichende Auflistung von Transaktionen pro Tag für unterschiedliche elektronische Zahlungsmittel in Abbildung 2 verdeutlicht. Demnach wickeln elektronische Zahlungsnetzwerke für traditionelle Währungen, wie Visa, Mastercard, American Express, PayPal oder Western Union, zwischen 10 und 3500 Mal so viele Zahlungen pro Tag ab wie Bitcoin.

Doch zurück zum Anfang der vW: Passend zur dezentralen Struktur ist Bitcoin ein Gründungsmythos eingeschrieben. Die erste Erwähnung von BTC geht auf das Jahr 2008 zurück, in dem Satoshi Nakamoto ein White Paper zu Bitcoins auf einer Kryptographie-Mailingliste[3] veröffentlichte (Nakamoto 2008). Dabei ist bislang unklar, ob sich hinter dem Pseudonym eine Person oder eine Gruppe verbirgt. Grundgedanke von BTC ist, dass Zahlungen direkt zwischen NutzerInnen abgewickelt werden können, ohne dass Finanzinstitute (z. B. Banken) im elektronischen Zahlungsverkehr zwischengeschaltet werden (Nakamoto 2008). Deren Abwicklungskosten sind zum einen beträchtlich, zum anderen können sie die Durchführung von Transaktionen ablehnen. Das Bitcoin-System ermöglicht hingegen die Abwicklung von nicht-reversiblen Zahlungen. Zudem gibt es keine zentrale Abwicklungs-, Ausgabe- oder Kontrollstelle für Bitcoins (wie z. B. eine Notenbank). Anstatt auf Vertrauen in eine zentrale Instanz funktioniert das System dezentral auf Basis eines mathematischen Algorithmus und kryptografischer Verfahren zur Verschlüsselung von Informationen.

Eine der größten Herausforderungen einer vW ist das Problem des Duplizierens (Nakamoto 2008). Für gewöhnlich lassen sich digitale Daten einfach und ohne Verlust kopieren. Derselbe Vorgang

[3] http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html, vom 01.11.2008 [Zugriff am 14.03.2015].

ist bei Geld jedoch problematisch, weil bei einfach zu kopierendem Geld der Tauschwert verloren geht (Böck 2013). Bei traditionellen Währungen wird die Problematik z. B. durch Sicherungsmerkmale auf Münzen und Banknoten entschärft, jedoch durch Fälschungen zugespitzt. Dem sogenannten „Double Spending"-Problem wird bei BTC dadurch begegnet, dass die Historie sämtlicher Transaktionen in Form der Block Chain[4] offengelegt und dauerhaft gespeichert wird. Würde ein/eine NutzerIn versuchen, eine BTC doppelt auszugeben, wäre das für die TeilnehmerInnen des Peer-to-Peer(P2P)-Netzwerks nachvollziehbar und die Transaktion würde als ungültig verworfen werden (Böck 2013).

Eine zweite Herausforderung im BTC-System stellt der Prozess der ‚Geldschöpfung' dar. TeilnehmerInnen des dezentralen P2P-Netzwerks – analog zum Goldschürfen auch als MinerInnen bezeichnet – werden für das Lösen von komplexen Rechenaufgaben beim Bestätigen von Transaktionen mit neuen BTC belohnt (Schweizerische Eidgenossenschaft 2014, S. 8). Dabei wird in der Block Chain vermerkt, dass der/die NutzerIn die Anzahl an BTC auch tatsächlich besitzt und nicht doppelt ausgibt. Die MinerInnen erhalten als Entschädigung für das Einbringen von Rechenleistung in das Netzwerk neue, quasi aus dem Nichts geschaffene Bitcoins (Böck 2013). Mit Stand vom März 2015 sind knapp 14 Millionen BTCs im Umlauf[5], die gesamte Anzahl an BTCs ist durch das Netzwerkprotokoll auf 21 Millionen Stück begrenzt (ECB 2012, S. 25). Diese Begrenzung und die steigende Komplexität der zu lösenden Rechenaufgaben können auch als Inflationsschutz verstanden werden.

Die Erläuterung von grundsätzlichen Funktionsmechanismen der digitalen Währung, eine Einordnung der ökonomischen Rolle von

[4] Eine Block Chain ist eine öffentliche Darstellung sämtlicher Bitcoin-Transaktionen, die jemals getätigt wurden. Die Kette von Blöcken wird ständig um neue Transaktionen chronologisch erweitert.
[5] https://blockchain.info/charts/total-bitcoins [Zugriff am 30.03.2015].

BTC und die Skizzierung zweier grundlegender Herausforderungen des Systems Bitcoin ebnen den Weg für eine Analyse der visuellen Darstellungsformen.

