Dominik Leibenger; Christoph Sorge

Automatismen in einem verteilten System: Das Beispiel Bitcoin

2016

https://doi.org/10.25969/mediarep/3938

Veröffentlichungsversion / published version
Sammelbandbeitrag / collection article

Empfohlene Zitierung / Suggested Citation:
Leibenger, Dominik; Sorge, Christoph: Automatismen in einem verteilten System: Das Beispiel Bitcoin. In: Norbert Otto Eke, Lioba Foit, Timo Kaerlein u.a. (Hg.): *Logiken strukturbildender Prozesse. Automatismen.* Paderborn: Fink 2016 (Schriftenreihe des Graduiertenkollegs "Automatismen"), S. 161–174. DOI: https://doi.org/10.25969/mediarep/3938.

Erstmalig hier erschienen / Initial publication here:
https://nbn-resolving.org/urn:nbn:de:hbz:466:2-24709

DOMINIK LEIBENGER, CHRISTOPH SORGE

AUTOMATISMEN IN EINEM VERTEILTEN SYSTEM: DAS BEISPIEL BITCOIN

Ein wesentlicher Aspekt gängiger Automatismen-Definitionen ist die Betrachtung von Automatismen als „Abläufe, die sich einer bewussten Kontrolle weitgehend entziehen“[1]. Versteht man die Informatik als eine ingenieurwissenschaftliche Disziplin, so erscheint das Auftreten von Automatismen zunächst überraschend: Wird ein informationsverarbeitendes System entworfen, erwarten die Nutzer in aller Regel ein deterministisches Verhalten. Diese Sichtweise greift aber zu kurz: So kann einerseits die Interaktion mit der Umwelt und menschlichen Nutzern zum Auftreten von Automatismen in informationsverarbeitenden Systemen führen[2]; andererseits wird beim Systementwurf oft versucht, ein bestimmtes, emergentes Verhalten durch Schaffen geeigneter Rahmenbedingungen hervorzurufen.[3]

Der vorliegende Beitrag beleuchtet nun ein konkretes Beispiel – nämlich das Bitcoin-System, das als Peer-to-Peer-Bezahlsystem in jüngerer Zeit Aufmerksamkeit auf sich gezogen hat. Hier sind verschiedene Formen von Automatismen zu beobachten: Einige sind für das Funktionieren des Systems erforderlich; andere produzieren Informationen, die nicht erwünscht sind. Zum Teil wurden ihre Voraussetzungen beim Systementwurf (vermutlich bewusst) geschaffen; zum Teil treten sie vollständig ungeplant auf. Daneben zeigen sich Entwicklungen, die den genannten Automatismen entgegenwirken und direkten Einfluss auf das Bitcoin-System haben. Es sei angemerkt, dass der Fokus des vorliegenden Textes zwar auf dem Bitcoin-System liegt, einige der beobachteten Effekte aber durchaus auch in anderen Peer-to-Peer-Systemen zu beobachten sind.

Nach einer Einführung in Peer-to-Peer-Systeme sowie die Besonderheiten von Bitcoin arbeitet dieser Beitrag heraus, wie und an welcher Stelle Automa-

---

1 Hannelore Bublitz/Roman Marek/Christina L. Steinmann/Hartmut Winkler (Hg.), *Automatismen*, München, 2010.

2 Dies wurde in einem Beitrag von Karl für Telekommunikationssysteme aufgezeigt: Holger Karl, „Struktur aus Zufall: Entstehung von Abhängigkeiten in Telekommunikationssystemen“, in: Hannelore Bublitz/Roman Marek/Christina L. Steinmann/Hartmut Winkler (Hg.), *Automatismen*, München, 2010, S. 71-78.

3 Das konkrete Ergebnis der dabei wirkenden Automatismen kann natürlich nicht sicher vorhergesagt werden. Weich spricht in diesem Zusammenhang auch davon, „Automatismen [zu] provozieren“. Andreas Weich, „These 7: Profile sind Selbst-Technologien. Sie setzen über planvoll eingesetzte mediale Infrastrukturen ungesteuerte Dynamiken des Selbstmanagements und der Entstehung von Wissensstrukturen in Gang“, in: Hannelore Bublitz/Irina Kaldrack/Theo Röhle/Mirna Zeman (Hg.), *Automatismen – Selbst-Technologien*, München, 2013, S. 311-316.

tismen im Bitcoin-System wirken. Entautomatisierend wirkende, entgegengesetzte Effekte werden im Anschluss diskutiert. Dabei sollen neben der Sicht der Informatik auch ökonomische und juristische Fragestellungen angerissen werden.

1. Peer-to-Peer-Systeme

Peer-to-Peer-Systeme erbringen einen Dienst, ohne dafür auf einen zentralen Server angewiesen zu sein. Alle Teilnehmer (auch als „Peers“ bezeichnet) können konzeptionell die gleiche Funktionalität erbringen. Ein gängiges Beispiel sind Filesharing-Netze, bei denen die Teilnehmer untereinander Dateien austauschen – diese werden also nicht auf einem zentralen Server gespeichert. In der Regel ist die Teilnahme an einem Peer-to-Peer-System offen – es kann also potenziell jeder Internetnutzer teilnehmen.

Mischformen zwischen einer Peer-to-Peer- und einer Client/Server-Architektur existieren – so erfolgt beispielsweise bei der IP-Telefonie-Software Skype[4] die Authentifizierung gegenüber einem Authentifizierungsdienst, der von Skype zentral betrieben wird. Die eigentliche Kommunikation wird jedoch in der Regel zwischen den einzelnen Peers selbst abgewickelt.

Zahlreiche Dienste, die auf Basis einer Client/Server-Architektur erbracht werden, sind prinzipiell auch als Peer-to-Peer-Systeme denkbar. Ein Problem, das bei der Umsetzung als reines Peer-to-Peer-System entsteht, ist allerdings das Fehlen einer als vertrauenswürdig bekannten Komponente – ohne eine solche erscheint beispielsweise die Umsetzung eines Bezahlverfahrens zunächst als unmöglich. Das Bitcoin-System zeigt aber, dass diese Annahme falsch ist.

