Christoph Sorge, Artus Krohn-Grimberghe

Bitcoin: Eine erste Einordnung

<Appetizer>

Einleitung

Bitcoin erfreut sich als „digitale Währung“ wachsender Beliebtheit. Die Geschichte des Bitcoin-Systems beginnt, soweit öffentlich bekannt, im November 2008: Unter dem Pseudonym Satoshi Nakamoto gibt dessen bis heute unbekannter Entwickler die Veröffentlichung eines Artikels[1] über die Bitcoin-Technik bekannt[2]. Im Januar 2009 folgt der tatsächliche Start des Systems und die Veröffentlichung der Software, die für die Verwendung von Bitcoin benötigt wird.

Unklarheiten über die rechtlichen Rahmenbedingungen haben bislang zu Unsicherheit unter den Nutzern des Bitcoin-Systems geführt. Dieser Artikel versucht daher eine erste juristische Einordnung; zuvor soll jedoch ein Überblick über die Technik und den aktuellen Einsatz von Bitcoins gegeben werden.

1 Technik

Zum Verständnis der Arbeitsweise des Bitcoin-Systems ist es zunächst nötig, das Konzept hashbasierter kryptographischer Arbeitsbeweise zu beleuchten.

1.1 Grundlagen

Zentraler Baustein für Bitcoins sind (kryptographische) Hashfunktionen[3]. Wesentliche Eigenschaft solcher Funktionen ist, dass, es nicht effizient möglich sein darf, aus deren Ausgabe (dem Hashwert) auf einen dazu passenden Eingabewert zurückzuschließen. Ebenso wenig soll es möglich sein, zwei beliebige Eingabewerte zu finden, die auf den gleichen Hashwert abgebildet werden[4].

Hashfunktionen werden als Grundlage für Arbeitsbeweise eingesetzt. Bislang werden solche Arbeitsweise beispielsweise verwendet, um Denial-of-Service-Angriffe zu erschweren: Bevor ein Server Ressourcen (z.B. Rechenzeit) in die Bearbeitung der Anfrage eines Clients investiert, muss der Client nachweisen, für diese Anfrage ebenfalls Ressourcen investiert zu haben. Der Server schickt dazu eine Zeichenkette an den Client und stellt diesen vor die Aufgabe, eine zweite Zeichenkette zu finden, so dass der Hashwert der beiden aneinandergehängten Zeichenketten z.B. mit fünf Nullen beginnt. Der Client kann eine solche zweite Zeichenkette nur durch Ausprobieren ermitteln und braucht für das Finden einer passenden Lösung (für einen Hashwert, der mit n Nullen beginnen soll) im Mittel 2^{n-1} Versuche. Der Server kann aber in einem Schritt verifizieren, ob die Lösung den gestellten Anforderungen genügt, der Arbeitsbeweis also erbracht ist.

1.2 Bitcoin

Das Konzept elektronischer Bezahlverfahren mit eigenen Werteinheiten ist als solches nicht neu; bereits vor 25 Jahren stellten Chaum et al.[5] ein Verfahren vor, mit dem eine „Bank“ elektronische Münzen ausgeben kann, die später anonym eingelöst werden können (weder sieht die Bank, welcher Kunde bei welchem Händler eingekauft hat, noch können verschiedene Händler erkennen, ob sie den gleichen Kunden vor sich hatten).[6]

Elektronisch vorliegende Daten können beliebig kopiert werden. Dies stellt bei klassischen elektronischen Bezahlverfahren ein Problem dar, welches in den meisten Verfahren umgangen wird: die Bank kann das Kopieren einer Münze trotz der sonst gewährleisteten Anonymität erkennen und auf den Verursacher zurückführen. Ziel von Bitcoin ist es aber, ohne zentrale Kontrollinstanz auszukommen.

Bitcoin verzichtet aus diesem Grund (trotz des Namens) auf das Konzept elektronischer Münzen und verwendet stattdessen lediglich Überweisungen, die mittels Schlüsselpaaren aus je einem öffentlichen und einem zugehörigen privaten Schlüssel ausgeführt werden können. Der öffentliche Schlüssel dient dabei als Empfangsadresse bei Überweisungen und kann als „Kontonummer“ interpretiert werden. Zusätzlich wird er von Dritten für die Verifikation von Überweisungen verwendet. Wichtig ist, dass nur der zu einem öffentlichen Schlüssel zugehörige (und geheim zu haltende) private Schlüssel Überweisungen erlaubt.

Die Bitcoin-Client-anwendung verfolgt die vergangenen Überweisungstransaktionen und leitet daraus für die Benutzer eine Saldenansicht ab. Um eine neue Transaktion vorzunehmen, verweist der Überweisende auf vorherige Transaktionen, mit denen er selbst Bitcoins erhalten hat. Darin enthalten sind die adressierten öffentlichen Schlüssel, denen die Bitcoins zugewiesen wurden. Weiterhin muss der Überweisende nachweisen, dass er zu jeder dieser vorherigen Transaktionen die zugehörigen privaten Schlüssel besitzt.

