Vertrauen aus Mathematik

Rüdiger Weis

1. Cryptographic Proof instead of Trust

Innerhalb weniger Jahre haben sich *Blockchains*, insbesondere durch den Erfolg der kryptographischen Währung *Bitcoin*, zu einer der meistdiskutierten ›neuen‹ Technologien entwickelt. Dieser sehr schnelle Aufstieg hat viele Problemstellungen zum verteilten Vertrauensmanagement, dem Energieverbrauch und dem Schutz der Privatsphäre von interessanten Forschungsfragen zu wichtigen Herausforderungen für eine nachhaltige wirtschaftliche und gesellschaftliche Entwicklung werden lassen.

Direkt während der großen Bankenkrise entstand mit *Bitcoin* eine digitale Währung, die zeitweise im dreistelligen Milliardenbereich zu Euro und Dollar gehandelt wurde. Der unter Pseudonym agierende Autor des *Bitcoin*-Systems erklärt das neue Vertrauensmodell mit einem einzigen Satz: »What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.«

Das Neuartige an einer auf *Blockchain* aufbauenden Währung besteht in dem Versuch einer Gruppe von Leuten, die dem bestehenden staatlichen Geldsystem sehr kritisch gegenübersteht, eine demokratische Alternative zu schaffen. Die ersten Ideen dazu kamen aus den USA, wo Libertäre und auch Krypto-Anarchisten Modelle entwickelt haben, mit denen sie darauf abzielten, eine Währung zu generieren, die weder auf staatlicher Kontrolle noch auf der Kontrolle von großen Organisationen beruht. Die Hauptidee war, eine demokratisch kontrollierte, für alle nachvollziehbare Art des Geldsystems mit einer festen Geldmenge zu schaffen.

Die Frage, ob eine feste Geldmenge oder eine wachsende Geldmenge vorzuziehen ist, ist eine grundlegende Frage der Politik. Lange Zeit waren an Gold gekoppelte Währungen vorherrschend, die einige Ähnlichkeiten zum *Bitcoin*-System aufweisen. So werden neue Währungseinheiten bei *Bitcoin* durch einen sogenannten *Mining*-Prozess generiert. Im Falle des heute gängigen Geldsystems bestimmen die Staaten oder die Zentralbanken mit unterschiedlicher Staatsnähe das Wachsen der Geldmenge, während es bei *Bitcoin* eine harte Begrenzung der

Menge der auszugebenden *Bitcoins* gibt. Wir können genau sagen, wie groß die Geldmenge bis zum Jahre 2140 sein wird (maximal 20.999.999,9769 *Bitcoins*). Die Frage, wie eine Geldmenge zu regeln ist, gilt bisweilen als der Heilige Gral der Volkswirtschaftslehre.

In der Praxis versteht man unter *Blockchain*-Technologien eine Mischung von unterschiedlichen Techniken aus der Mathematik und Informatik, die gewährleistet, dass Daten ohne einen zentralen Vertrauensanker in einer bestimmten Reihenfolge angeordnet werden. Diese Liste wird dann mit einem sehr einfachen Protokoll an alle Teilnehmer verteilt. Mit kryptographischen Verfahren, freier Software und einem dezentralen, robusten Netzwerkprotokoll hat man einen Ansatz, mit dem Informationen für alle zugänglich und überprüfbar sind, ohne dass eine zentrale Stelle benötigt wird, der man vertrauen müsste.

Die eigentliche *Blockchain* besteht aus einer verketteten Liste von Blöcken mit Hash-Zeigern und gehört zu den einfachsten Datenstrukturen der Informatik. Hashfunktionen sind Verfahren, welche kurze Prüfsummen für Daten berechnen. Sie sind zentrale und gründlich untersuchte Bausteine in allen in der Praxis weiterverbreiteten Signaturprotokollen. Die grundlegenden Methoden zur Erzeugung einer kryptographisch gesicherten Buchführung wurden in der Forschung schon seit vielen Jahrzehnten diskutiert. Aus Sicht der Programmierer ist eine *Blockchain* eine verteilte und authentifizierte Datenbank. Die Daten haben die Form eines Transaktionsbuchs und werden in Blöcken gespeichert und dabei durch kryptographische Techniken miteinander so verkettet, dass eine Manipulation praktisch nicht möglich ist. Weiterhin unterstützt das Konzept von *Open Source* die Idee der größtmöglichen Transparenz.

