Im Maschinenraum einer Kryptowährung

3 Im Maschinenraum einer Kryptowährung

Wie viel Anarchismus steckt im Bitcoin? Wer entlohnt die Programmierer? Was könnten Privatbanken mit Kryptowährungen anstellen? Und sollte man damit sein Bier bezahlen? Einer der vier Bitcoin-Maintainer weltweit gibt Antworten.

Ronnie Grob trifft Jonas Schnelli

Jonas, mit welchem Argument überzeugst du einen Laien, dass er Bitcoin nutzen sollte?
Bitcoin ist eine Revolution des Informationsaustauschs, bei dem die Macht wieder zurück zum Einzelnen geht. Blickt man zurück, so sind die Finanzsysteme nur in den letzten paar hundert Jahren durch den Staat kontrolliert worden – vorher nicht. Lange pflegte man den Tauschhandel, handelte mit Muscheln. Irgendwann einigte man sich auf goldgebundene Tokens, auch der Schweizer Franken war ja lange Zeit goldgebunden. Mittlerweile aber haben wir es mit Finanzsystemen zu tun, die von Realwerten abgelöst sind und von Nationalbanken bestimmt werden, oft auch von privaten Organisationen wie das FED in den USA. Diese Organisationen bestimmen, wie viel Geld im Umlauf ist. Ihre Systeme haben funktioniert und sie funktionieren nach wie vor. Der Gedanke von Bitcoin ist aber, dass die Menschen über das Geld entscheiden und bestimmen sollen.

Laien sagen jeweils: schön und gut, aber wie bewährt sich Bitcoin im Alltag? Wo kann ich dieses Zeug endlich mal ausgeben?
Mich erinnert das an die Ende der 1980er Jahre häufig gestellte Frage: «Wie hat sich denn E-Mail bisher bewährt?» Ich kann mich erinnern, wie froh ich war, als ich mit meinem ersten Modem endlich mal jemanden fand, dem ich eine E-Mail schicken konnte.

Sind wir mit Bitcoin 2018 da, wo das Internet 1993 war?
Das kann man so sagen. Allerdings: rückblickend hat sich das Internet schnell entwickelt; ich weiss nicht, ob das bei Kryptowährungen auch der Fall sein wird. Der Aufstieg des Bitcoins mag rasant aussehen, ich denke aber, dass er noch eine lange Entwicklung vor sich hat. Die Risiken des weitgehend unerforschten Gebiets der Dezentralität sind jedenfalls nicht zu unterschätzen.

Welche Branchen werden Kryptowährungen in Bedrängnis bringen?
Die Banken werden wohl nicht rar werden. Die Auswirkungen einer Neuerung sind oft anders, als man vermutet: Wer hätte zum Beispiel in den 1980er Jahren gedacht, dass das Internet das klassische Taxigewerbe in Bedrängnis bringt, so wie es jetzt durch Uber geschieht? Dienstleistungen wie Paypal oder Western Union könnten angegriffen werden, vielleicht in zweiter Linie auch Kreditkartenunternehmen. Das sind Firmen mit sehr hohen Margen: starke, kräftige Unternehmen. Vielleicht brauchen wir auch bald keine Notare mehr.

Macht es Sinn für mich, ein Bier mit Bitcoin zu zahlen, wenn ich für Kleinbeträge hohe Gebühren zahlen muss?
Aktuell liegt die Gebühr umgerechnet bei rund 30 Rappen.

Kaufe ich mir ein Bier für fünf Franken, sind die 30 Rappen relativ viel, und die Transaktion dauert auch zu lange.
Ja, diese Gebühr ist viel zu hoch für eine solche Transaktion. Dafür ist die Sicherheit immens viel höher als bei einer Kreditkarten- oder Banktransaktion. Die mathematische Sicherheit der Unveränderlichkeit (Immutability), die man bei einer Bitcoin-Transaktion hat, ist so hoch, dass es für fünf Franken schlichtweg hinausgeschmissenes Geld ist. Für grosse Transaktionen lohnt es sich aber, denn die Gebühr bleibt grundsätzlich dieselbe, ob bei fünf oder bei fünf Millionen Franken. Bei einer Bitcoin-Transaktion handelt es sich wie bei einer Transaktion im Bankenwesen nur um Daten. Die Gebühren bei den Banken sind höher, weil die Risiken höher sind. Bei Bitcoin existieren die Risiken dagegen nur ausserhalb des Systems: es sind die Nutzer, die etwas falsch machen könnten.