4. Bitcoin-Symbole und -Logos

Im White Paper von Nakamoto (2008) findet sich keinerlei Hinweis auf ein Bitcoin-Symbol oder -Logo. Es wird lediglich definiert, dass eine elektronische Münze eine Reihe von digitalen Signaturen darstellt (Nakamoto 2008, S. 2). Die dezentrale Funktionsweise von BTC spiegelt sich jedoch im Umgang mit visuellen Symbolen der vW wider. Demnach gibt es keine zentrale Institution, die Bitcoin-Logos bzw. physische Ausformungen der digitalen Signatur ausgibt oder verwaltet. Dieser Grundsatz gilt auch für die bei BTC zum Einsatz kommende Open-Source-Software. Zum einen ist der Programmiercode öffentlich verfügbar, damit EntwicklerInnen mitgestalten und die Software weiterentwickeln können.[6] Zum anderen ist die BTC-Software für NutzerInnen kostenfrei zugänglich. Grundgedanke von BTC ist folglich, dass die vW von der Community selbständig verwaltet wird. Zusätzlich haben sich, basierend auf dem Protokoll des Open-Source-Projektes, zahlreiche alternative vW zu BTC herausgebildet, die unter dem Begriff „Altcoins" zusammengefasst werden (ECB 2015, S. 9). Sie basieren meist auf denselben dezentralen Prinzipien, doch ist bspw. ihr Stückpreis wesentlich niedriger und die Transaktionen werden schneller bestätigt, brauchen damit einen geringeren Energieaufwand und sind günstiger in der Erzeugung. Als Beispiele sind Litecoin oder Dogecoin zu nennen, welche in Abbildung 1 mit ihrem jeweiligen Logo ersichtlich sind.

[6] https://bitcoin.org/de/entwicklung [Zugriff am 30.03.2015].

Eine schnelle Recherche in einer beliebigen Suchmaschine zeigt, dass eine Vielzahl an BTC-Logos im Umlauf ist, doch hat sich aktuell die in Abbildung 3 dargestellte Variante durchgesetzt. Dieses populäre Logo besteht aus einem geneigten B in Serifenschrift, das von zwei vertikalen Strichen durchkreuzt wird. Der in Weiß gehaltene Buchstabe wird von einem orangen Kreis umschlossen. Die Anlehnung an das Währungssymbol des US-Dollars ist unverkennbar. Die Parallelen zum US-Dollar können als Orientierung an einer Währung interpretiert werden, die weltweit gehandelt wird, dementsprechend Vertrauen genießt und als entsprechendes Zahlungsmittel fungiert.

Nachdem es keine zentrale Instanz gibt, die darüber entscheidet, welches Logo offiziell verwendet wird, ist die Akzeptanz innerhalb der Gemeinschaft der BTC-NutzerInnen ein entscheidender Faktor. Im Juni 2014 wurde eine Arbeitsgruppe innerhalb der Bitcoin Foundation eingerichtet, in der Freiwillige aktuelle BTC-Logos und Symbole standardisieren sollen, um die allgemeine Akzeptanz zu erhöhen (Hajdarbegovic 2014b). Bei der Bitcoin Foundation[7] handelt es sich um eine nicht-profitorientierte Organisation, die als Interessensvertretung der Community agiert und Standardisierung sowie Normung von Bitcoin vorantreibt. Es gibt auf einschlägigen Foren[8] zahlreiche divergierende Diskussionsbeiträge dazu, welches Bitcoin-Symbol von den NutzerInnen und der Branche bevorzugt wird. Zum Beispiel wurde anfangs lange das Symbol ฿ verwendet, um Bitcoin zu repräsentieren, allerdings wird es nicht von jedem System gleich gut dargestellt (Cawrey 2014). Deshalb macht sich eine Gruppe von Industrievertretern[9] zunehmend für das Symbol Ƀ stark, das im Unicode-Standard in

[7] http://bitcoinfoundation.org/ [Zugriff am 03.04.2015].
[8] https://bitcointalk.org/index.php?topic=369.0 [Zugriff am 04.04.2015].
[9] http://bitcoinsymbol.org/ [Zugriff am 04.04.2015].

einer standardisierten Computer-Schriftart verwendet werden kann. Auch das Symbol für den thailändischen Baht (฿) wird gerne für die digitale Währung verwendet, birgt jedoch Verwechslungsgefahr.[10] Diese kurze Skizzierung einiger Bitcoin-Symbole lässt die Schwierigkeit erahnen, unterschiedliche Positionen in einem konsensbasierten Prozess zusammenzubringen.

