DOI: 10.1007/s10273-013-1589-y

Christoph Sorge, Artus Krohn-Grimberghe

Bitcoin – das Zahlungsmittel der Zukunft?

Bitcoin[1] ist ein System, das zur elektronischen Bezahlung von Waren oder Dienstleistungen eingesetzt werden kann. Es wird auch als „virtuelle Währung" bezeichnet, denn Bitcoin ist nicht für die reine Zahlungsabwicklung entworfen worden. Vielmehr beinhaltet das System auch ein eigenes Wertmaß – der Preis von Gütern kann in der Einheit „Bitcoin" angegeben werden. Eine Währung im juristischen Sinne ist Bitcoin dennoch nicht, da Bitcoins weder vom Staat noch von einer staatlich ermächtigten Stelle ausgegeben werden. Vielmehr ist Bitcoin nach deutschem Recht wohl als Rechnungseinheit einzuordnen.[2]

Eine Besonderheit von Bitcoin ist seine dezentrale Organisationsform. So gibt es keine zentrale Instanz, die das System betreibt. Vielmehr handelt es sich um ein Peer-to-Peer-System: Jeder Rechner, der mit dem Internet verbunden ist, kann sich anschließen und als gleichberechtigtes Mitglied teilnehmen. Im Kern besteht Bitcoin aus einem Verfahren, das Überweisungen zwischen Konten der Nutzer ermöglicht – jeder Nutzer kann aber beliebig viele dieser Konten haben. Die Konten werden durch Bitcoin-Adressen identifiziert; in der Regel wird in der Literatur auch nur auf diese Adressen Bezug genommen.[3]

Der Verzicht auf eine vertrauenswürdige Instanz führt zu einer technischen Herausforderung: Mittels kryptographischer Verfahren kann man zwar einfach sicherstellen, dass von jedem Konto nur Beträge überwiesen werden, die vorher auf dieses Konto überwiesen wurden. Es gibt aber niemanden, der garantieren kann, dass ein Betrag von einem Konto nicht mehrfach überwiesen wird. Dieser Herausforderung begegnet Bitcoin durch die Veröffentlichung aller bereits durchgeführten Transaktionen. Diese Transaktionen werden dafür im Peer-to-Peer-System bekanntgegeben. Zunächst gelten neue Transaktionen als unbestätigt. Jeder Teilnehmer, der dies möchte, kann (als sogenannter „Miner") neue Transaktionen prüfen und der öffentlichen Liste bestätigter Transaktionen hinzufügen. Damit aber böswillige Teilnehmer (im Jargon der IT-Sicherheitsforschung: „Angreifer") nicht ohne weiteres Transaktionen unterdrücken oder fehlerhafte Transaktionen bestätigen können, erfordert die Bestätigung die vorherige Berechnung eines kryptographischen Arbeitsbeweises: Die Miner versuchen, eine Aufgabe zu lösen, die von der bisherigen Liste bestätigter Transaktionen und von den neu hinzugefügten Transaktionen abhängt und sehr großen Rechenaufwand erfordert. Wer dies zuerst schafft, fügt den (einfach zu überprüfenden) Beweis über die gelöste Aufgabe der neuen Liste bestätigter Transaktionen bei. Spätere Transaktionen werden der neuen Liste hinzugefügt, die dann wiederum auf dem gleichen Weg bestätigt wird.

Bestehen (beispielsweise aufgrund eines Angriffs) mehrere solcher Listen, so gilt diejenige als gültig, in die die meiste Rechenleistung geflossen ist. Eine Fälschung ist also nur möglich, wenn der Angreifer mehr Rechenleistung hat als alle legitimen Miner zusammengenommen.

Der Anreiz, als Miner Rechenleistung zu investieren, liegt einerseits in (geringen) Transaktionsgebühren, die in Bitcoin an die Miner gezahlt werden. Andererseits dürfen sich Miner auch einen Betrag „aus dem Nichts" gutschreiben. Dieser Betrag sinkt im Laufe der Zeit immer weiter. Da es keinen anderen Mechanismus gibt, um neue Bitcoins zu schaffen, ist die Gesamtzahl an Bitcoins, die jemals geschaffen werden können, beschränkt – es sei denn, die Gemeinschaft der Bitcoin-Teilnehmer einigt sich auf eine veränderte Variante der „Geldschöpfung".

Anonymität

Bereits seit den 1980er Jahren werden in der Informatik anonyme Bezahlverfahren diskutiert, bei denen der Betreiber einzelne Zahlungen den Teilnehmern nicht zuordnen kann und Händler anhand eines Bezahlvorgangs nicht einmal erkennen können, ob der gleiche Kunde schon einmal eine Transaktion mit ihnen durchgeführt hat.

Jun.-Prof. Dr. Christoph Sorge lehrt am Institut für Informatik der Universität Paderborn.

Jun.-Prof. Dr. Artus Krohn-Grimberghe lehrt dort am Institut für Analytische Informationssysteme und Business Intelligence.