Der Überweisende erstellt nun eine Dateneinheit, die den öffentlichen Schlüssel des Empfängers, einen Hash über die Dateneinheit der vorherigen Transaktion(en) und eine vom Überweisenden erzeugte Signatur über beide Werte enthält. Zur Verifikation der Signatur wird lediglich der öffentliche Schlüssel des Überweisenden benötigt, der mit dem Zielkonto der vorherigen Transaktion(en) übereinstimmt. Dadurch, dass beim Überweisen der Hash der vorherigen Transaktions-Dateneinheiten mitsigniert wird, ist sichergestellt, dass die neue Transaktion den vorherigen zugeordnet ist.

Bei diesem Verfahren entsteht aber ein Problem analog zu doppelt ausgegebenen elektronischen Münzen: Der Kontoinhaber könnte zwei verschiedenen

[1] http://bitcoin.org/bitcoin.pdf

[2] Über eine Mailingliste zum Thema Kryptographie, siehe http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

[3] Siehe Dobbertin, Digitale Fingerabdrücke, DuD 2/1997, S. 82-87.

[4] Detaillierte Erläuterung z.B. in Albrecht Beutelspacher, Heike B. Neumann und Thomas Schwarzpaul: Kryptografie in Theorie und Praxis, Vieweg+Teubner, 2. Auflage, Wiesbaden 2010, S. 177.

[5] David Chaum, Amos Fiat und Moni Naor: Untraceable Electronic Cash. In Advances in Cryptology — CRYPTO' 88, Springer, Berlin/Heidelberg 1990, S. 319-327. Lecture Notes in Computer Science, Band 403.

[6] Siehe Petersen, Anonymes elektronisches Geld, DuD 7/1997, S. 403-410.

Empfängern nachweisen, einen ausreichenden Betrag erhalten zu haben, und sein Konto durch Überweisungen an beide Empfänger überziehen. Bitcoin löst diese Problematik wie folgt: Wird von einem Konto der gleiche Betrag mehrfach ausgegeben, besitzt immer nur die erste dieser Transaktionen Gültigkeit – es muss also einen Weg geben, die erste Transaktion zu identifizieren. Um den Zeitpunkt einer Transaktion später nachzuweisen, verwenden andere Systeme Zeitstempel-Server. Da bei Bitcoin keine zentrale Instanz zum Einsatz kommen soll, geht man hier einen anderen Weg: Transaktionen werden an alle Teilnehmer gesendet, die diese dann in Blöcken sammeln und jeweils versuchen können, einen Arbeitsbeweis zu berechnen. Teilnehmer, die sich an diesem Versuch beteiligen, werden als „Miner" bezeichnet. Der erste erfolgreiche Miner schickt den neuen Block mitsamt dem Arbeitsbeweis an alle anderen Teilnehmer. Da jeder Block einen Hashwert des vorherigen Blocks enthält, entstehen so Ketten von Transaktionsblöcken. Die längste Kette, die auch als *Blockchain* bezeichnet wird, gilt als korrekt, und weitere Blöcke werden dort angehängt.

Ein Angreifer, der eine Transaktion löschen möchte, muss den Block, der sie enthält, modifizieren – dies bedeutet, dass er den Arbeitsbeweis für diesen Block und alle darauffolgenden neu berechnen muss. Er muss dies zudem schneller tun, als das Kollektiv der anderen Teilnehmer wiederum weitere Blöcke an die längste Kette anhängt.

Ein Teilnehmer, der einen Arbeitsbeweis vor allen anderen erbracht hat, darf sich die mit den verarbeiteten Transaktionen verknüpften Transaktionsgebühren sowie eine Belohnung („Block Reward") für das Erbringen des Arbeitsbeweises gutschreiben; diese Belohnung ist der einzige Weg, auf dem Bitcoins geschöpft werden. Die Rate der Geldschöpfung sinkt, so dass nicht beliebig viele Bitcoins geschöpft werden können. Dies muss der Verbreitung von Bitcoin jedoch nicht im Wege stehen, da auch Transaktionen mit sehr kleinen Bruchteilen von Bitcoins möglich sind. Die Verwendung dieser Bruchteile führt dazu, dass aus technischer Sicht eine nahezu beliebige Geldmenge zur Verfügung steht, auch wenn die ökonomischen Folgen noch zu untersuchen wären.

Das Bitcoin-System speichert (sieht man von diversen Optimierungen ab) die gesamte Transaktionshistorie seit der ersten Bitcoin-Transaktion. Zwar ist dieses Konzept nicht besonders datenschutzgerecht, doch kann zumindest jeder Teilnehmer beliebig viele Konten haben und sich sogar für einzelne Transaktionen neue Konten erschaffen; dies erschwert das Zusammenführen aller Transaktionen eines Besitzers.

Das Mitteilen aller Transaktionen an alle Teilnehmer stellt weiterhin auch ein Problem für die Skalierbarkeit von Bitcoin dar[7]. Diesem Problem kann durch eine stärkere Zentralisierung begegnet werden – beispielsweise könnten einige wenige Banken das eigentliche Bitcoin-System untereinander betreiben und nur diese Banken tatsächlich Transaktionen bearbeiten.