Neben Bitcoin-Logos und -Symbolen verbreiten sich im Internet auch zahlreiche 3D-Darstellungen der virtuellen Währung. Ihnen ist gemein, dass sie nicht reguliert werden und somit der künstlerischen Freiheit und Kreativität im Grunde keine Grenzen gesetzt sind, außer eventuell bei der technischen Umsetzung. Das linke 3D-Rendering in Abbildung 4 verwendet das Symbol aus dem populären Logo (siehe Abbildung 3), ist in Gold gehalten und hat neben dem Entstehungsjahr zwei Leitsprüche ‚eingraviert'. Der eine ist als politischer Begriff zu verstehen und lautet „Libertas, Aequitas, Veritas"; auf Deutsch: „Freiheit, Gleichheit, Wahrheit". Der andere Spruch ist eine Anlehnung an das „In God We Trust" auf US-Dollarscheinen und heißt in Abwandlung: „In Cryptocurrency We Trust", also „Wir vertrauen in Kryptowährungen". Die mittlere 3D-Darstellung orientiert sich am Euro und verwendet dasselbe Symbol wie der thailändische Baht, ergänzt um ein C. Der in Gold gehaltene äußere Ring hat 24 Sterne eingraviert, auf der silbernen Innenfläche ist eine Weltkarte dargestellt. Auf einen Spruch wird hier verzichtet. Das rechte, in Gold gehaltene Rendering trägt dieselben beiden Mottos wie die linke Münze und verwendet das Unicode-Symbol Ƀ. Obwohl sich die visuellen Darstellungen in Bezug auf die Bitcoin-Symbole unterscheiden, haben sie auch eine Gemeinsamkeit: Sie sind physischen Münzen nachgeahmt. Dreidimensionale Bitcoin-Visualisierungen stellen die Vorstufe zu physischen, haptischen Ausformungen der digitalen Währung dar, die im nächsten Abschnitt analysiert werden.

[10] https://en.bitcoin.it/wiki/Bitcoin_symbol [Zugriff am 04.04.2015].

6. Physische Formen von Bitcoin

Bei der Frage nach physischen Ausformungen der vW Bitcoin sind zwei wesentliche Unterschiede zu gesetzlichen Zahlungsmitteln zu beachten: Entsprechend dem Umstand, dass es keine zentrale Ausgabestelle gibt, können theoretisch beliebig viele Unternehmen Bitcoin-Münzen oder -Scheine herstellen. Gleichzeitig ist der physische Markt für virtuelle BTCs nicht sehr groß und bislang eher von eingefleischten Fans und Sammlern erschlossen (Hajdarbegovic 2014a). BTC-Münzen werden somit nur von einer Handvoll Firmen erzeugt, die tendenziell entweder hochwertiges Edelmetall verarbeiten oder ansprechendes Design zum kleinen Preis anbieten. In einem Artikel auf Coindesk werden zehn verschiedene BTC-Münzen von unterschiedlichen Herstellern präsentiert (Hajdarbegovic 2014a). Der zweite Unterschied zu offiziellen Währungen bezieht sich auf den Inhalt, da es sich bei den physischen Formen von BTCs um Träger für die digitalen Signaturen handelt, die ein Aufbewahren der vW ermöglichen. Auf einer physischen Münze sind die öffentliche Adresse und der private Schlüssel enthalten, mit dem auf den online hinterlegten Betrag in BTC zugegriffen werden kann.

Exemplarisch für eine physische Abbildung von digitalen BTC sei die des größten Herstellers für BTC-Münzen erwähnt, die Casascius-Coins[11] (siehe Abbildung 5). Das Prinzip dieser Münze funktioniert wie folgt: Auf der einen Seite sind ein Bitcoin-Symbol und das Jahr der Prägung angebracht. Auf der anderen Seite der Münze ist der öffentliche Schlüssel aufgedruckt. Darunter befindet sich ein Hologramm-Aufkleber, unter dem sich der private Schlüssel als Zahlen- und Buchstabenabfolge befindet. Beide Schlüssel werden benötigt, um auf den BTC-Wert, der auf der Münze vermerkt ist, online zuzugreifen. Um Missbrauch zu verhindern bzw. um

[11] https://www.casascius.com/ [Zugriff am 01.04.2015].

eine Entwertung anzuzeigen, wurde das Hologramm vom Hersteller so konstruiert, dass es beim Ablösen eine Wabenstruktur hinterlässt (siehe Abbildung 6). Lediglich ein unbeschädigtes Hologramm garantiert, dass der Besitzer der Münze den BTC-Wert online nutzen kann. Allerdings wurden auf der Defcon[12], einem der weltweit größten Hacker-Treffen, Möglichkeiten präsentiert, den Aufkleber abzulösen und den privaten Schlüssel auszulesen, ohne das Hologramm dabei zu beschädigen. Damit kann die Münze weitergegeben werden, ohne dass die Verfügbarkeit über ihren Wert für den neuen Besitzer sichergestellt ist. Der Zweck der Münzen – einen virtuellen Wert sicher offline aufbewahren zu können – ist somit ad absurdum geführt. Die Casascius-Coins[13] wurden in Nennwerten von 0,5 bis 25 BTC in mehreren Serien aus Gold, Silber oder Aluminium gefertigt. Sie sind mittlerweile nicht mehr vom Hersteller zu beziehen, da eine Behörde des US-Finanzministeriums den Vertrieb der Münzen als Geldübermittlung eingestuft und daran Regulierungs-bestimmungen geknüpft hat, welche die Kapazität des Unternehmens übersteigen.[14]