2. Bitcoin

Das von Satoshi Nakamoto[5] entwickelte und im Jahr 2008 veröffentlichte Bitcoin-System ist ein elektronisches Bezahlsystem, das als reines Peer-to-Peer-System organisiert ist. Es kommt also völlig ohne zentrale Instanz aus. Aufgrund seiner aus Sicht der Informatik interessanten Eigenschaften, aber auch seiner schnellen Verbreitung wurde das System Gegenstand zahlreicher Forschungsarbeiten.[6]

---

4 *Skype*, online unter: http://www.skype.com/de/ zuletzt aufgerufen am 21.08.2013.

5 Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, online unter: http://bitcoin.org/bitcoin.pdf, zuletzt aufgerufen am 05.08.2013. Vermutlich handelt es sich bei dem Namen des Autors um ein Pseudonym; auch ist unklar, ob es sich nur um einen oder möglicherweise um mehrere Autoren handelt. In diesem Beitrag wird Satoshi Nakamoto als alleiniger Entwickler angenommen.

6 Neben den im Folgenden noch zitierten Arbeiten sei erwähnt, dass Bitcoin auch ein Forschungsgegenstand der Wirtschaftswissenschaften ist; beispielhaft kann hier die Arbeit von

Jeder Bitcoin-Nutzer kann beliebig viele Konten erzeugen, denen jeweils ein Schlüsselpaar[7] eines digitalen Signaturverfahrens zugeordnet ist. Ein kryptografischer Hashwert[8] des öffentlichen Schlüssels (die Bitcoin-Adresse) dient als Äquivalent einer Kontonummer. Der zugehörige private Schlüssel ist nur dem Kontoinhaber bekannt. Transaktionen werden mit diesem privaten Schlüssel signiert und können mit dem zugehörigen öffentlichen Schlüssel verifiziert werden.

Eine Transaktion kann mehrere Quell- und mehrere Zielkonten (mit unterschiedlichen Zahlungsbeträgen) haben. Um nachvollziehbar zu machen, welcher Betrag auf den Quellkonten für die Transaktion zur Verfügung steht, enthält die Transaktion Verweise auf eingehende Transaktionen der Quellkonten. Jede eingehende Transaktion darf dabei nur ein einziges Mal als Nachweis verwendet werden. Sollen Teilbeträge auf den Quellkonten verbleiben, können diese Konten als zusätzliche (Wechselgeld-)Zielkonten angegeben werden. Das Signaturverfahren stellt nun sicher, dass nur Berechtigte über ein Konto verfügen können. Allerdings verhindert es nicht, dass ein Berechtigter einen einmal eingegangenen Betrag „kopiert", indem er eine eingehende Transaktion mehrfach als Nachweis verwendet („double spending"). Im Gegensatz zu bisherigen Verfahren gibt es auch keine vertrauenswürdige Instanz, die Kontosalden nachvollziehen und Dritten gegenüber garantieren könnte, dass eine Transaktion ordnungsgemäß durchgeführt werden kann.

Bitcoin hat aus diesem Grund eine öffentliche Transaktionshistorie, die sogenannte Blockchain, die die Reihenfolge von Transaktionen nachvollziehbar und eine Mehrfachverwendung eingehender Transaktionen erkennbar macht. Um die Erstellung der Blockchain zu ermöglichen, wird jede Transaktion im Peer-to-Peer-System öffentlich bekanntgemacht. Jeder Peer kann sich als sogenannter „Miner" betätigen – was bedeutet, dass er eingehende Transaktionen prüft, an die bestehende Blockchain anhängt und dann versucht, einen Arbeitsbeweis über die somit entstandene neue Blockchain zu berechnen. Ein Arbeitsbeweis ist dabei der Nachweis, Rechenleistung investiert zu haben – seine Schwierigkeit wird so angepasst, dass die weltweit aufgewendete Rechenleistung im Durchschnitt alle 10 Minuten zu einem neuen Arbeitsbeweis

---

Joshua A. Kroll/Ian C. Davey/Edward W. Felten, „The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", in: *Proceedings of the 12th Workshop on the Economics of Information Security* (WEIS 2013), online unter: http://weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf , zuletzt aufgerufen am 23.04.2014, genannt werden.

7 Bei der asymmetrischen Kryptografie hat jeder Nutzer (mindestens) ein Schlüsselpaar. Im Fall von digitalen Signaturverfahren wird der private Schlüssel zum Erzeugen von Signaturen und der öffentliche Schlüssel zu deren Überprüfung verwendet.

8 Eine Hashfunktion bildet eine Eingabe beliebiger Länge auf eine Ausgabe fester Länge ab. Von kryptografischen Hashfunktionen wird erwartet, dass es praktisch nicht möglich ist, aus einem Hashwert auf eine passende Eingabe zu schließen oder zwei Eingabewerte zu finden, die auf den gleichen Hashwert abgebildet werden.

führt.[9] Da jeder Arbeitsbeweis nicht nur die neu hinzugekommenen, sondern auch die vorherigen Transaktionen umfasst, ist also umso mehr Rechenleistung in die Bestätigung von Transaktionen geflossen, je älter diese sind. Sofern mehrere unterschiedliche Blockchains existieren, gilt die längste – also diejenige, in die die meiste Rechenleistung geflossen ist – als korrekt. Um sicher zu sein, dass eine Transaktion erfolgreich war, sollte man abwarten, bis genügend Rechenleistung investiert wurde.Will ein Angreifer nämlich eine gefälschte Blockchain – aus der beispielsweise eine Transaktion entfernt wurde – erstellen, benötigt er mehr Rechenleistung als alle Miner, die korrekt arbeiten, zusammengenommen. Wartet man nach der Transaktion eine Stunde ab, müsste ein Angreifer nicht nur schneller Arbeitsbeweise erstellen als die Gesamtheit der korrekt arbeitenden Miner, sondern zusätzlich die Arbeitsbeweise einer Stunde nachholen – nur so könnte er die längste Blockchain erzeugen. Die zentrale, vertrauenswürdige Instanz traditioneller Bezahlverfahren wird auf diese Weise durch die Gesamtheit der Miner und deren Rechenleistung ersetzt.