2 Das Bitcoin-Ökosystem

In diesem Abschnitt widmen wir uns der Umsetzung des Bitcoin-Systems in die Praxis.

2.1 Technischer Betrieb

Die Blockchain, die oben beschriebene Kette von Transaktionsblöcken, ist das Fundament des Bitcoin-Ökosystems. Sie erlaubt jedem Bitcoin-Nutzer, Überweisungen – und somit Kontostände – genau zu verfolgen, und ihre Fortschreibung dient dem Festschreiben neuer Transaktionen und der Schöpfung neuer Bitcoins.

Zugang zur Blockchain erlauben sowohl Dienste wie blockexplorer.com oder blockchain.info, welche Informationen über die bereits gefundenen Arbeitsbeweise und die in den Blöcken enthaltenen Transkationen bieten, als auch die für Endbenutzer bestimmten „wallet"-Anwendungen. Jene Brieftaschen bewahren die Schlüsselpaare eines oder mehrerer Benutzer auf und bieten so Zugriff auf die Bitcoinbeträge, welche mit den jeweiligen Schlüsselpaaren verbunden sind. Weitere wesentliche Funktionen sind die Abwicklung von Überweisungen und das Erzeugen neuer Schlüsselpaar bzw. das Verwalten eines Adressbuchs.

Als Brieftaschen beliebt sind sowohl (trotz immenser Sicherheitsrisiken) Online-Dienste, die von überall auf der Welt Zugriff versprechen, als auch die „offizielle" Bitcoin-Clientanwendung[8], welche aktuell von einem Kern-Entwicklerteam als Open Source gepflegt wird. Seit Mitte letzten Jahres zeigte sich jedoch deutlich, dass sowohl Online-Dienste als auch „der" Bitcoin-Client einige Sicherheitsmängel aufweisen, wenn sie ohne die nötige Sorgfalt verwendet werden.

So kamen MyBitcoin.com, dem seinerzeit größten Anbieter von „Online Wallets", im Juli letzten Jahres rund die Hälfte der verwalteten 50.000 Bitcoins (bei einem damaligen Marktwert von über 20 USD je Bitcoin) abhanden, bevor der Betreiber der Seite abtauchte[9]. Etwa zur gleichen Zeit wurden einem Nutzer 25.000 Bitcoins gestohlen: Ein Schadprogramm kopierte die Datei wallet.dat mit seinen privaten Schlüsseln[10]. Dieser Angriff war sehr einfach durchzuführen, da die Datei durch den „offiziellen" Bitcoin-Client unverschlüsselt abgelegt wurde. In der aktuellen Version wurde diesbezüglich Abhilfe geschaffen und wurden Angriffe erschwert. Der Vorfall hat zudem mehreren Projekten zu alternativen Clients Anschub gegeben; eine Anwendung, die speziell auf sicherheitsbewusste Nutzer abzielt, befindet sich bereits kurz vor Fertigstellung der ersten öffentlichen Version[11].

Die Bitcoin-Miner stellen den zweiten Interaktionsmechanismus mit der Blockchain und somit die tragende Säule von Bitcoin dar. Während auf der einen Seite sämtliche Clientanwendungen die Blockchain lediglich lesen und neue Transaktionen nur im Netz ankündigen können, bestimmen die Bitcoin-Miner, welche Transaktionen in die Blockchain aufgenommen werden. Sie erfüllen eine notwendige Schutzfunktion, indem sie ungültige Transaktionen ignorieren, während sie eine steigende Anzahl von Transaktionen im Bitcoin-Netz festschreiben.

Während sich bis vor etwa einem Jahr jeder Nutzer alleine an die Erbringung von Arbeitsbeweisen machen konnte, ist dies aufgrund der aktuellen Rechenzeitanforderungen für die meisten Einzelpersonen nicht mehr sinnvoll möglich: ein typisches System mit einer Hashrate von 500 MHash/s hat innerhalb von vierzehn Tagen nur eine etwa elfprozentige Chance, einen Arbeitsbeweis zu finden[12]. Weiterhin steigt aktuell alle 14

[7] Darauf weist auch Dan Kaminsky in einem Vortrag hin, s. http://www.slideshare.net/dakami/bitcoin-8776098 (Folien 8ff.), abgerufen am 28.03.2012

[8] http://bitcoin.org/

[9] http://www.betabeat.com/2011/08/05/mybitcoin-disappeared-with-bitcoins/

[10] https://bitcointalk.org/index.php?topic=16457.msg214423#msg214423

[11] http://bitcoinarmory.com/

[12] https://en.bitcoin.it/wiki/Why_pooled_mining

Tage die Schwierigkeit um etwa 6,5%[13], womit sich die Wahrscheinlichkeit eines Arbeitsbeweises entsprechend reduziert.