1 Erstmals beschrieben in: S. Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, http://bitcoin.org/bitcoin.pdf – es handelt sich um eine reine Online-Veröffentlichung. Der Name des Autors ist vermutlich ein Pseudonym.

2 C. Sorge, A. Krohn-Grimberghe: Bitcoin – eine erste Einordnung, in: Datenschutz und Datensicherheit, 36. Jg. (2012), Nr. 7, S. 479-484.

3 In der Folge wird der Begriff „Konto" verwendet, da er eher dem normalen Sprachgebrauch entspricht.

Bitcoin bietet diese Eigenschaften nicht und ist nicht einmal mit dem Ziel der Anonymität entworfen worden. Dennoch wird dem System gelegentlich Anonymität unterstellt. Für die Teilnahme ist auch in der Tat keine Registrierung erforderlich, und somit kann sich jedermann beliebig viele Bitcoin-Konten anlegen. Andererseits können aber IP-Adressen der Parteien, die Transaktionen initiieren, aufgezeichnet werden. Mit Kenntnis einer IP-Adresse lässt sich (sofern kein Anonymisierungsnetz wie TOR verwendet wurde) in der Regel zumindest der Internet-Service-Provider und die Region des zugehörigen Internetanschlusses feststellen, bei Mitwirkung des Providers auch die Identität des Anschlussinhabers.

Dienstleistungen

Diverse Dienstleister haben sich im Bitcoin-Umfeld etabliert. Wesentliche Dienstleistungen sind insbesondere die Verwaltung von Bitcoin-Geldbörsen (insbesondere den zugehörigen kryptographischen Schlüsseln), der Umtausch von Bitcoins in Währungen wie Euro oder US-Dollar sowie das Angebot von Plattformen für spekulative Bitcoin-Geschäfte. MtGox als derzeit größte Handelsplattform setzt momentan rund 500 000 Bitcoin (entsprechend ca. 70 Mio. US-$) binnen 30 Tagen um.[4]

Auch gibt es mittlerweile eine Vielzahl von Akzeptanzstellen für Bitcoin. Zwar ist mit Silk Road einer der ersten prominenten Anbieter aufgrund des Eingreifens der Strafverfolgungsbehörden nicht mehr verfügbar – an seine Stelle sind jedoch zahlreiche legale Angebote getreten. Darunter fallen Onlineshops, Dienstleistungen aus dem IT-Umfeld, aber auch Rikscha-Fahrten, Lebensberatung und Partnerbörsen.

Teilnehmer

Die Erstellung genauer Statistiken zu den Teilnehmerzahlen ist schwierig, da sich – wie erwähnt – niemand für die Teilnahme am Bitcoin-System registrieren muss. Die Zahl der Konten, die an Transaktionen beteiligt sind, lässt sich zwar ermitteln. Jedoch kann jeder Teilnehmer sich beliebig viele Konten anlegen. In der Literatur wird daher eine Schätzung verwendet: Wenn Beträge von mehreren Konten in eine Transaktion eingehen, werden diese dem gleichen Teilnehmer zugeordnet. So fanden Ron und Shamir[5] im Mai 2012 ca. 3,1 Mio. Konten und ca. 2,5 Mio. Teilnehmer (wobei die Teilnehmerzahl eher als Obergrenze zu verstehen ist, da nicht notwendigerweise alle Konten eines Teilnehmers erfolgreich zusammengeführt werden können). In einer neueren Analyse (Stand: April 2013) wurden verschiedene Heuristiken verwendet, um die mittlerweile ca. 12 Mio. Konten auf 3,4 Mio. Teilnehmer abzubilden.[6]

Angriffe und Risiken

Der Entwurf des Bitcoin-Protokolls kann aus Sicht der IT-Sicherheit als sehr gelungen gelten. Bislang sind keine schwerwiegenden Fehler in Bitcoin bekanntgeworden – dies gilt allerdings nur, falls eine Grundannahme des Systems auch weiterhin erfüllt bleibt: Kein Angreifer darf mehr Rechenleistung zur Verfügung haben als alle ehrlichen Teilnehmer zusammengenommen. Gänzlich auszuschließen ist indes nicht, dass ein Angreifer dieses Ziel erreicht – beispielsweise, weil er es schafft, über eine Sicherheitslücke in einem gängigen Betriebssystem automatisiert viele Miner auf einmal unter seine Kontrolle zu bringen.

Bisherige Angriffe betreffen allerdings eher Dienstleister im Bitcoin-Umfeld; es finden sich zahlreiche Fälle, in denen Dienstleister Opfer von Angriffen, die zum Verlust von Bitcoins geführt habe, wurden. In einzelnen Fällen führte mangelnde Sorgfalt (fehlendes Backup) auch ohne Angriffe zu Datenverlust. Bis Mai 2013 sind, soweit öffentlich bekannt, mindestens 3 Mio. US-$ durch solche Zwischenfälle (Angriffe sowie mangelnde Sorgfalt der Anbieter) verlorengegangen.[7]

Für die Nutzer besteht noch ein weiteres Risiko: Der Wechselkurs zu Währungen wie dem US-Dollar oder dem Euro schwankt nicht unerheblich. Eine Darstellung für die Handelsplattform MTGox findet sich in Abbildung 1.