Neben BTC-Münzen gibt es als zweite Variante physischer Bitcoins BTC-Scheine, die ebenso ein langfristiges Aufbewahren ermöglichen. Im Vergleich zum Verwahren von BTCs auf dem Smartphone, Computer oder im Internet gilt das Hinterlegen von BTCs in ausgedruckter Form als sicherer, da sie quasi nicht geknackt werden können.[15] Beispielhaft ist in Abbildung 7 die Vorder- und Rückseite eines solchen BTC-Scheins von BitcoinPaper-PaperWallet zu sehen. Der Schein wird gefaltet und mit einem Hologramm-Sticker versehen, um den privaten Schlüssel vor dem Auslesen zu schützen. Das basale Prinzip ist dasselbe wie bei den

[12] http://codinginmysleep.com/casascius-physical-bitcoins-cracked-at-defcon/, vom 04.08.2013 [Zugriff am 01.04.2015].
[13] https://www.casascius.com/ [Zugriff am 01.04.2015].
[14] http://www.wired.com/2013/12/casascius/, vom 12.12.2013 [Zugriff am 01.04.2015].
[15] https://bitcoinpaperwallet.com/ [Zugriff am 02.04.2015].

BTC-Münzen: Der öffentliche Schlüssel wird auf der Außenseite des Scheins, meist als maschinell lesbarer QR-Code, aufgedruckt und ermöglicht das Einsehen des BTC-Wertes (das linke schwarz-weiße Kästchen in Abbildung 7). Der private Schlüssel wird verdeckt am Schein angebracht (das rechte schwarz-weiße Kästchen in Abbildung 7), meist ebenfalls als QR-Code, und z. B. durch einen Hologramm-Sticker gesichert. Beim Einsehen des privaten Schlüssels werden eindeutige Spuren hinterlassen, die dem Inhaber die Entwertung des BTC-Scheins signalisieren.

Es existieren zahlreiche (kommerzielle) Anbieter solcher BTC-Scheine. Manche erlauben es auch, ein sogenanntes Paper-Wallet selber auszudrucken.[16] Dieser kostenfreie Service wird zumeist um die zahlungspflichtige Bestellmöglichkeit von Hologramm-Stickern zum Versiegeln des privaten Schlüssels, wasserresistenten, verschließbaren Plastiktaschen oder auf einer CD abgespeicherter Software zum offline Erstellen einer elektronischen Brieftasche ergänzt. Jedoch gibt es an der Schnittstelle zwischen Online- und Offline-Welt zahlreiche Sicherheitsrisiken, beispielsweise wenn beim Ausdrucken des Schlüsselpaares andere NutzerInnen unerlaubt die digitale Signatur einsehen.[17] Auch muss dem Erzeuger eines BTC-Scheins vertraut werden, denn dieser könnte durch eine Kopie des Schlüsselpaares Zugang zu dem BTC-Wert erlangen. Da die Sicherheitsmechanismen gegenwärtig noch Luft nach oben haben, eignen sich physische Ausformungen von BTC nicht für anonyme Geschäftstransaktionen mit größeren Summen. Grundsätzlich ist es aufgrund der dezentralen Funktionsweise von BTC der Kreativität der Anbieter überlassen, welche Produkte auf den Markt gebracht werden, um die Sicherheit und v. a. den Auslesesschutz des privaten Schlüssels von BTC-Münzen bzw. -Scheinen zu erhöhen. Im nächsten Abschnitt werden u. a. die physischen

[16] http://www.coindesk.com/information/paper-wallet-tutorial/ [Zugriff am 02.04.2015].
[17] https://bitcoinpaperwallet.com/#security [Zugriff am 02.04.2015].

Formen von Bitcoin in Kontext zu vertrauensbildenden Maßnahmen gesetzt, um herauszuarbeiten, wie durch diese potentielle NutzerInnen angesprochen werden sollen.

7. Mechanismen der Vertrauensbildung

Von staatlichen Institutionen ausgegebene Währungen, auch FIAT-Geld genannt, haben im Gegensatz zu Warengeld keinen ‚inneren Wert' und sind auch nicht durch Gold gedeckt (Deutsche Bundesbank 2014, S. 17). FIAT-Währungen (z. B. Euro, US-Dollar) sind als gesetzliches Zahlungsmittel zugelassen und leben vom Vertrauen der MarktteilnehmerInnen in ihre Tauschmittelfunktion (Deutsche Bundesbank 2014). Demzufolge akzeptieren NutzerInnen FIAT-Geld im Austausch für Güter und Dienstleistungen. Die Herstellung von FIAT-Geld ist zudem erheblich günstiger als mit einem Sachwert gedecktes Warengeld, wodurch theoretisch unbegrenzte Geld-Mengen hergestellt werden können (Deutsche Bundesbank 2014, S. 17). Traten in der Vergangenheit solche Fälle inflationärer Geldproduktion auf, ging dies mit Geldentwertung, Vertrauens- und Akzeptanzverlust einher. Dieselbe Wirkungskette tritt ein, wenn die NutzerInnen das Vertrauen in die Währung verlieren, folglich sinkt auch deren Wert. Ebensolche Wirkungsmechanismen und Zusammenhänge von Wertverfall und Verlust der Akzeptanz durch die NutzerInnen können auch für virtuelle Währungen angenommen werden. Im Folgenden werden vier Elemente diskutiert, die das Vertrauen von potentiellen Bitcoin-NutzerInnen positiv bzw. negativ beeinflussen können.