Aus diesem Grund ist der Zusammenschluss von Minern zu sogenannten Pools beliebt, bei denen gemeinsam daran gearbeitet wird, den jeweils nächsten Arbeitsbeweis zu finden. Aktuell gibt es mehr als 30 eingetragene Mining-Pools auf bitcoin.it, dem meistgenutzten Bitcoin-Wiki. Die beiden größten Pools bringen jedoch zusammen bereits rund 50% der gesamten Hashrate des Netzes auf. Der größte Pool, deepbit, erreichte bereits mindestens einmal die 50%-Marke[14]. Diese Konzentration ist nicht unproblematisch, denn 50% der Rechenleistung des Gesamtsystems sind für einen Angreifer ausreichend, um Arbeitsbeweise für eine gefälschte Blockchain zu erbringen, die von den Bitcoin-Clients als legitim akzeptiert wird. Eine zu hohe Konzentration der Rechenleistung von Bitcoin-Minern birgt auch das Risiko, dass ein Denial-of-Service-Angriff an einer einzigen Stelle zu einem erheblichen Verlust an Rechenleistung führt, wie bereits einmal im Juni 2011 geschehen[15].

Insgesamt wird auf Seiten der Bitcoin-Miner aktuell eine kombinierte Hashleistung von 11,5 Terahashes/s aufgewendet[16]. Dieser Wert lässt sich nicht direkt mit dem üblichen Maß der Rechenleistung von Supercomputern vergleichen; eine Überschlagsrechnung[17] führt jedoch zu ungefähr dem 80. Platz auf der Top500-Liste der Supercomputer vom November 2011[18] (entsprechend ca. 150 Petaflops) oder etwa 29,000 Desktopcomputern mit einer leistungsfähigen Grafikkarte für etwa 300 USD (AMD Radeon HD 6970)[19].

2.2 Handel und Tausch

Neben der Verwaltung und Überweisung von Bitcoins auf der einen Seite und dem Schöpfen neuer Bitcoins und dem Erhalt von Transaktionsgebühren auf der anderen Seite spielte der Tausch von Bitcoins von Anfang an eine große Rolle, nicht zuletzt auch, weil andere Nutzungsmöglichkeiten sehr spärlich gesät waren. Während ursprünglich der Tausch von Bitcoins gegen virtuelle Güter wie „Second Life Linden Dollar“ dominierte, stellt mittlerweile der US-Dollar das wichtigste Tauschgut dar[20]. Neben der Möglichkeit des Over-the-Counter-Handels floriert das Geschäft der Wechselstuben. MtGox.com hat in diesem Marktsegment eine deutliche Vormachtstellung, insbesondere nachdem mit TradeHill.com der größte Konkurrent Mitte Februar den Betrieb eingestellt hat. MtGox wickelt derzeit mit einem Handelsvolumen von etwa 2,2 Millionen BTC pro Monat bei einem durchschnittlichen Handelspreis von 4,90 USD je BTC das 35-fache Volumen des nächstkleineren Anbieters ab[21]. Fortgeschrittene Handelsoptionen wie Short-Selling und Leverage bietet beispielsweise der Dienst Bitcoinica, welcher nach eigenen Angaben bereits für etwa ein Drittel des Handelsvolumens auf MtGox.com verantwortlich ist.

In zunehmendem Maß wird Bitcoin auch ganz ähnlich wie klassische elektronische Bezahlverfahren eingesetzt. Während sie zu Anfang lediglich von anderen Enthusiasten zum Ausgleich von Verbindlichkeiten akzeptiert wurden, bildete sich rasch ein Geflecht zumdeist dubioser bitcoinakzeptierender Dienstleister. Stellvertretend für jene Dienstleistungen, welche insbesondere dem Substanzmissbrauch zugerechnet wurden, steht der Online-Marktplatz Silk Road, welcher im Februar 2011 öffnete. Nach diesen Anfängen hat sich das Spektrum der Dienstleistungen und Güter, die für Bitcoins angeboten werden, jedoch deutlich erweitert. So listet das Bitcoin-Wiki unter der Rubrik „Handel“[22] derzeit über 700 Akzeptanzstellen von Bitcoins für Beratung, Erwerb von Edelmetallen, IT-Dienstleistungen, Blumen, Kleidung, Büchern und vielem mehr auf, welche sich allesamt verpflichten, keine in den USA oder in Japan illegalen Leistungen oder Produkte anzubieten. Auch gibt es mittlerweile mehrere Online-Auktionshäuser, welche über Bitcoins abrechnen, und erste Anwaltskanzleien und Steuerberater, die ihre Dienste gegen Bitcoins offerieren. Unterstützt wird dies dadurch, dass bereits Zahlungsdienstleister die Abwicklung von Bitcoin-Zahlungen anbieten.

Das aktuelle Handelsvolumen und der Wechselkurs von Bitcoin schwanken stark. In den 30 Tagen bis zum 16.03.2011 wechselten beispielsweise 2,5 Millionen BTC zu einem durchschnittlichen Marktpreis von 4,74 USD den Besitzer. Zehn Tage später sind es nur noch rund 2,2 Millionen BTC, dafür jedoch mit einem durchschnittlichen Marktpreis von 4,90 USD[23]. Betrachtet man Bitcoin als handelbares Gut, so lag die Marktkapitalisierung am 16.03.2012 bei etwas über 34 Mio. EUR (44,9 Mio. USD)[24]. Ihren Höchststand hatte die Marktkapitalisierung am 08.06.2011 mit 188 Mio. USD bei stündlich gemittelten Preisen[25]. Das tägliche Überweisungsvolumen liegt derzeit bei etwa 700.000 USD mit Spitzen von über 17 Millionen US-Dollar am 6. Dezember 2011[26].