Was ist deine persönliche Rolle bei der Entwicklung von Bitcoin?
Ich bin seit fünf Jahren aktiv dabei als Entwickler von Bitcoin Core und seit ein bisschen mehr als zwei Jahren auch Maintainer. Das heisst, ich habe die Rechte, Änderungen in den Kerncode einzuspielen. Es gibt vier Maintainer weltweit.

Sind dir die anderen drei bekannt?
Man kennt sie, wenn man in diesem Feld aktiv ist. Maintainer müssen aber nicht öffentlich präsent sein. Maintaining ist aufwendig – man hat darum gar nicht die Zeit, noch hundert Sachen nebenbei zu machen.

Erhältst du für diese Leistung von jemandem eine Vergütung?
Die chinesische Bitcoin-Mining-Firma Bitmain ist auf mich zugekommen und hat mir angeboten, mich zu vergüten, also ein Spon-

soring zu machen. Bitmain hat über hundert Angestellte und macht geschätzt einen Umsatz von 100 000 US-Dollar plus jeden Tag.

Warum? Was haben die davon?
Die Chinesen denken sehr langfristig, also eher in Dekaden als in Jahren. Sie wissen, dass es ihre Einnahmen ohne Bitcoin nicht geben würde und dass sie künftig auch abhängig davon sind, dass Entwickler dieses System weiterentwickeln. Selbst sind sie kulturell zu weit entfernt von der Entwicklung, sie verfügen nicht über die notwendigen Fachkräfte. Deshalb haben sie sich wohl dazu entschlossen, etwas zu unternehmen, damit es den bestehenden Fachkräften gut geht und sie damit weitermachen. Die fünfzehn aktivsten Entwickler bei Bitcoin Core werden allesamt privat finanziert.

Wie unabhängig bist du von diesem Sponsoring?
Ich habe völlig andere Ansichten als meine Sponsoren. Auch öffentlich vertrete ich meine Ansichten nach wie vor völlig frei. Die Leute von Bitmain tolerieren es, dass sie keinen Einfluss auf meine Meinung und Arbeit haben. Von anderen, die von US-Firmen gesponsert werden, habe ich gehört, dass Meinungsverschiedenheiten finanzielle Folgen haben können. So könnte ich nie arbeiten.

Du wirst in Bitcoins bezahlt?
Ja.

Bitcoin gibt es seit 2009. Was wurde seither am Code geändert?
Zuerst mal muss man die verschiedenen Ebenen auseinanderhalten. In der Konsensus-Ebene ist das Regelwerk festgehalten: wie viele Bitcoins gibt es, wann werden sie generiert, was sind die Algorithmen für die Inflationsrate, für das Mining etc. Im Bitcoin Core Client, der früher einfach Bitcoin Client hiess, gibt es aber noch weitere Ebenen, zum Beispiel die Peer-to-Peer-Ebene, in der es um die Verknotung des Netzwerks geht, was für das Überleben von Bitcoin von einiger Relevanz ist. Während seit der Urversion schon Tausende, wenn nicht Millionen Zeilen Code verändert worden sind, wurden auf der Konsensus-Ebene, also im Regelwerk, nur sehr wenige Änderungen implementiert. Sie sind schwierig umzusetzen, weil für eine Änderung auf dieser Ebene alle Teilnehmer gleichzeitig ihr System aktualisieren müssen. Man muss auch vorsichtig sein beim Umsetzen von Änderungen: aktuell hat Bitcoin an manchen Tagen ein Marktvolumen von rund zehn Milliarden Franken. Ein Schaden im System wäre deshalb viel verheerender als noch 2011, als man einfach hätte sagen können: nun gut, das Experiment ist halt fehlgeschlagen.

Welche Änderungen sind geplant?
Diskutiert wird ein neues Signaturschema, ein asymmetrisches Kryptoverfahren. Damit soll eine bessere Skalierung möglich werden. Wenn man tausend Signaturen in eine fassen kann, können grössere Daten schneller verarbeitet werden. Das Problem der Skalierung ist ein grundsätzliches: es ist fraglich, ob Massentauglichkeit mit einem dezentralen System erreicht werden kann. Denn Dezentralität und Skalierung sind technologisch betrachtet Gegenpole: je besser die Skalierung ist, desto schlechter die Dezentralität – und umgekehrt. Was den Bitcoin aber letztlich ausmacht – gegenüber Paypal und anderen Systemen –, ist ja eben die Dezentralität und die Zensurresistenz.