Streng genommen besteht für das Funktionieren dieses Verfahrens keine Garantie: Der Arbeitsbeweis wird erbracht, indem verschiedene Eingabewerte in einer Hashfunktion durchprobiert werden, bis ein Hashwert mit einer bestimmten Eigenschaft produziert wird.[10] Im August 2013 mussten hierfür im Durchschnitt ca. 10^{17} mögliche Eingaben durchprobiert werden – umgekehrt heißt das, dass die Berechnung des Arbeitsbeweises mit einer Wahrscheinlichkeit von ca. 10^{-17} bereits im ersten Versuch erfolgreich ist. Dass ein Angreifer gar zufällig mehrfach infolge Arbeitsbeweise mit wesentlich weniger Versuchen berechnet als vorgesehen, ist so unwahrscheinlich, dass dieses Risiko bedenkenlos in Kauf genommen werden kann.

Sobald ein Miner einen Arbeitsbeweis gefunden hat, darf er sich eine vorher vereinbarte (vom Überweisenden zu begleichende) Transaktionsgebühr sowie einen festgelegten Betrag (aus dem „Nichts“, also ohne Belastung eines anderen Kontos) gutschreiben. Dies ist auch der einzige Mechanismus, mit dem Bitcoins geschöpft werden können. Im Laufe der Zeit wird der Betrag, den sich ein Teilnehmer ohne Belastung eines anderen Kontos gutschreiben darf, geringer. Vorgegeben ist eine Reduktion des Betrags um jeweils 50 %, sobald eine bestimmte Anzahl an Arbeitsbeweisen erbracht wurde.[11] Er wird bis auf null sinken, so dass – im Gegensatz zu Buchgeld, bei dem ebenfalls Geldschöpfung stattfindet – die Gesamtzahl an Bitcoins, die im Umlauf sein

---

[9] Vgl. Nakamoto (2008), Bitcoin; bezüglich des konkreten Werts: „Difficulty“, in: *Bitcoin-Wiki*, online unter: https://en.bitcoin.it/wiki/Difficulty, zuletzt aufgerufen am 09.01.2014.

[10] Dabei wird vorausgesetzt, dass die verwendete Hashfunktion (allgemein sowie für Eingaben mit bestimmtem Präfix) surjektiv ist, also jedes Element aus der Menge möglicher Hashwerte auch tatsächlich generieren kann – eine plausible und gängige, aber unbewiesene Annahme, deren Nichtzutreffen die im Weiteren genannten Wahrscheinlichkeiten verändern würde und einen konkreten Arbeitsbeweis im Extremfall sogar unmöglich machen könnte.

[11] Die Anzahl entspricht ungefähr einem Zeitraum von vier Jahren.

werden, begrenzt ist. Es steht zu vermuten, dass dieser Effekt zu einer Deflation, also einem steigenden Wert der Bitcoins, führen wird.

In den folgenden Abschnitten stellen wir nun die in Bitcoin auftretenden Automatismen sowie Gegentendenzen dar.

2.1 Netzeffekte

Aus ökonomischer Sicht wurden Netzeffekte bzw. Netzexternalitäten bereits 1985 beschrieben.[12] Ein direkter Netzeffekt tritt auf, wenn der Nutzen eines Guts für einen Nutzer mit der Anzahl der anderen Nutzer dieses Guts steigt. Bei Bitcoin ist das der Fall: Solange es wenige Nutzer gibt, die am Bitcoin-System teilnehmen, kann auch ein einzelner Nutzer nur mit wenigen anderen Handel treiben; sobald viele Nutzer vorhanden sind, steigt auch für jeden Nutzer die Wahrscheinlichkeit, Zahlungen mit Bitcoin abwickeln zu können. Steht hinter einem System, das solche Netzeffekte aufweist, ein Betreiber, so kann dieser durch geeignete Marketingmaßnahmen für eine installierte Basis zu sorgen versuchen, die einen hinreichenden Nutzen für später hinzukommende Nutzer verspricht. Ist dies erreicht, kann die Teilnehmerzahl (und damit der Nutzen für neue Teilnehmer) weiter steigen, ohne dass der Betreiber erneut investieren muss.

Das Bitcoin-System indes hat keinen Betreiber. Wie trotzdem eine Nutzerzahl zustande gekommen ist, die das System am Leben erhält, ist noch nicht abschließend untersucht. Denkbar ist aber, dass die Aussicht auf einen finanziellen Gewinn einen Anreiz darstellte: Das Erzeugen eines Arbeitsbeweises war zu Beginn noch einfach auf üblicher Hardware, also zu geringen Kosten, machbar. Als Belohnung für einen solchen Arbeitsbeweis darf man sich, wie oben erwähnt, einen Betrag in Bitcoin gutschreiben. Dieser war zwar anfangs wertlos, da Bitcoins nirgendwo akzeptiert wurden; allerdings bestand die Hoffnung, einen hohen Gewinn zu erzielen, falls das Bitcoin-System sich durchsetzen würde. Wie sich mittlerweile gezeigt hat, war diese Hoffnung berechtigt. Die Rahmenbedingungen wurden für das Bitcoin-System also so gesetzt, dass Automatismen wirksam wurden: Ohne explizite Steuerung – und in der Regel ohne das Bewusstsein, damit das Bitcoin-System am Leben halten zu wollen, sondern lediglich mit individueller Gewinnerzielungsabsicht – haben zahlreiche Akteure unabhängig voneinander beschlossen, Ressourcen zu investieren. Ein Grund für die Annahme, Gewinn erzielen zu können, dürfte dabei die im Bitcoin-System zu erwartende Deflation sein.