2. Trust the Math

Betrachtet man die Kursentwicklung von *Bitcoin*, wird deutlich, dass die Vertrauenskrise gegenüber staatlichen Institutionen nach den Enthüllungen durch Edward Snowden eine deutliche Verschärfung erfuhr. Gleichzeitig wurde die Mathematik, meist bezogen auf kryptographische Verfahren, als die letzte Vertrauenslinie vielfach gepriesen. Bruce Schneier, einer der weltweit führenden Kryptographen, erklärte im Guardian am 5. September 2013: »Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted.« Am folgenden Tage formuliert Schneier am gleichen Ort noch zugespitzter: »Trust the math. Encryption is your friend.«

Eine der großen Freuden für Mathematiker ist, dass man in der mathematischen Forschung immer wieder auf Resultate trifft, welche unstrittigerweise, teilweise sogar im strengen mathematischen Sinne, unendliche Schönheit ausstrah-

len. Nichtmathematikern kann man in einigen Teilbereichen versuchen, einen Eindruck hiervon zu vermitteln. Computer ermöglichen unter der Verwendung von einfachen Formeln visuelle Reisen theoretisch bis zur Unendlichkeit in farbenfrohe fraktale Welten. Im Bereich der Kryptographie ist es möglich, mit einer hübschen einfachen Formel, den Einzelnen gegen Kriminelle und völlig aus dem Ruder gelaufene Geheimdienste zu schützen.

3. Because of Its Supreme Uselessness

Nützlichkeit ist für viele Mathematiker kein notwendiges, ja nicht einmal eine anzustrebende Eigenschaft. So schrieb Godfrey Harold Hardy 1940 in seiner *A Mathematician's Apology*: »if mathematics is the queen of the sciences, then the theory of numbers is, because of its supreme uselessness, the queen of mathematics«. Bemerkenswert ist, dass die grundlegenden Verfahren für *Blockchains* einfache Mathematik benutzen, welche man durchaus in den ersten Semestern eines Mathematikstudiums problemlos durchdringen sollte. Der Kontozugriff innerhalb von *Bitcoin* verwendet Unterschriftsverfahren über Elliptische Kurven und damit anspruchsvolle Zahlentheorie. Fragen des Schutzes der Privatsphäre benötigen weitere Forschung. *Zero-Knowledge*-Verfahren gehören zu der Art von Mathematik, die selbst nach jahrzehntelanger Beschäftigung mit der Materie oftmals mit dem Gefühl der Lösung von scheinbar unlösbaren Problemen mittels Magie von natürlichen Zahlen einhergehen.

4. Weltweit verteilt und unlöschbar

Ein zentraler Punkt bei *Bitcoin* ist, dass die Information zu jeder Transaktion weltweit einsehbar ist und auf sehr viele Rechner verteilt ist. Dies ist im Vergleich zu normalen Bankdaten, auf die nur nach klar definierten Grundlagen von staatlichen Stellen zugegriffen werden darf, eine signifikante Verschlechterung hinsichtlich des Schutzes der Kontoinhaber gegenüber rechtswidrigen Angriffen von Geheimdiensten und Kriminellen. So kann jeder in der Welt erkennen, wer wieviel Geld auf einem Konto hat. Kriminelle können so die großen *Bitcoin*-Konten automatisch auffinden und die Kontoinhaber direkt angreifen. Es sind nur wenige Programmzeilen nötig, um Millionen Konten automatisch zu attackieren. *Bitcoin* versucht durch die Verwendung von Pseudonymen, einige der Datenschutzprobleme zu adressieren. Moderne Analysetechniken mithilfe von recht einfacher Graphentheorie reduzieren jedoch in beträchtlichen Rahmen den Schutz durch pseudonyme Konten. Es gibt bereits mehrere Anbieter auf dem Markt, die das

Durchleuchten von *Bitcoin*-Flüssen als Dienstleistung anbieten. Auch alternative Systeme, die einen erweiterten Schutz der Privatsphäre anbieten, sind gegen derartige Analysemethoden nicht vollständig abgesichert.

Ohne Pseudonyme wäre *Bitcoin* ein Alptraum, mit Pseudonymen ist es datenschutzrechtlich aber immer noch äußerst problematisch. Hier besteht ein starker Forschungs- und Entwicklungsbedarf.