Zum einen ist der Inflationsschutz als vertrauensschaffender Mechanismus zu nennen: Um einem Vertrauensverlust durch unbegrenzte Ausgabe vorzubeugen, sind Bitcoins mathematisch auf 21 Millionen begrenzt (Becker 2012 et al.). Die Knappheit bzw. Mengenbeschränkung soll dafür sorgen, dass ein gewisser, mit der Währung assoziierter Wert erhalten bleibt.

Zum anderen ist die Pseudonymität zu nennen, die dem Bitcoin-System eigen ist (ECB 2015, S. 22). Diese ermöglicht gemeinsam mit kryptografischen Verfahren einen hohen Schutz der Privatsphäre, indem bei der Durchführung einer Transaktion zwischen zwei NutzerInnen deren physische Identität nicht preisgegegeben werden muss. Gleichzeitig ermöglicht die im dritten Abschnitt beschriebene Offenlegung der Block Chain auch vergangene Transaktionen mit realen Identitäten zu verknüpfen, wenn einer Bitcoin-Adresse externe Daten zur physischen Identität zugeordnet werden können (Bitcoin Foundation 2014, S. 5). An dieser Stelle soll zumindest erwähnt werden, dass Bitcoins auch für die Bezahlung von illegalen Waren eingesetzt werden. So geschehen z. B. bei Silk Road, einem 2003 geschlossenen Marktplatz im TOR-Netzwerk, das nicht über gängige Suchmaschinen erfasst werden kann. Andererseits ist etwa der Bereich der Spenden ein legaler Einsatzbereich von Bitcoin, der gerade bei politisch brisanten Einrichtungen wie der Enthüllungsplattform Wikileaks Zuwendungen in quasi anonymer Form ermöglicht (Becker 2012 et al.).

Ein dritter vertrauensschaffender Mechanismus liegt in der Verbreitung von physischen Ausformungen von Bitcoin sowie der Nutzung von dessen Symbol. Obwohl BTC-Münzen und -Scheine lediglich digitale Signaturen tragen, erfüllen sie doch eine wichtige Funktion. Menschen assoziieren weltweit mit Geld etwas Haptisches, besonders in Form von Banknoten und Münzen. Diese haptische Vertrautheit kann ebenso bei BTC-Münzen und -Scheinen zutage treten. Eine abstrakte Währung, die bislang eher Technik-affinen, Spekulanten und Interessierten zugänglich war, erhält durch physische Manifestationen von BTC somit das Potential, jedermann zu erreichen. Hierbei können auch Bestrebungen, die Standardisierung des Bitcoin-Logos und -Symbols voranzutreiben, den Wiedererkennungswert und die Akzeptanz der digitalen Währung steigern. Die allermeisten der bislang im Umlauf befindlichen BTC-Logos, -Symbole, -Scheine und -Münzen sind an etablierte

und global gehandelte FIAT-Währungen wie den US-Dollar oder den Euro angelehnt. Dies geschieht vermutlich nicht ohne Grund, sondern spiegelt eine Sehnsucht wider, dass Bitcoin ebenso weltweit Akzeptanz findet und genutzt wird.

Ein viertes Element, das die Vertrauensbildung dieser virtuellen Währung beeinflusst, ist die hohe Volatilität von Bitcoin im Wechselkurs zu FIAT-Währungen. Während beispielsweise ein Bitcoin am 11. April 2014 einen gewichteten Tageskurswert von 444,58 Euro hatte, war es am 11. April 2015 nur 224,82 Euro wert.[18] Die dezentrale Struktur von Bitcoin bewirkt, dass es keine zentrale Stelle gibt, die regulativ eingreift und Preisstabilität sicherstellt (ECB 2015, S. 23). Hohe Wertschwankungen kommen bei Bitcoin dadurch zustande, dass der Preis von Bitcoin ausschließlich durch das Angebot (der HändlerInnen) und die Nachfrage (der UserInnen) bestimmt wird. Um Preisschwankungen für HändlerInnen aufzufangen, haben sich Zahlungs-dienstleister wie PitBay gegründet, die für eine fixe monatliche Gebühr Bitcoin unmittelbar zu einem garantierten Wechselkurs in Euro oder US-Dollar umrechnen (ECB 2015, S. 14). Tendenziell wird die Volatilität der Währung durch ein niedriges Handelsvolumen und die geringe Akzeptanz von NutzerInnen verstärkt (ECB 2012). Gleichzeitig begünstigen gefestigte Sicherheitsmechanismen und eine vermehrte Nutzung die Stabilität der digitalen Währung Bitcoin. Mit diesen vier Mechanismen, die Vertrauensbildung bei Bitcoin beeinflussen, schließt der Abschnitt.