[12] Vgl. Michael L. Katz/Carl Shapiro, „Network Externalities, Competition, and Compatibility“, in: *The American Economic Review* 75, 3 (1985), S. 424-440.

2.2 Rollendifferenzierung

Bitcoin ist als reines Peer-to-Peer-System angelegt – und doch haben sich im Laufe der Zeit Differenzierungen zwischen den Teilnehmern ergeben, ohne dass diese explizit im Bitcoin-Konzept vorgesehen wären. Hierfür lassen sich verschiedene Gründe finden:

- Während sich grundsätzlich jeder Teilnehmer als Miner betätigen kann, tun viele das faktisch nicht. Dies liegt darin begründet, dass bei Verwendung gängiger Hardware die Energiekosten mittlerweile den Erlös aus Transaktionsgebühren und selbst gutgeschriebenen Bitcoins übersteigen. Damit sich die Tätigkeit als Miner lohnt, ist also die Anschaffung spezieller Hardware erforderlich.
- Das Bitcoin-System ist nicht beliebig skalierbar. Die Übermittlung aller Transaktionen an viele Miner wird bei hoher Transaktionszahl impraktikabel; eine Konzentration auf wenige Miner mit schneller Anbindung ist daher absehbar, wenn das Transaktionsvolumen erheblich wachsen sollte. Im Bitcoin-System ist also ein natürliches Oligopol der Miner angelegt, das lediglich bei den momentanen Transaktionszahlen noch nicht sichtbar wird.
- Einige Teilnehmer bieten weitergehende Dienstleistungen an (Handelsplattformen, z. B. zur Spekulation, aber auch Wechselstuben für den Umtausch Bitcoin – Euro), die eine Investition erfordern, zum Teil sogar erlaubnispflichtig sind. Diese Investition kann ebenfalls nicht jeder Teilnehmer erbringen.

Bei der beschriebenen Rollendifferenzierung lässt sich, da sie sich ohne zentrale Steuerung herauskristallisiert hat, von einem Automatismus sprechen.

2.3 Transaktionsgraph

Auch im Bitcoin-Transaktionsgraphen[13] finden sich Effekte nicht eingeplanter Automatismen. Die Bitcoin-Blockchain und somit alle Transaktionen sind öffentlich verfügbar. Dies hat eine Reihe von Publikationen ermöglicht, die den Bitcoin-Transaktionsgraphen untersuchen.

Ober et al.[14] haben diverse Parameter des Transaktionsgraphen untersucht: So wird beispielsweise aufgezeigt, dass das Verhältnis aus der Anzahl von Bitcoin-Adressen und der Anzahl von Nutzern von Anfang 2011 bis zum Ende des untersuchten Zeitraums (Januar 2013) konstant geblieben ist und ungefähr bei zwei liegt. Dies gilt, obwohl ein solches Verhältnis nicht im Entwurf des

[13] Ein Graph ist eine abstrakte Struktur aus Objekten (*Knoten*) und deren Verbindungen (*Kanten*). Der Transaktionsgraph ist der Graph, der sich ergibt, wenn die durchgeführten Transaktionen als Knoten und ihre Verweise auf Vorgänger-Transaktionen (siehe Abschnitt 0) als Kanten aufgefasst werden.

[14] Vgl. Micha Ober/Stefan Katzenbeisser/Kay Hamacher, „Structure and Anonymity of the Bitcoin Transaction Graph“, in: *Future Internet* 5, 2 (2013), S. 237-250.

Bitcoin-Systems angelegt ist. Zu bemerken ist allerdings, dass möglicherweise nicht alle Adressen eines Nutzers erfolgreich zusammengeführt werden können; die Zahl Zwei ist somit lediglich eine Untergrenze.

Die Autoren zeigen darüber hinaus, dass zumindest zwei Parameter des Bitcoin-Systems jeweils einer skalenfreien Verteilung unterliegen.[15] Für eine skalenfreie Verteilung gilt, dass ein Parameter *a* proportional zu b^g ist, wobei *b* ein zweiter Parameter ist und der Exponent *g* empirisch ermittelt wird. Die skalenfreie Verteilung gilt für

- die Anzahl der Bitcoin-Adressen pro Nutzer. Der Parameter *b* ist hier die Anzahl der Adressen und *a* die Anzahl der Nutzer, für die der jeweilige Wert von *b* zutrifft.
- die Aktivitätszeiträume (also die Zeiträume zwischen jeweils erster und letzter Aktivität eines Nutzers). Hier ist *b* der Aktivitätszeitraum in Tagen und *a* die Anzahl der Nutzer, für die dieser Zeitraum zutrifft.

Auch hier gilt, dass sich diese Verteilung nicht durch zentrale Kontrolle eingestellt hat, sondern auf den – in der Regel voneinander unabhängigen – Entscheidungen Einzelner basiert. Ähnlich wie Karl[16] es für Telekommunikationssysteme im Allgemeinen gezeigt hat, entsteht im Bitcoin-System also Struktur, ohne geplant worden zu sein. Es ist anzunehmen, dass diese Struktur für das Funktionieren des Systems nicht erforderlich ist.

Die Analyse des Transaktionsgraphen ist aber auch auf einer anderen Ebene aufschlussreich: So handelt es sich bei den „Nutzern", über die Ober et al.[17] Aussagen treffen, gar nicht um Informationen, die im Transaktionsgraph bewusst enthalten sind – dieser enthält nur Bitcoin-Adressen, die von beliebigen Personen in beliebiger Anzahl generiert werden können. Vielmehr handelt es sich bei diesen Nutzern um Informationen, die in einer Vorarbeit von Reid und Harrigan[18] aus dem Transaktionsgraph zunächst herausgearbeitet werden mussten.