SNB-Direktoriumsmitglied Thomas Moser sagt (siehe S. 62), Bitcoin entstamme Anarchistenkreisen. Bist du Anarchist?
Ich sehe mich nicht als Anarchisten. Aber die Wurzeln der Kryptowährungen gehen zurück zu den Cypherpunks, also zu Leuten wie Hal Finney, Adam Back, Nick Szabo, die den Gedanken hatten, sich Big Brother zu entziehen. Das ist nicht in dem Sinne anarchistisches Gedankengut, dass man das staatliche Gewaltmonopol abschaffen will, sondern dass man, im Sinne der Bürgerrechte, die Privatsphäre gewährleisten sollte. Egal, ob man etwas zu verstecken hat oder nicht – man kommt nicht umhin, festzustellen, wie flächendeckend sich die Überwachung ausbreitet. Da ist es nur folgerichtig, dass es eine Gegenbewegung gibt. Und das waren oder sind die Cypherpunks.

Wo stehst du politisch?
Ich habe zu wenig Zeit, um mich mit Schweizer Politik zu beschäftigen.

Aber Bitcoin ist ja etwas sehr Politisches.
Das mag sein. Mir geht es aber um die Weiterentwicklung der Software und das Interesse an der Technologie.

Trotzdem: hat der Bitcoin mit der Förderung persönlicher Freiheiten zu tun?
Wir Schweizer haben sehr viele Freiheiten und sind uns dieser nicht immer bewusst. Wenn wir aber über den Tellerrand hinausblicken, sehen wir, was finanzielle Freiheit wirklich bedeutet: es ist die Freiheit, zu bezahlen, wen man will. Das Recht, Informationen frei austauschen zu können, ist für mich ein menschliches Grundrecht, und zu diesem Informationsaustausch zähle ich auch finanzielle Transaktionen. Bitcoin und andere Kryptowährungen ermöglichen es dem Einzelnen, dieses Grundrecht auf den freien Informationsaustausch, das weltweit betrachtet eben nicht so selbstverständlich ist, wahrzunehmen.

Wie schützt du dich gegen die Überwachung? Wie verhältst du dich im Internet?
Ich gehe mit einem Mindset an meine Arbeit, dass das, was ich mache, öffentlich ist – als könnte es jeder sehen. Gerade weil ich als Programmierer die Komponenten von Computersystemen und ihre Komplexität kenne, halte ich es für unredlich, zu behaupten, diese seien sicher. Es gibt Löcher, die durch Kriminelle oder andere Instanzen ausgehebelt werden können. Es ist alles nur eine Frage des Geldes: wenn jemand 10 000 Franken aufwendet, kann er alles verfolgen, was ich an meinen Geräten mache.

In letzter Zeit habe ich viele Leute von einem Lightning-Netzwerk sprechen gehört. Was ist das?
Das Lightning-Netzwerk ist möglich geworden mit Segregated Witness (SegWit). Das ist ein Peer-to-Peer-Zahlungssystem, bei dem aber nicht jede Transaktion auf der Bitcoin-Blockchain abgebildet wird. Wir können also ein Konto eröffnen im Lightning-Netzwerk und einander darin bezahlen – und erst am Ende wird der Saldo im Bitcoin-Netzwerk abgerechnet.

Welche Herausforderungen wollt ihr mit dem Bitcoin noch lösen?
Mit den Instant Transactions im Lightning-Netzwerk könnten wir eine gewisse Massentauglichkeit erreichen. Dann beschäftigt uns die Frage, wie man Menschen und nicht nur Bitcoin-Adressen bezahlen kann: noch ist es nicht möglich, jemanden bei Bitcoin, eine Person, zu suchen und zu finden und zu bezahlen. Hier fehlt uns noch ein Element. Das Web of Trust, aber auch andere Projekte arbeiten in diese Richtung. Ob auch dort eine dezentrale Lösung möglich ist, muss sich zeigen. Meine fast grösste Sorge ist aber das Key Management. Auch wenn es immer heisst, man könne seine eigene Bank sein, vergisst man, dass damit grosse Risiken einhergehen. Key Management ist deshalb kritisch, weil am Ende nur 256 Bits das Geld kontrollieren. Man kann schon diversifizieren, aber am Ende geht es darum, irgendwelche privaten Nümmerchen privat zu halten. Auch die Probleme mit dem Vererben von Krypto-Assets nach dem Tod sind noch völlig ungelöst.