8. Resümee

In diesem Artikel wurde die virtuelle Währung Bitcoin unter dem Gesichtspunkt analysiert, wie ihre symbolischen und physischen

[18] https://www.bitcoin.de/de/chart [Zugriff am 13.04.2015].

Darstellungsformen dazu beitragen können, Vertrauen zu ihren (potentiellen) NutzerInnen zu schaffen bzw. dieses zu beeinflussen. Dazu wurde in einem ersten Schritt die digitale Währung in Bezug zu staatlich kontrollierten Währungen gesetzt. Darauf folgte eine Abgrenzung zu anderen virtuellen Währungen, wobei Bitcoin zu – am freien Markt gebildeten – Wechselkursen in FIAT-Währungen getauscht werden kann und vice versa. Sofern von Händlern akzeptiert, können mit Bitcoin Waren und Dienstleistungen erworben werden. Bei der Einschätzung der ökonomischen Rolle von BTC zeigte sich, dass die gesamtwirtschaftliche Bedeutung der virtuellen Währung derzeit begrenzt ist, obwohl es sich bei BTC um eine der bekanntesten seiner Art handelt. Als grundsätzliche Funktionsmechanismen von Bitcoin wurden das Peer-to-Peer-Prinzip und die dezentrale Abwicklung von Transaktionen beschrieben. Auch wurden zwei grundlegende Herausforderungen des Bitcoin-Systems analysiert, das ‚Double Spending'-Problem und der ‚Geldschöpfungs-prozess'.

Mit diesem Vorwissen zu Bitcoin wurden im nächsten Abschnitt BTC-Symbole und -Logos behandelt. Entsprechend dem dezentralen Funktionsprinzip der digitalen Währung gibt es keine zentrale Institution, die BTC-Logos und -Symbole verwaltet, vielmehr hängt es von der Akzeptanz der Community ab, welche Darstellungsformen sich durchsetzen. Bei der Untersuchung von physischen Ausformungen von Bitcoin wurden zwei Unterschiede zu FIAT-Währungen herausgearbeitet: zum einen, dass es keine zentrale Ausgabestelle für BTC-Münzen und -Scheine gibt; zum anderen, dass es sich bei physischen Formen um Träger der digitalen Signatur der virtuellen Währung handelt. Exemplarisch wurden eine BTC-Münze und ein BTC-Schein mit unterschiedlichen Vor- und Nachteilen betrachtet. Der letzte Abschnitt beschäftigte sich mit Vertrauen, das sowohl bei FIAT-Währungen als auch bei digitalen Währungen ein zentrales Element für die Akzeptanz der NutzerInnen darstellt. Im Besonderen wurden vier Mechanismen

untersucht, die Vertrauensbildung in das Bitcoin-System beeinflussen: der Inflationsschutz, die Pseudonymität, physische Formen von BTC und die Wechselkurs-Volatilität.

Zukünftige Entwicklungen von Bitcoin bleiben ungewiss, seriöse Prognosen lassen sich nur schwer abgeben. Jedenfalls hat die virtuelle Währung nicht den Status eines gesetzlichen Zahlungsmittels, wenngleich Funktionen von Geld teilweise erfüllt werden. Liegt der Zahlungsmittelfunktion das Versprechen zugrunde, dass mit der Währung ein gewisser Wert einhergeht, ist dieser bei Bitcoin von der Akzeptanz durch die NutzerInnen abhängig. Die Funktion als Wertaufbewahrungsmittel ist bei Bitcoin unsicher, ähnlich wie bei Geld (mit Ausnahme der Einlagensicherung). Die Funktion der Recheneinheit – die eine gemeinsame Sprache darstellt – ist bei Bitcoin ebenfalls erfüllt, jedoch um die Wechselkurs-Volatilität erschwert. Bislang ist die FIAT-Währung oftmals die Bezugsgröße, die dann in BTC umgerechnet wird.

Bitcoin kann als technologische Innovation gesehen werden, die nicht nur als alternative Zahlungsmethode, sondern auch durch ihre dezentral und pseudonym operierenden Netzwerke Chancen und Herausforderungen für NutzerInnen mit sich bringt. Ob diese oder eine andere virtuelle Währung sich mittelfristig etablieren kann, wird auch davon abhängen, ob die NutzerInnen daran glauben. Denn: Währungen funktionieren, weil Menschen daran glauben.

Dank

Dieser Beitrag basiert auf dem laufenden österreichisch-deutschen Forschungsprojekt BITCRIME; gefördert durch das österreichische Sicherheitsforschungs-Förderprogramm KIRAS – eine Initiative des Bundesministeriums für Verkehr, Innovation und Technologie (bmvit).