Reid und Harrigan modellieren hierzu einen Graphen, in dem all jene Bitcoin-Adressen repräsentierende Knoten verbunden sind, die irgendwann einmal gemeinsam als Quellkonto für eine Transaktion genutzt wurden. Da für die Durchführung einer Transaktion die privaten Schlüssel aller Quellkonten benötigt werden, kann davon ausgegangen werden, dass alle Bitcoin-Adressen, die in diesem Graph – auch indirekt, d. h. über mehrere Knoten hinweg – verbunden sind, zum gleichen Nutzer gehören. Durch Kombination der Infor-

---

[15] Skalenfreie Verteilungen finden sich auch in anderen Netzen, siehe Oliver Hein/Michael Schwind/Wolfgang König, „Scale-Free Networks: The Impact of Fat Tailed Degree Distribution on Diffusion and Communication Processes", in: *Wirtschaftsinformatik* 48, 4 (2006), S. 267-275.

[16] Vgl. Karl (2010), Struktur aus Zufall.

[17] Vgl. Ober/Katzenbeisser/Hamacher (2013), Structure and Anonymity of the Bitcoin Transaction Graph.

[18] Fergal Reid/Martin Harrigan, „An Analysis of Anonymity in the Bitcoin System", in: Yaniv Altshuler/Yuval Elovici/Armin B. Cremers/NadavAharony/Alex Pentland (Hg.), *Security and Privacy in Social Networks*, Berlin, Heidelberg, 2013, S. 197-223.

mationen aus dem Transaktionsgraphen und der so ermittelten Beziehungen zwischen Bitcoin-Adressen machen Reid und Harrigan eine Struktur sichtbar, die im Transaktionsgraph zunächst verborgen scheint: Sie zeigt nun nicht mehr nur Beziehungen zwischen Transaktionen, sondern Beziehungen zwischen Transaktionen und Nutzern. Ist dabei auch nur eine einzige Bitcoin-Adresse einer konkreten Person zuordenbar – was in einigen Fällen, wie von Reid und Harrigan gezeigt, durchaus möglich ist – so werden durch diese Struktur sämtliche Transaktionen dieser Person sichtbar. Diese Strukturentstehung wird somit nicht nur *unbewusst* und *ungeplant* von den Teilnehmern des Bitcoin-Systems angetrieben, sondern sie erfolgt – im Gegensatz zum vorherigen Beispiel – darüber hinaus auch *ungewollt*.

2.4 Zweckentfremdung

Besonders kritisch sind die durch den Transaktionsgraph nicht-intentional veröffentlichten Informationen aber, wenn man die Erwartungen der Teilnehmer einbezieht: So wurde das Bitcoin-System zwar lediglich mit der Zielsetzung einer *Pseudonymisierung*[19] der Teilnehmer entwickelt;[20] fälschlicherweise hat das System in den vergangenen Jahren aber den Ruf eines vermeintlich *anonymen* Bezahlverfahrens erlangt[21] und daher auch Verbreitung etwa im illegalen Drogenhandel[22] gefunden. Akteure in diesem Kontext getätigter Transaktionen wiegen sich in einer Sicherheit, die offenkundig nicht existiert.

Wie aber kam es zur Etablierung dieses Rufes, der eine Art Zweckentfremdung des Bitcoin-Systems begründete? Es mag nahe liegend erscheinen, diese Entwicklung ebenfalls auf Automatismen zurückführen zu wollen – schließlich ist Zweckentfremdung vielerorts beobachtbar und wird von zahlreichen Menschen in vergleichbarer Form praktiziert.[23] Plausibler scheint in diesem konkreten Fall aber eher, irreführendes Marketing einzelner Akteure als Ursache anzunehmen. So behauptet etwa die Enthüllungsplattform WikiLeaks: „Bitcoin is a secure and anonymous digital currency“[24]. Dass diese Aussage falsch ist, wurde im vorangegangenen Abschnitt bereits diskutiert.

---

[19] Hierzu werden Teilnehmer innerhalb des Systems lediglich anhand zufällig gewählter, öffentlicher Schlüssel repräsentiert.

[20] Vgl. Nakamoto (2008), Bitcoin.

[21] „Bitcoin: Monetarists Anonymous“, in: *The Economist* vom 29.09.2012, online unter: http://www.economist.com/node/21563752, zuletzt aufgerufen am 05.08.2013.

[22] Vgl. Andy Greenberg, „Meet the Dread Pirate Roberts, the Man Behind Booming Black Market Drug Website Silk Road“, in: *Forbes* vom 02.09.2013, online unter: http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/, zuletzt aufgerufen am 05.08.2013.

[23] Dies wird ausführlich herausgearbeitet bei Uta Brandes/Miriam Steffen/Sonja Stich, „Alltäglich und medial: NID – Nicht Intentionales Design“, in: Gisela Ecker/Susanne Scholz (Hg.), *Umordnungen der Dinge*, Königstein/Taunus, 2000, S. 115-131.

[24] *Donate to WikiLeaks*, online unter: http://shop.wikileaks.org/donate#dbitcoin, zuletzt aufgerufen am 21.08.2013.

Tatsächlich scheinen bei dieser Zweckentfremdung sogar entgegengesetzte Effekte beobachtbar: Nicht nur sind es keine Automatismen, die die Zweckentfremdung verursachen. Es scheint sogar, dass die stattdessen erfolgende zentrale Steuerung – indirekt – *entautomatisierend* wirkt. So haben sich infolge der Fehlwahrnehmung von Bitcoin als anonymem Bezahlsystem zahlreiche Forschergruppen das Ziel gesetzt, durch Erweiterungen des Bitcoin-Konzepts eben jene Anforderungen zu erfüllen, die diesem System ohnehin schon zugesprochen werden. Den Automatismen, aus denen die in Abschnitt 0 beschriebenen Strukturen emergieren, soll hierzu ihr Nährboden entzogen werden.