5. Schlechte Kryptographie führt zu Oligarchie

Die Ursprungsidee von *Bitcoin* war ein demokratisches System, in dem alle Teilnehmer jeweils eine Stimme haben und in welchem ein gemeinsamer Konsens durch eine demokratische Mehrheit gefunden wird. Allerdings haben die Entwickler von *Bitcoin* an verschiedenen Stellen nicht die aktuelle kryptographische Forschung beachtet. Konkret wurde auf der untersten Ebene eine zu einfache Funktion gewählt, die sich zu gut in Hardware implementieren lässt. Das führt dazu, dass Leute, die viel Geld in Hardware-Entwicklung investierten, ein höheres Gewicht haben.

Bei der zugrunde liegenden Funktion für das *Mining* neuer *Bitcoins* handelt es sich um die kryptographische Hashfunktion SHA-256. Diese Hashfunktion wurde gezielt in einer Form entworfen, die eine möglichst einfache Hardware-Realisierung ermöglicht. Dies führt dazu, dass diejenigen, die die bessere Hardware und billigeren Strom nutzen können, den Markt kontrollieren. Hätte man die aktuelle kryptographische Forschung verfolgt, hätte man diese problematische Entwicklung zumindest abbremsen können. Diese zu wenig durchdachten Designentscheidungen führten jedoch dazu, dass sich inzwischen eine starke Zentralisierung herausgebildet hat. Die Kontrolle über die *Blockchains* konzentriert sich in der Praxis auf wenige *Mining-Pools*. Dies widerspricht nicht nur der Grundidee der Dezentralisierung, es bringt auch einige gewichtige praktische Probleme mit sich.

Die kryptographische Forschung hat sich im Zusammenhang mit *Password-Hashing* schon sehr lange damit beschäftigt, Funktionen zu entwickeln, welche möglichst schlecht auf Spezialhardware (insbesondere ASICs) zu realisieren sind. Viele alternative Kryptowährungssysteme verwenden derartige Verfahren, zum Teil allerdings nicht mit ausreichend sicheren Parametern. Interessant im Sinne der Nachhaltigkeit ist, dass im Zuge der Hardwareentwicklung für *Mining*-Berechnungen viel Aufwand für eine energiesparende Implementierung der benötigten Verfahren betrieben wurde. Es gibt Überlegungen, alternative *Mining*-Verfahren vorzuschlagen, welche als Nebenaspekt eine energieeffizientere Implementierung von auch anderweitig benötigten Verfahren mit sich bringen könnten.

6. *Grassroot*-Ökonomie und Technologiesprung

Die interessante philosophische Diskussion, ob Staaten Segen oder Fluch für das menschliche Zusammenleben sind, erhält in vielen Ländern der Welt einen gewichtigen Realitätsbezug. Wie organisiert man wirtschaftlichen Austausch, wenn schlicht kein funktionierender Staat da ist? Systeme, die auf einer *Blockchain* basieren, haben den Vorteil, ein hohes Maß an Diskriminierungsfreiheit zu gewährleisten. Wer die wenigen *Bits* des zu einem Konto gehörenden Schlüssels kennt, hat Zugriff auf das dort liegende Geld.

Die Möglichkeit, mittels *Blockchain*-Technologien digitale Vertrauensstrukturen zu bauen, welche nur geringe Anforderungen an die analoge Welt stellen, schafft interessante Chancen für sich entwickelnde Volkswirtschaften. In einigen afrikanischen Ländern gibt es spannende Entwicklungen von Zahlungssystemen, die auf dem Mobiltelefon basieren, besonders in Ländern mit nur gering entwickeltem Bankwesen. Auch wenn es in einigen Fällen zahlreiche Probleme im Bereich der Privatsphäre und den teilweise inakzeptabel hohen Transaktionsgebühren gibt, attestieren viele Beobachter sehr positive Entwicklungen.