Literatur

Becker, Jörg / Breuker, Dominic / Heide, Tobias et al. (2012): Geld stinkt, Bitcoin auch – Eine Ökobilanz der Bitcoin Block Chain, in: GI-Jahrestagung 2012, S. 39-50.

Bitcoin Foundation (2014): Removing Impediment's to Bitcoin's Success: A Risk Management Study. Research Brief No. 1, https://bitcoinfoundation.org/wp-content/uploads/2014/04/Bitcoin-Risk-Management-Study-Spring-2014.pdf [Zugriff am 14.04.2015], S. 1-27.

Böck, Hanno (2013): Bitcoin. Kryptographie der virtuellen Währung,http://www.golem.de/news/bitcoin-krypotografie-der-virtuellen-waehrung-1305-99305.html [Zugriff am 23.03.2015].

Cawrey, Daniel (2014): Industry Group Aims to Change Bitcoin Symbol to 'B', http://www.coindesk.com/industry-website-advocate-bitcoins-unicode-symbol/ [Zugriff am 03.04.2015].

ECB – European Central Bank (2012): Virtual Currency Schemes, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [Zugriff am 18.02.2015], S. 1-53.

ECB – European Central Bank (2015): Virtual currency schemes - a further analysis, http://www.ecb.europa.eu/pub/ pdf/other/virtualcurrencyschemesen .pdf [Zugriff am 12.03.2015], S. 1-37.

Deutsche Bundesbank (2014): Geld und Geldpolitik, Frankfurt am Main.

FAFT – Financial Action Task Force (2014): Virtual currencies – Key Definitions and Potential AML/CFT-Risks, http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [Zugriff am 15.01.2015], S. 1-15.

Hajdarbegovic, Nermin (2014a): 10 Physical Bitcoins: the Good, the Bad and the Ugly, http://www.coindesk.com/10-physical-bitcoins-good-bad-ugly/ [Zugriff am 01.04.2015].

Hajdarbegovic, Nermin (2014b): Bitcoin Foundation to Standardise Bitcoin Symbol and Code Next Year, http://www.coindesk.com/ bitcoin-foundation-standardise-bitcoin-symbol-code-next-year/ [Zugriff am 03.04.2015].

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf [Zugriff am 14.03.2015], S. 1-9.

Schweizerische Eidgenossenschaft (2014): Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070), http://www.news.admin.ch/ NSBSubscriber/message/ attachments/35361.pdf [Zugriff am 16.03.2015], S. 1-32.

Abbildungen

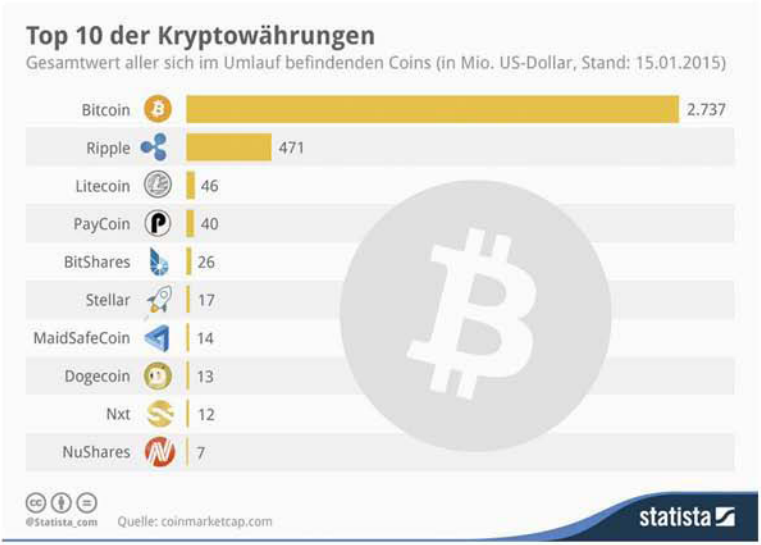

Abbildung 1: Vergleich des Wertes unterschiedlicher virtueller Währungen, http://de.statista.com/infografik/1939/marktkapitalisierung-von-krypto-waehrungen/, vom 15.01.2015 [Zugriff am 19.03.2015].

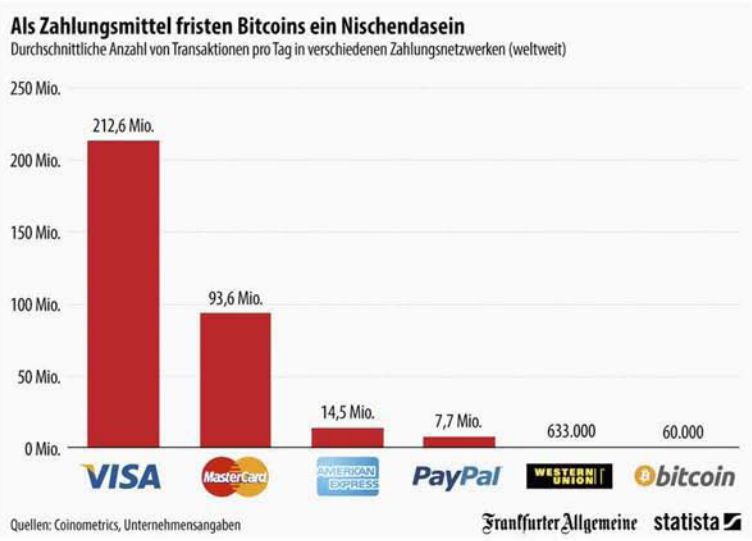

Abbildung 2: Bitcoin im Vergleich zu anderen elektronischen Zahlungsmitteln, http://de.statista.com/infografik/1771/transaktionen-pro-tag-in-zahlungsnetzwerken/, vom 13.01.2014 [Zugriff am 19.03.2015].