Die wirtschaftliche Bedeutung von Bitcoin zeigt sich auch darin, dass Bitcoin-Nutzer und -Dienstleister vermehrt in das Visier von Kriminellen geraten. So wurden alleine seit Juni letzten Jahres in vier spektakulären Fällen mindestens rund 100.000 Bitcoins mit einem Marktwert von über einer Mio. USD entwendet[27].

Ein wesentlicher Faktor für die Chancen von Bitcoin ist die Bewertung durch Geschäftsbanken. Jene stehen Bitcoin aktuell eher kritisch gegenüber[28]. So beklagen sich Bitcoin-Unternehmer über Kontoschließungen bzw. die Weigerung, Konten zu eröffnen[29].

2.3 Die Bitcoin-Community

Die aktuellen Trends und Strömungen in der Gemeinschaft der Bitcoin-Nutzer spiegeln sich vor allem bei bitcointalk.org, dem größten Bitcoin-Forum, und in verschiedenen Bitcoin-bezogenen Kanälen des Internet Relay Chats wider.

[13] http://bitcoin.sipa.be/, abgerufen am 16.3.2012

[14] http://www.bitcoinminer.com/post/5328668205/deepbit-50-percent-threshold

[15] http://bitcointalk.org/index.php?topic=14520.0

[16] http://bitcoinwatch.com/ am 13. März 2012

[17] ebda.

[18] http://www.top500.org/lists/2011/11

[19] https://en.bitcoin.it/wiki/Mining_hardware_comparison - Grafikkarten eignen sich besonders für die von Bitcoin benötigten Rechenoperationen.

[20] http://bitcoincharts.com/markets/

[21] Werte ermittelt am 25.3.2012

[22] https://en.bitcoin.it/wiki/Trade

[23] http://bitcoincharts.com/markets/

[24] http://bitcoincharts.com/bitcoin/

[25] http://bitcoincharts.com/charts/

[26] http://blockchain.info/charts/estimated-transaction-volume-usd

[27] Siehe https://bitcointalk.org/index.php?topic=16457.msg214423#msg214423, https://bitcointalk.org/index.php?topic=66979.0, http://www.betabeat.com/2011/08/05/mybitcoin-disappeared-with-bitcoins/, https://bitcointalk.org/index.php?topic=66916.0

[28] http://www.finextra.com/news/fullstory.aspx?newsitemid=23440

[29] So zum Beispiel bei MtGox und TradeHill. S. http://tradehillblog.com/2012/02/13/tradehill-suspending-trading-and-returning-client-funds/ Dabei muss jedoch davon ausgegangen werden, dass neben Bitcoin im Regelfall andere riskante Aspekte der jeweiligen Geschäftsmodelle bei der Entscheidung, Kontoeröffnungen abzulehnen oder Kontoschließungen auszusprechen, den Ausschlag gegeben haben werden.

Zusätzlich gab es seit Anfang 2011 bereits Bitcoin-Tagungen mit dreistelligen Nutzerzahlen in New York, Prag und San Antonio. Im Dezember steht mit 500 Teilnehmern die bislang größte Tagung in London auf der Agenda. Daneben hat auch die Wissenschaft das Thema Bitcoin entdeckt: es gibt bereits erste wissenschaftliche Beiträge und einen Workshop zur Jahrestagung der Gesellschaft für Informatik.

Insgesamt ist das Bitcoin-Ökosystem noch in einem sehr jungen Stadium und geprägt von technischen getriebenen Entrepreneuren und Enthusiasten. Dies spiegelt sich in dem noch begrenzten und IT-lastigen Angebot von direkt in Bitcoin bezahlbaren Gütern und Dienstleistungen einerseits und den derzeit noch regelmäßig wiederkehrenden technischen und betriebswirtschaftlichen Malheuren bei wesentlichen Akteuren andererseits wider[30].

3 Wirtschaftliche Aspekte

Aus wirtschaftlicher Perspektive sind im Wesentlichen vier Aspekte an Bitcoin interessant:

Erstens die Möglichkeit, globale elektronische „Überweisungen" mit nur sehr geringen Kosten durchzuführen. Während die Gebühren von Banken und Zahlungsdienstleistern üblicherweise jenseits von 1% bzw. im zweistelligen EUR-Bereich liegen, kosten vergleichbare Transaktionen – wenn überhaupt – Bitcoin-Beträge im Promillebereich.[31] Es ist zwar zu erwarten, dass gleichzeitig mit der schrumpfenden Schöpfungsrate neuer Bitcoins auch die Transaktionsgebühren steigen, jedoch ist es das Ziel Bitcoins auch in Zukunft noch selbst für Micropayments oberhalb von 0,01 USD interessant zu bleiben[32].