Effizienz und Kosten

Zwei wesentliche Kritikpunkte am Bitcoin-Sytsem sind seine mangelnde Skalierbarkeit und hohe (Energie-) Kosten, die durch das Mining – also das Bestätigen von Transaktionen, für das die Miner Belohnungen erhalten – entstehen.

Die mangelnde Skalierbarkeit liegt darin begründet, dass alle Transaktionen stets allen Bitcoin-Minern zur Verfügung gestellt werden müssen. Der daraus folgende Kom-

4 Laut http://bitcoincharts.com/markets/mtgoxUSD.html (5.10.2013).

5 D. Ron, A. Shamir: Quantitative Analysis of the Full Bitcoin Transaction Graph, in: Financial Cryptography and Data Security 2013, Lecture Notes in Computer Science, Bd. 7859, Berlin, Heidelberg 2013, S. 6-24.

6 S. Meiklejohn et al.: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Proceedings of the Internet Measurement Conference 2013, Veröffentlichung in Vorbereitung, Vorabversion unter http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

7 A. Krohn-Grimberghe, C. Sorge: Practical Aspects of the Bitcoin System, arXiv.org ePrint Service, arXiv:1308.6760, http://arxiv-web3.library.cornell.edu/abs/1308.6760.

Abbildung 1
Wechselkurs Bitcoin-US-Dollar bei MTGox
Tägliche Schlusskurse

Quelle: http://bitcoincharts.com/charts/mtgoxUSD#rg360ztgCzm1g10zm2g25. Diese Abbildung ist lizensiert unter Creative Commons Attribution-Share-Alike 3.0 Unported License, http://creativecommons.org/licenses/by-sa/3.0/deed.de.

munikationsaufwand ist momentan noch problemlos zu meistern. Bleibt die derzeitige Struktur bestehen, wird der Kommunikationsaufwand aber bei weiterem Wachstum so stark steigen, dass zumindest Privatnutzer nicht mehr in der Lage sein werden, als Miner an Bitcoin teilzunehmen. Einer Nutzung, um lediglich Zahlungen zu empfangen oder zu versenden, steht das jedoch nicht entgegen.

Bereits jetzt zeichnet sich ein zweites Problem von Bitcoin ab. Die Bestätigung von Transaktionen benötigt Rechenleistung – und je mehr Rechenleistung im Bitcoin-System zur Verfügung steht, desto schwieriger werden die zu lösenden Aufgaben gemacht, so dass deren Lösung im Durchschnitt immer ungefähr gleich lange dauert. Miner setzen daher immer stärker auf spezielle Hardware – die Hauptprozessoren handelsüblicher PCs sind im Vergleich so langsam, dass sich deren Nutzung für das Mining nicht mehr lohnt. Laut einer Schätzung von blockchain.info[8] liegt der kumulierte Energiebedarf der Miner aktuell bei ca. 23,5 GWh über einen Zeitraum von 24 Stunden – die Leistungsaufnahme liegt dieser Schätzung nach also in der Größenordnung der Leistung eines Atomkraftwerks. Da nur die gesamte Rechenleistung beobachtbar ist, die Leistungsaufnahme für die durchgeführten Berechnungen sich aber je nach eingesetzter Hardware erheblich unterscheidet, kann die Schätzung durchaus stark vom korrekten Wert abweichen. Bedenkt man aber, dass nie mehr als 75 000 Transaktionen pro Tag durchgeführt wurden,[9] so wird trotz dieser Ungenauigkeit deutlich, dass Bitcoin alles andere als energieeffizient ist. Da die benötigte Rechenleistung nicht direkt von der Transaktionszahl abhängt, ist eine Steigerung der Energieeffizienz (ebenso wie das Gegenteil) durchaus denkbar. Soll Bitcoin dauerhaft weiter bestehen, so wird eine verbesserte Energieeffizienz notwendig werden – ebenfalls laut Schätzung von blockchain.info arbeitet der durchschnittliche Miner angesichts der Energiekosten momentan mit Verlust.[10] Dieser Zustand wird sich kaum dauerhaft aufrechterhalten lassen.

Fazit

Das Bitcoin-System ist das erste Bezahlsystem, das auf einem Peer-to-Peer-Netz basiert und praktisch eingesetzt wird. Für die Teilnehmer birgt es zur Zeit noch Risiken und ist auch kaum als effizient zu bezeichnen, doch bringt die Unabhängigkeit von einem zentralen Anbieter auch Vorteile. Sollte das System weiter wachsen, wird sich wohl nur noch eine kleinere Zahl von Nutzern als Miner beteiligen können, womit der ursprüngliche Charakter von Bitcoin ein Stück weit verlorengeht.

8 Vgl. https://blockchain.info/de/stats (5.10.2013).

9 Vgl. https://blockchain.info/de/charts/n-transactions (5.10.2013).
10 Vgl. Fußnote 8.