Abbildung 3: Beispiel eines populären Bitcoin-Logos, https://en.bitcoin.it/wiki/File:BC_Logo_.png, vom 23.04.2011 [Zugriff am 03.04.2015].

Abbildung 4: Verschiedene 3D-Darstellungen von Bitcoin

links: http://www.reddit.com/r/Bitcoin/comments/1a03gu/as_a_3d_artist_this_is_my_take_on_the_bitcoin/ [Zugriff am 04.04.2015].

Mitte: https://en.bitcoin.it/wiki/Promotional_graphics [Zugriff am 04.04.2015].

rechts: http://bitcoinsymbol.org/ [Zugriff am 01.04.2015].

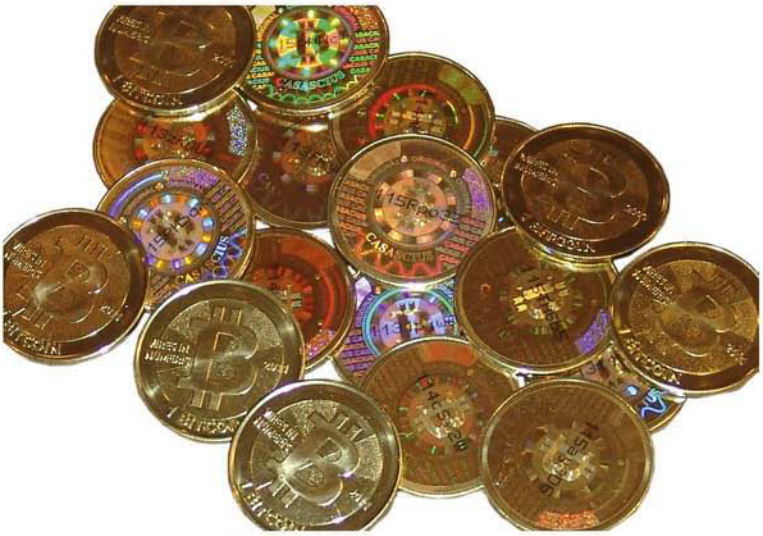

Abbildung 5: Beispiel für eine physische Bitcoin-Münze, https://www. casascius.com/photos.aspx [Zugriff am 02.04.2015].

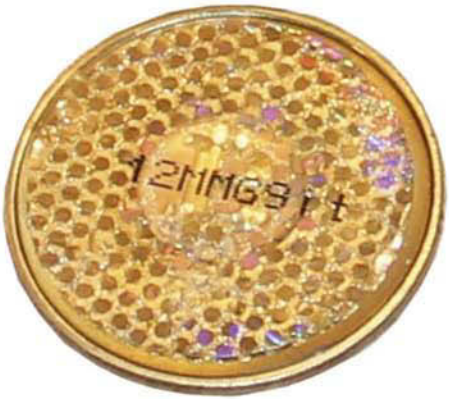

Abbildung 6: Entwertete Bitcoin-Münze, https://www.casascius.com/ photos.aspx [Zugriff am 02.04.2015].

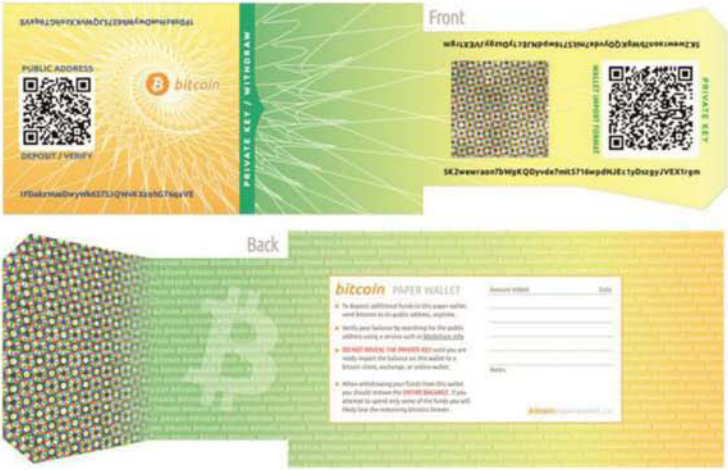

Abbildung 7: Beispiel für einen Bitcoin-Schein, https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html# [Zugriff am 02.04.2015].