Zweitens spricht insbesondere die Irreversibilität der Transaktionen im Bitcoin-Netzwerk die Zahlungsempfänger an. Während eine solche Irreversibilität üblicherweise für Bargeldzahlungen, innerdeutsche Überweisungen und die europäischen SEPA-Überweisungen gegeben ist, fehlt sie klassischerweise sowohl bei elektronischen Zahlungsdiensten wie Kreditkartenzahlungen und PayPal als auch den in den USA überwiegend genutzten ACH-Überweisungen. Ist die Irreversibilität von Zahlungen nicht gewährleistet, muss das Risiko des Zahlungsausfalls von den haftenden Parteien (üblicherweise Zahlungsdienstleister und Zahlungsempfänger) eingepreist werden. Diese Kosten entfallen bei Bitcoin. Andererseits hat der Besitzer von Bitcoins ein deutlich erhöhtes Verlustrisiko, das er durch entsprechende Vorkehrungen mindern muss.

Drittens das Fehlen einer zentralen Instanz oder einer Oligarchie von Intermediären. Dieses Merkmal verspricht, dass protokollkonforme Transaktionen zwischen zwei Parteien nicht von einer dritten Partei verhindert werden können und nicht eine Partei über den Zahlungsfluss im Netzwerk entscheiden kann. Die kürzlich durch PayPal und einige traditionelle Kreditkartenanbieter durchgeführte Blockade einzelner Zahlungsempfänger ist mit Bitcoin nicht möglich. Wie bereits angemerkt, kann sich aufgrund der steigenden Anforderungen des Bitcoin-Protokolls hinsichtlich Speicherplatz und Netzwerkdurchsatz eine Hierarchie im Netzwerk ähnlich der Aufteilung in Banken und Nutzer entwickeln; dennoch wird auch in einem solchen Szenario die Blockade von Transaktionen schwierig bleiben.

Viertens leistet Bitcoin im Vergleich mit aktuell eingesetzten elektronischen Bezahlverfahren wie Kreditkartenzahlung oder Paypal eine bessere Wahrung der Anonymität, wenngleich diese mit dem Verfahren von Chaum oder Bargeld nicht vergleichbar ist. Im Vergleich zu Bargeld fällt auch die bei Bitcoin erheblich höhere Transaktionsdauer auf: während der Zahler zwar seine Transaktion umgehend dem Netzwerk gegenüber bekannt macht, werden derzeit nur alle zehn Minuten Blöcke gefunden, die diese Transaktion festschreiben und damit bestätigen. Im Mittel muss so fünf Minuten auf dieses Ereignis gewartet werden. Bei höheren Beträgen verlängert das Bedürfnis nach mehreren Bestätigungen (nachfolgend gefundenen Arbeitsbeweisen, welche den Block mit der Zahlung referenzieren) die Transaktionsdauer gegenüber einer Bargeldtransaktion deutlich.

4 Einordnung: Was sind Bitcoins?

Für die Zukunft von Bitcoin und der Unternehmen, die damit handeln, ist die Frage von zentraler Bedeutung, wie aus wirtschaftlicher und rechtlicher Sicht, wie mit dem Bitcoin-System umgegangen werden soll. Dieser Artikel soll aus Sicht des deutschen Rechts einen Beitrag zur Klärung dieser Frage liefern.

Das Bitcoin-Wiki[33] bezeichnet Bitcoin als „digitale Währung"; dem juristischen Währungsbegriff wird das System indes nicht gerecht, denn dieser betrifft lediglich staatliche Geldordnungen[34].

4.1 E-Geld[35]

Naheliegender ist der Begriff des E-Geldes, der in §1a Abs. 3 Zahlungsdiensteaufsichtsgesetz (ZAG) definiert ist: Demnach ist E-Geld „jeder elektronisch, darunter auch magnetisch, gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge im Sinne des § 675f Absatz 3 Satz 1 des Bürgerlichen Gesetzbuchs durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird."

Fraglich ist hier aber bereits, ob bei Bitcoins ein „monetärer Wert" gespeichert wird. Zwar hat eine Bitcoin keinen in einer Währung festgelegten Wert, doch wird ihr seitens der Nutzer durchaus ein (wenn auch schwankender) Wert zugeschrieben. Diskutabel ist, ob dieser Wert auch „gespeichert" wird, da Bitcoin – ähnlich, wie das bei Buchgeld der Fall ist – nur Transaktionen speichert und nicht etwa digitale Münzen einsetzt. Die Speicherung der Transaktion, mit der ein Nutzer einen gewissen Betrag erhalten hat, ist jedoch im Ergebnis gleichwertig mit der Speicherung einer Münze, die diesen Betrag repräsentiert. Das Merkmal eines gespeicherten monetären Werts kann daher im Ergebnis bejaht werden.

Die Annahme, Bitcoins seien E-Geld, scheitert aber am Merkmal der „Forderung gegenüber dem Emittenten"[36], da

[30] So beispielsweise das Ende der seinerzeit bedeutsamen Handelsplattformen BitOMat.pl (https://bitcointalk.org/index.php?topic=33453.0) und TradeHill.com (http://tradehillblog.com/2012/03/06/dwollasuit/), zu dem mangelnde Professionalität der Akteure in erheblichem Umfang beigetragen haben dürfte.