7. Automatisierte Verträge

Smart Contracts erweitern das Einsatzgebiet von *Blockchain*-Technologien in einer theoretisch und auch soziologisch faszinierenden Weise. Bei solchen Verträgen wird Vertrauen nicht über einen Notar oder einen rechtlichen Rahmen abgesichert, der meistens durch Staaten gewährleistet wird, sondern mathematisch. Man kann beispielsweise kryptographisch Verträge konstruieren, bei denen man zwei Stimmen braucht, um das Geld freizugeben. Das bedeutet, wenn zwei Vertragsteilnehmer sich einig sind, muss ein Schiedsrichter gar nicht gefragt werden. Wenn man uneinig ist, müssen die Beteiligten dem Schiedsrichter die jeweilige Haltung darstellen und dieser entscheidet dann. Es wird also keine Durchsetzung von Ansprüchen durch gerichtliche Verfahren und Forderungseintreibung benötigt. In der Welt der *Smart Contracts* können wir sagen: »Wir machen einen Vertrag, als Schiedsrichter wählen wir irgendjemand auf der Welt.« Das bedeutet, wir brauchen keinen Staat mehr, um Verträge miteinander zu schließen. Denn zu deren Absicherung reicht allein die Mathematik.

8. Sonnenunterstützte Entwicklungsideen

Interessanterweise haben einige gängige digitale Währungssysteme Eigenschaften, welche sich gut mit regenerativen Energiequellen vertragen. Sonnen- und Windenergie haben die Eigenschaft, dass sie stark schwankende Einspeisungen generieren. Oftmals befinden sich die zur Energiegewinnung günstigen Orte weit entfernt von den Hauptabnehmern. Sowohl Transport als auch Speicherung von größeren Strommengen verbrauchen in nicht unerheblichem Maße Energie. Die gerade innerhalb des Netzes nicht benötigte Energie direkt in digitale Währungen umzusetzen, scheint eine spannende Idee zu sein. Die sogenannte *Miningpool*-Freundlichkeit von *Bitcoin* ermöglicht eine voraussagbare Umsetzung von Energie in digitale Währungseinheiten. Autonome Systeme könnten in sonnenreichen, infrastrukturarmen Gebieten eingesetzt werden, dort eigenständig mit Solarenergie eigene *Mesh*-Netze aufbauen und mit dem *Minen* von kryptographischen *Coins* beginnen.

Für die Teilnahme an einer *Blockchain*-Ökonomie reicht zunächst ein *Global System for Mobile Communications* oder eine Satellitentelefon-Außenverbindung mit geringer Bandbreite für das gesamte *Mesh*-Netz. Die Rechnung für die mobile Verbindung könnte mit den aus Sonnenenergie gewonnen *Coins* beglichen werden. Analog könnte bei einer späteren Anbindung an das konventionelle Stromnetz tagsüber Solarstrom eingespeist und für den nachts benötigten Strom die Rechnung mit kryptographischem Geld bezahlt werden.

Setzt man im Bereich der Konsensfindung auf sozial nützliches *Mining*, etwa für die Bereitstellung von Speicherplatz für Dateien, könnte man ökologisch verantwortungsvoll realisierte und lokal kontrollierte *Cloud*-Dienste zur Verfügung stellen. Eine vielversprechende Idee hierfür sind *Prof-of-Space*-Verfahren. Hierbei wird das Speichern von Daten belohnt anstatt die Berechnung von Zufallsfunktionen. Ein interessanter Ansatz hierfür ist *Filecoin* (https://filecoin.io/), dem 2017 ein dreistelliges Millionen-*Initial-Coin-Offering* gelang.

9. Anforderungen für nachhaltige *Blockchains*

Der Schutz der Privatsphäre bei öffentlichen *Blockchain*-Sytemen stellt neue Herausforderungen an den kryptographischen Schutz der Teilnehmer. Bei *Bitcoin* führte ein Design, basierend auf kryptographischem Halbwissen, schnell zu einer Entdemokratisierung der grundlegenden Prozesse und einem starken Zuwachs des Energieverbauches. Die Nutzung von regenerativen Energiequellen und die Möglichkeit, Vertrauenssysteme ohne Staat zu erstellen, bieten schon aktuell interessante Möglichkeiten für nachhaltige Entwicklungen. Die kryptographische Forschung bietet eine Reihe von Ideen, nachhaltigere *Blockchain*-Systeme zu entwickeln.

Quellen:

Godfrey Harold Hardy: A Mathematician's Apology, Cambridge 1940.

Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (31. Oktober 2008).

Rüdiger Weis: Nachhaltige Blockchains, in: Ökologisches Wirtschaften 4/2018 (2018), S. 27–29.