Die Autoren von „Zerocoin“[25] etwa schlagen die Einführung einer zusätzlichen Münzenart – der sog. Zerocoins – vor, um eine Art Geldwäscheservice in das Bitcoin-System zu integrieren: Nutzer können dazu Bitcoins in Zerocoins überführen, die in einem gemeinsamen Pool gespeichert werden. Später können diese Nutzer dann *andere* Zerocoins aus diesem Pool in Bitcoins zurücktauschen, um die Beziehungen der neu erhaltenen Bitcoins zu früheren Transaktionen zu verschleiern. Geschickt eingesetzte kryptografische Verfahren stellen dabei sicher, dass ein Nutzer nur so viele Zerocoins aus dem Pool entnehmen kann, wie ihm zustehen – ohne Vertrauen in eine zentrale Instanz zu erfordern und ohne die von ihm eingezahlten Zerocoins aufzudecken.

Über die beschriebene Zweckentfremdung hinaus, der *indirekt* eine entautomatisierende Wirkung zugeschrieben wurde, lassen sich aber auch Zweckentfremdungen beobachten, die *direkt* entautomatisierend wirken. So gibt es – wie bei jedem IT-System – auch beim Bitcoin-System Angreifer, die aus unterschiedlichsten Beweggründen das System stören. Im Folgenden werden beispielhaft zwei existierende Systeme skizziert, die die zentrale Datenstruktur von Bitcoin – die Blockchain – verwenden, um vom Bitcoin-System scheinbar unabhängige Dienste zu erbringen. Ihre entautomatisierende Wirkung bezieht sich dabei nicht auf die in Abschnitt 0 beschriebenen Automatismen, die deanonymisierende Informationen hervorbringen, sondern auf jene, die das Bitcoin-System als solches am Leben halten.

Dan Kaminsky präsentiert in einem Vortrag[26] einen Dienst, der das Bitcoin-System – missbräuchlich – zweckentfremdet, um beliebige Daten (z. B. Dokumente oder Bilder) in der hochredundant verteilt vorgehaltenen Blockchain so zu archivieren, dass diese später durch beliebige Nutzer wieder ausgelesen werden können. Ermöglicht wird dies, indem einerseits Daten in nur vermeintlich existierende Bitcoin-Adressen codiert und Geldbeträge an diese überwiesen werden; andererseits werden Schwachstellen des Bitcoin-Systems zur Unterbringung größerer Datenmengen in der Blockchain verwendet. Dieser

[25] Ian Miers/Christina Garman/Matthew Green/Aviel D. Rubin, „Zerocoin: Anonymous Distributed E-Cash from Bitcoin“, in: *SP'13. Proceedings of the 2013 IEEE Symposium on Security and Privacy*, Washington, DC, 2013, S. 397-411.

[26] Kaminsky, Dan, „*Black Ops of TCP/IP*“, Vortrag auf dem 28th Chaos Communication Congress, 2011, online unter: http://www.youtube.com/watch?v=gQoykhNoBbY, zuletzt aufgerufen am 21.08.2013.

Dienst arbeitet in zweierlei Hinsicht destruktiv: Zum einen werden (geringe) Geldbeträge – permanent – vernichtet, da niemand den zur Bitcoin-Adresse gehörigen privaten Schlüssel kennt; zum anderen werden die Rest-Speicherkapazitäten aller weltweit aktiven Miner, die für den Betrieb des Bitcoin-Systems erforderlich sind, durch den beschriebenen Missbrauch deutlich reduziert. Würde der beschriebene Dienst verwendet, bis die Speicherkapazitäten der aktiven Miner erschöpft sind, so würde das Bitcoin-System hierdurch vollständig entautomatisiert – also lahmgelegt.

Weniger destruktiv gehen verteilte Zeitstempel-Dienste wie etwa BTProof[27] vor. Sie ermöglichen Nutzern, den Besitz eines Dokuments zu einem bestimmten Zeitpunkt mithilfe des Bitcoin-Netzwerks zu beglaubigen. Ähnlich wie im zuvor beschriebenen Angriff wird hierzu ein Hashwert über die Information, dass der Nutzer das Dokument besitzt, als vermeintlich existierende Bitcoin-Adresse aufgefasst und ein geringer Geldbetrag an diese überwiesen. Da die Transaktion (mitsamt Zeitstempel) in die Blockchain aufgenommen und fortan von allen Minern dauerhaft vorgehalten wird, ermöglicht sie, den Besitz dieser Information zum Zeitpunkt der Transaktion später nachzuweisen. Zwar hat auch dieser Dienst ein gewisses Potenzial zur Entautomatisierung, da (geringe) Geldbeträge durch Transaktionen vernichtet und die den Minern zur Aufrechterhaltung des Bitcoin-Betriebs zur Verfügung stehenden Speicherkapazitäten reduziert werden. Dieses ist gegenüber dem zuvor beschriebenen Dienst aber deutlich eingeschränkt: Zum einen wird mit jeder Beglaubigung nur ein marginaler Geldbetrag vernichtet (es ist nur eine Transaktion erforderlich), weshalb laut Aussagen der Betreiber der Effekt einer Vielzahl von Beglaubigungen geringer ausfällt als der regelmäßig auftretende Verlust privater Schlüssel (und damit des zugehörigen Geldes) durch Nutzer.[28] Zum anderen belegt eine Beglaubigung (bzw. eine Transaktion) nur marginal Speicherplatz in der Blockchain.