[31] Je geringer die Transaktionslast im Netz, je mehr Bestätigungen die referenzierten Eingangstransaktionen bereits erhalten haben und je weniger Eingangstransaktionen benötigt werden, desto geringer fällt die Transaktionsgebühr aus, die der Standardclient vorschlägt. Notwendig sind Transaktionsgebühren jedoch nicht. Es muss sich lediglich ein Miner finden, der die Transaktion zu den angebotenen Gebühren durch Erbringen eines Arbeitsbeweises in einen Block einbaut.

[32] https://bitcointalk.org/index.php?topic=10702.20

[33] https://de.bitcoin.it/wiki/Hauptseite, abgerufen am 20.3.2012

[34] Grothe, Helmut: Fremdwährungsverbindlichkeiten. Verlag Walter de Gruyter, Berlin 1999, S. 12.

[35] Zu rechtlichen, volkswirtschaftlichen und technischen Aspekten elektronischen Geldes siehe auch Schwerpunktheft DuD 7/1997.

[36] So auch die Bundesanstalt für Finanzdienstleistungsaufsicht und die Generaldirektion Bin-

der Besitz von Bitcoins keine Forderung begründet oder belegt. Zudem ist fragwürdig, ob von einem Emittenten gesprochen werden kann: Bitcoins entstehen nur dadurch, dass Teilnehmer, die einen Arbeitsbeweis erstellt haben, sich selbst einen gewissen Betrag gutschreiben und andere Teilnehmer diese Gutschrift als legitim akzeptieren. Die Existenz von Tauschbörsen, die Bitcoins in reguläre Währungen umtauschen, ändert daran nichts; außerdem sind auch diese nicht zu einem Umtausch verpflichtet. Ob jeder Teilnehmer, der sich selbst Bitcoins gutschreibt, als Emittent eingestuft werden kann, ist diskutabel; mangels Erfüllung des Merkmals gespeicherter Forderungen kann dies jedoch dahinstehen.

4.2 Geld

Denkbar ist außerdem die Einordnung von Bitcoin als Geld. Es existiert keine einheitliche und allgemeingültige Definition des Geldbegriffs; vielmehr hängt diese vom Kontext ab[37]. Der strafrechtliche Geldbegriff der §§ 146ff StGB trifft nicht zu, denn er setzt voraus, dass Geld „vom Staat oder einer durch ihn dazu ermächtigten Stelle als Wertträger beglaubigt“[38] wird. Selbst, wenn man dieser staatlichen Theorie des Geldes nicht folgt, fehlt aber im Vergleich zu „klassischem“ Geld dessen weite Verbreitung – eine Voraussetzung, die sowohl in der Literatur[39] als auch von Behörden gesehen wird: die mangelnde Verbreitung von Bitcoins bewog beispielsweise die Financial Services Authority des Vereinigten Königreichs dazu, Bitcoin die Geldeigenschaft abzusprechen[40].

Dennoch lohnt sich ein Blick auf weitere Merkmale von Geld. Aus ökonomischer Sicht sind das seine Funktionen als Zahlungs- bzw. Tauschmittel, als Wertaufbewahrungsmittel sowie als Wertmaß und Rechnungseinheit[41]. Bitcoin ist grundsätzlich zur Erfüllung der Tausch- und Zahlungsmittelfunktion geeignet: Waren und Dienstleistungen können gegen Bitcoins getauscht werden, anstatt einen direkten Austausch von Waren oder Dienstleistungen gegeneinander durchzuführen, und dies wird auch in derzeit zwar sehr geringem, aber steigendem Umfang praktiziert. Die Wertaufbewahrungsfunktion (siehe dazu auch unter „E-Geld“) ist dadurch gegeben, dass Bitcoin als System ein Speichern von Gegenwerten erlaubt und nicht die sofortige Ausgabe von erworbenen Bitcoins erzwingt. Auch ermöglicht Bitcoin die abstrakte Repräsentation von Vermögen. Dass der Wert von Bitcoins schwankt, macht die Nutzung der Wertaufbewahrungsfunktion zu einem Risiko, doch gilt dies in unterschiedlichem Ausmaß sowohl für nahezu alle Währungen als auch für Edelmetalle und wird gemäß des Nominalismusprinzips in der Literatur als unbeachtlich angesehen, solange keine Hyperinflation vorliegt[42].

4.3 Rechnungseinheit

Eine nähere Betrachtung lohnt sich bezüglich des Begriffs der Rechnungseinheit[43]. Der Begriff ist nicht legaldefiniert, und eine allgemein akzeptierte positive Definition findet sich auch in der Literatur nicht[44]. Jedenfalls dient eine Rechnungseinheit aber dazu, Werte von Gütern durch eine Mengenangabe in dieser Einheit ausdrücken zu können[45].