Es lassen sich aber auch Zweckentfremdungen des Bitcoin-Systems beobachten, denen weder direkt noch indirekt eine entautomatisierende Wirkung zugesprochen werden kann. So gibt es Dienste, die zwar das Bitcoin-Konzept verwenden, aber losgelöst vom Bitcoin-System – d. h. auf einer separaten, eigenen Blockchain – operieren und somit eine Störung des unabhängig arbeitenden Bitcoin-Systems vermeiden. Auf diese Weise realisiert beispielsweise das Namecoin-System[29] aufbauend auf der Bitcoin-Codebasis eine separate Währung – den Namecoin –, um eine vollständig dezentrale Alternative zum Domain Name System (DNS) zu schaffen.

Auffällig ist jedoch, dass es sich hierbei um eine andere Art von Zweckentfremdung handelt: Während den zuvor beschriebenen, entautomatisierend wir-

---

[27] *BTProof – Bitcoin Trusted Timestamping*, online unter: http://www.btproof.com, zuletzt aufgerufen am 21.08.2013.

[28] Ebd.

[29] *Namecoin*, online unter: http://namecoin.info, zuletzt aufgerufen am 21.08.2013.

kenden Zweckentfremdungen ein Zuwiderlaufen der ursprünglichen Intention des Bitcoin-Entwicklers unterstellt werden kann, handelt es sich hier um eine Zweckentfremdung, die in gewisser Weise vom Entwickler intendiert wurde. Der Grund ist, dass das Bitcoin-System als Open-Source-Projekt veröffentlicht wurde, was bedeutet, dass nicht nur eine Weitergabe, sondern auch eine Veränderung der Bitcoin-Software explizit erwünscht ist. So kann zwar insofern von einer Zweckentfremdung die Rede sein, als dass ihre konkrete Ausprägung vom Entwickler nicht vorhersehbar war; die Rahmenbedingungen, die sie ermöglicht haben, wurden aber bewusst geschaffen.

2.5 Rechtliche Regulierung

Für die praktische Umsetzung des Bitcoin-Systems sind nicht nur technische Parameter und beim Entwurf gesetzte Rahmenbedingungen relevant, sondern auch die Einwirkung des Rechtssystems. Aus juristischer Sicht stellt sich die Frage, wie die Regulierung eines Peer-to-Peer-Systems gestaltet werden soll. Insbesondere gibt es keinen Betreiber, der für das System als Ganzes verantwortlich gemacht werden kann. Dies zeigt sich beim Bitcoin-System besonders deutlich: Selbst der ursprüngliche Entwickler des Systems ist nicht greifbar, da seine Identität nicht bekannt ist. Auch wenn sie bekannt wäre, ergäbe sich daraus noch kein Anknüpfungspunkt für die Regulierung: Durch die Gestaltung des Systems selbst sind nur Rahmenbedingungen gesetzt. Auf das Verhalten während der Laufzeit hat der ursprüngliche Entwickler nicht mehr Einfluss als beliebige andere Teilnehmer.

Bislang hat der Gesetzgeber zumindest in Deutschland nicht auf die Problematik von Peer-to-Peer-Systemen reagiert. Aus Sicht des Telemediengesetzes (TMG) kann jeder einzelne Teilnehmer eines Peer-to-Peer-Systems Dienstanbieter sein und somit den Datenschutzverpflichtungen des Gesetzes unterliegen;[30] eine praktische Durchsetzung dieser Regelungen findet aber nicht statt. Dies gilt ebenso für § 3a Bundesdatenschutzgesetz (BDSG), wonach die „Gestaltung von Datenverarbeitungssystemen […] an dem Ziel auszurichten [ist], so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen". Auch wenn das Bitcoin-System nicht mit dem Ziel der Anonymität entworfen wurde, sind datenschutzrechtliche Fragestellungen bislang kaum diskutiert und die Datenschutzbeauftragten der Länder und des Bundes bislang nicht tätig geworden.

Im Fall des Bitcoin-Systems erlangt die gesetzliche Regulierung aber dort praktische Relevanz, wo einzelne Teilnehmer herausgehobene Rollen haben – wer beispielsweise den Handel bzw. die Spekulation mit Bitcoins ermöglicht, unterliegt in Deutschland der Erlaubnispflicht, da Bitcoin als Rechnungsein-

[30] Vgl. Christoph Sorge, „Datenschutz in P2P-basierten Systemen: Peer-to-Peer-Netze jenseits des Filesharing", in: *Datenschutz und Datensicherheit* 31, 2 (2007), S. 102-106.

heit einzustufen ist.[31] In Thailand sind Bitcoin-Transaktionen sogar vollständig verboten.[32] Wo das Rechtssystem erfolgreich eingreift, kann es die Rahmenbedingungen für Automatismen beeinflussen und damit auch die Funktionalität eines Systems als Ganzes stören. Ob ein solcher Eingriff das mit ihm verbundene Ziel erreichen kann, ist indes fraglich: Die Automatismen spielen sich in einem globalen System ab, es sind aber nur lokale Einflussnahmen möglich.

3. Fazit

Der vorliegende Beitrag hat am Beispiel des Bitcoin-Systems das Wechselspiel zwischen Automatismen und Bestrebungen der Entautomatisierung innerhalb technischer Systeme untersucht. Es wurde aufgezeigt, wie bei der Entwicklung des Bitcoin-Systems einerseits gezielt Automatismen provoziert wurden, die das System heute – ohne zentrale Steuerung – am Leben halten; wie aber andererseits auch völlig ungeplante Automatismen wirken, die – ungewollt – Informationen über die Teilnehmer des Bitcoin-Netzwerks offenbaren. Für beide Fälle wurden Praktiken aufgezeigt, die – bewusst oder unbewusst, erfolgreich oder nicht erfolgreich – störend auf die genannten Automatismen einwirken.

In diesem Sinne bestätigt dieser Beitrag Weichs These[33], der zufolge „bestimmte – und auf einen bestimmten Zweck hin ausgerichtete – Automatismen provozier[t]“ werden können. Es wurde aber zudem aufgezeigt, dass diese Automatismen nicht zwingend nur die dabei intendierten Strukturen erzeugen, sondern auch darüber hinaus gehende, ungeplante Strukturen hervorbringen können.