Selbst in den Online-Shops, die eine Bezahlung mit Bitcoins ermöglichen, wird der Wert von Gütern meist in Euro oder US$ angegeben. An der Eignung von Bitcoins als Wertmaß ändert das nichts, doch diese Eignung ist zunächst für jedes Gut gegeben – der Preis eines Liters Öl definierter Güte wäre für diese Funktion genauso denkbar, denn die Funktion als Rechnungseinheit hängt nicht von der tatsächlichen Verfügbarkeit oder Handhabbarkeit als Tauschmittel ab.

Angesichts der Rechtsfolgen, die das Kreditwesengesetz (KWG) an das Vorliegen einer Rechnungseinheit knüpft, kann die theoretische Eignung als Wertmaß zumindest im Sinne dieses Gesetzes nicht ausreichend sein. Umgekehrt würde die Einschränkung auf staatlich autorisierte Maßeinheiten dem Schutzzweck dieser Regelungen nicht gerecht werden, da diese durch Definition abgeleiteter Rechnungseinheiten umgangen werden könnten. Auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sieht dementsprechend „privatrechtlich ausgegebene Komplementärwährungen wie Regionalwährungen“ als Rechnungseinheiten an[46]. Insofern ist auf die tatsächliche Verwendung grundsätzlich geeigneter Einheiten als Maßeinheit für Werte von Gütern abzustellen.

Bitcoin wurde im September 2011 durch die BaFin nach Konsultation mit Bundesbank und dem Bundesministerium für Finanzen folgerichtig als Rechnungseinheit eingestuft[47]. Aus dieser Einordnung folgt nach § 1 Abs. 11 Satz 1 KWG, dass Bitcoins Finanzinstrumente im Sinne des § 1 Abs. 1 bis 3 und 17 KWG sowie im Sinne des § 2 Abs. 1 und 6 KWG darstellen. Dies führt insbesondere dazu, dass das gewerbsmäßige Erbringen der in § 1 Abs. 1a Satz 2 aufgeführten Dienstleistungen mit Bitcoins, wie beispielsweise der Betrieb eines multilateralen Handelssystems, der Erlaubnis der BaFin bedarf (§ 32 Abs. 1 KWG). Auch die (eng umgrenzte) Ausnahme des § 32 Abs. 6 KWG für ebenfalls erlaubnispflichtige Zahlungsinstitute ändert an diesem Ergebnis nichts.

Fazit

Betrugsfälle, Diebstähle und mangelnde Sorgfalt von Dienstleistern haben bereits zu großen finanziellen Verlusten bei Nutzern geführt. Nimmt man die hohen Umsätze mit Bitcoins hinzu, so wird deutlich, dass die Aufsichtspflicht, die sich aus der Einordnung als Recheneinheit ergibt, auch im Sinne der Nutzer ist. Sie trägt zur Rechtssicherheit bei und soll durch die erhöhten Anforderungen für Finanzdienstleistungsunternehmen eine gewisse Mindestbefähigung der betreffenden Dienstanbieter bewirken.

---

nenmarkt und Dienstleistungen der Europäischen Kommission als Antwort auf eine entsprechende Anfrage der Autoren in Bezug auf die E-Geld-Richtlinie. Ähnlich auch das Merkblatt „Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten“ der BaFin vom 22.12.2011, http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html

[37] Proctor, Charles: Mann on the Legal Aspect of Money, 6. Auflage. Oxford University Press 2005. Rn. 1.08

[38] BGH NJW 1984, 1311; auch Proctor (Rn 1.50) folgt diesem Geldbegriff in seiner Modern State Theory of Money.

[39] Proctor, Rn. 1.50

[40] So die Antwort auf eine entsprechende Anfrage an die FSA, die den Autoren vorliegt.

[41] Proctor, Rn. 1.07, mit weiteren Nachweisen. Die Funktionen Wertmaß und Rechnungseinheit werden in der Literatur oft gleichgesetzt.

[42] Proctor Kapitel 10; dagegen: Grothe, S. 16

[43] Als Synonym wird oft der Begriff der Recheneinheit verwendet.

[44] Auch Proctor (Rn. 2.34) weist auf diese Schwierigkeit hin.

[45] Proctor, Rn. 2.32. Rechnungseinheiten können unabhängig oder von anderen Rechnungseinheiten abgeleitet („Recurrent Link“) sein.

[46] Merkblatt „Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 Sätze 1 bis 3 KWG“ der BaFin vom 20.12.2011 mit Aktualisierungen bis März 2012, http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html

[47] Merkblatt der BaFin vom 22.12.2011 (siehe oben Fn. 36).

Weiterhin beseitigt diese Einordnung eine drohende Belastung von Bitcoins mit Umsatzsteuer, wie sie beispielsweise von den schwedischen Finanzbehörden befürwortet wird. Die Zukunft von Bitcoin bleibt dennoch ungewiss – so muss sich noch zeigen, ob angemessene Organisationsstrukturen für wachsende Transaktionszahlen gefunden werden und die technische Sicherheit aufrechterhalten werden kann. Nicht zuletzt sollte das System auch Akzeptanz außerhalb eines immer noch vergleichsweise kleinen Kreises von Enthusiasten gewinnen, um auf Dauer bestehen zu können.