Erzeugt diese ungeplante Komponente eigentlich geplanter Automatismen Strukturen, die von den Teilnehmern ungewollt sind (etwa weil sie Deanonymisierung ermöglichen), so scheint sie außerdem Prozesse der Entautomatisierung (etwa die Entwicklung von Erweiterungen) in Gang zu setzen, die für sich betrachtet zentral gesteuert erscheinen würden.

---

[31] Vgl. Christoph Sorge/Artus Krohn-Grimberghe, „Bitcoin: Eine erste Einordnung“, in: *Datenschutz und Datensicherheit* 36, 7 (2012), S. 479-484.

[32] Vgl. „Bitcoin-Verbot in Thailand“, in: *Heise Online*, online unter: http://heise.de/-1926521, zuletzt aufgerufen am 21.08.2013.

[33] Weich (2013), These 7: Profile sind Selbst-Technologien.

Literatur

„Bitcoin: Monetarists Anonymous“, in: *The Economist* vom 29.09.2012, online unter: http://www.economist.com/node/21563752, zuletzt aufgerufen am 05.08.2013.

„Bitcoin-Verbot in Thailand“, in: *Heise Online*, online unter: http://heise.de/-1926521, zuletzt aufgerufen am 21.08.2013.

„Difficulty“, in: *Bitcoin-Wiki*, online unter: https://en.bitcoin.it/wiki/Difficulty, zuletzt aufgerufen am 09.01.2014.

Brandes, Uta/Steffen, Miriam/Stich, Sonja, „Alltäglich und medial: NID – Nicht Intentionales Design“, in: Gisela Ecker/Susanne Scholz (Hg.), *Umordnungen der Dinge*, Königstein/Taunus, 2000, S. 115-131.

BTProof – Bitcoin Trusted Timestamping, online unter: http://www.btproof.com, zuletzt aufgerufen am 21.08.2013.

Bublitz, Hannelore/Marek, Roman/Steinmann, Christina L./Winkler, Hartmut (Hg.), *Automatismen*, München, 2010.

Donate to WikiLeaks, online unter: http://shop.wikileaks.org/donate#dbitcoin, zuletzt aufgerufen am 21.08.2013.

Greenberg, Andy, „Meet the Dread Pirate Roberts, the Man Behind Booming Black Market Drug Website Silk Road“, in: *Forbes* vom 02.09.2013, online unter: http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/, zuletzt aufgerufen am 05.08.2013.

Hein, Oliver/Schwind, Michael/König, Wolfgang, „Scale-Free Networks: The Impact of Fat Tailed Degree Distribution on Diffusion and Communication Processes“, in: *Wirtschaftsinformatik* 48, 4 (2006), S. 267-275.

Kaminsky, Dan, „*Black Ops of TCP/IP*“, Vortrag auf dem 28th Chaos Communication Congress, 2011, online unter: http://www.youtube.com/watch?v=gQoykhNoBbY, zuletzt aufgerufen am 21.08.2013.

Karl, Holger, „Struktur aus Zufall: Entstehung von Abhängigkeiten in Telekommunikationssystemen“, in: Hannelore Bublitz/Roman Marek/Christina L. Steinmann/ Hartmut Winkler (Hg.), *Automatismen*, München, 2010, S. 71-78.

Katz, Michael L./Shapiro, Carl, „Network Externalities, Competition, and Compatibility“, in: *The American Economic Review* 75, 3 (1985), S. 424-440.

Kroll, Joshua A./Davey, Ian C./Felten, Edward W., „The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries“, in: *Proceedings of the 12th Workshop on the Economics of Information Security (WEIS 2013)*, online unter: http://weis-2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf, zuletzt aufgerufen am 23.04.2014.

Miers, Ian/Garman, Christina/Green, Matthew/Rubin, Aviel D., „Zerocoin: Anonymous Distributed E-Cash from Bitcoin“, in: *SP'13. Proceedings of the 2013 IEEE Symposium on Security and Privacy*, Washington, DC, 2013, S. 397-411.

Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, online unter: http://bitcoin.org/bitcoin.pdf, zuletzt aufgerufen am 05.08.2013.

Namecoin, online unter: http://namecoin.info, zuletzt aufgerufen am 21.08.2013.

Ober, Micha/Katzenbeisser, Stefan/Hamacher, Kay, „Structure and Anonymity of the Bitcoin Transaction Graph“, in: *Future Internet* 5, 2 (2013), S. 237-250.

Reid, Fergal/Harrigan, Martin, „An Analysis of Anonymity in the Bitcoin System“, in: Yaniv Altshuler/Yuval Elovici/Armin B. Cremers/Nadav Aharony/Alex Pentland

(Hg.), *Security and Privacy in Social Networks*, Berlin, Heidelberg, 2013, S. 197-223.

Skype, online unter: http://www.skype.com/de/, zuletzt aufgerufen am 21.08.2013.

Sorge, Christoph, „Datenschutz in P2P-basierten Systemen: Peer-to-Peer-Netze jenseits des Filesharing“, in: *Datenschutz und Datensicherheit* 31, 2 (2007), S. 102-106.

Ders./Krohn-Grimberghe, Artus, „Bitcoin: Eine erste Einordnung“, in: *Datenschutz und Datensicherheit* 36, 7 (2012), S. 479-484.

Weich, Andreas, „These 7: Profile sind Selbst-Technologien. Sie setzen über planvoll eingesetzte mediale Infrastrukturen ungesteuerte Dynamiken des Selbstmanagements und der Entstehung von Wissensstrukturen in Gang“, in: Hannelore Bublitz/Irina Kaldrack/Theo Röhle/Mirna Zeman (Hg.), *Automatismen – Selbst-Technologien*, München, 2013, S. 311-316.