Selbst den direkten Zugang zu seinem Vermögen zu haben, bedeutet sehr viel Verantwortung für den Eigentümer.
Ja, denn es ist auch der direkte Zugang zum sofortigen Verlust des Vermögens. Wer 1 Million Franken bei einer Bank angelegt hat, kann diese Million abheben und sie auf der Strasse in die Luft werfen – aber wir sind uns einig: ganz so einfach ist das nicht, es braucht auch etwas Zeit, bis man mit einer Million Bargeld aus einer Bank herauslaufen kann. Bei Bitcoin dagegen kann die Million in Sekunden überwiesen sein – oder ganz weg sein, wenn zum Beispiel das Wallet-Passwort verlorengeht.

Ist das nicht die grosse Chance für Banken, sich einzubringen?
Key Management, also die sichere Verwahrung von Kryptowährungen, ist für die Banken das Zukunftsmodell. In Venezuela mag das vielleicht anders sein, aber in Ländern mit stabilen Bankensystemen wie der Schweiz ist der Normalbürger durchaus dazu bereit, seine Keys bei einer Bank aufzubewahren. Die Frage ist, wer das Risiko trägt. Denn es ist anzunehmen, dass die Banken sich Rechte offenhalten wollen, also im Sinne von: «Wenn uns die Coins geklaut werden, hast du sie auch nicht mehr.»

Wenn bei Bitcoin mehr Teilnehmer mitmachen und aktiv einen Knotenpunkt betreiben, es also mehr Nodes gibt, funktioniert dann das Dezentrale und das Netzwerk nicht besser?
Einen Knotenpunkt (Node) betreiben nur jene, die einen Bitcoin-Computer oder Bitcoin-Software bei sich zu Hause betreiben, also nicht jene, die nur Transaktionen machen im Bitcoin-Netzwerk. Dass das die breite Masse machen wird, ist nicht realistisch. Rekapitulieren wir: Bitcoin ist entwickelt worden, um das Problem «Trusted parties are security holes» zu überwinden. Diesen Gedanken leben kannst du aber nur, wenn du selbst einen Node betreibst. Denn wenn du eine Bitcoin-Transaktion erhältst, wo schaust du nach, ob du sie erhalten hast? Bei einer Trusted Third Party, also vielleicht auf Coinbase.com oder auf Blockchain.info. Die Idee von Bitcoin ist aber vielmehr, dass du niemandem vertrauen musst. Mit einem eigenen Node verifizierst du die Transaktion auf deinem eigenen System. Du schaust selbst dort nach, ob sie angekommen ist.

Sagen wir, ich bin eine kleine Privatbank in Zürich, die sich neu erfinden will. Würde es da Sinn machen, einen Node zu betreiben?
Natürlich! Ich würde sogar sagen, es ist eine fahrlässige Handlung, in so einem Fall keinen Node zu betreiben. Ein Laie kann einen Node für 100 Franken bauen, aber bei einer Bank ist ja alles etwas komplizierter: ich würde also sagen, dass ein Node in einem professionellen IT-Umfeld für 10 000 bis 50 000 Franken gebaut werden kann. Nur so hat der Betreiber die Sicherheit, dass Transaktionen wirklich ankommen. Wer mit Millionenbeträgen hantiert, sollte diese 50 000 aufbringen. Eine Bank, die das nicht macht, wird auf einen Mittelsmann angewiesen sein, der ihr sagt: Ja, die Transaktion ist wirklich erfolgt. Oder nein, sie ist nicht erfolgt. Ich glaube, dass alle Betriebe, die im Auftrag ihrer Anleger mit Krypto-Assets handeln, sich diese Gedanken machen müssen: Banken, Vermögensverwalter, Family Offices etc.

Was ist deine persönliche Vision: wo sollte Bitcoin in zehn Jahren stehen?
Alle Währungssysteme haben mit Vertrauen zu tun: Wie lange es etwas gibt, ist für die Menschen wichtig. Aber kann es nicht tausende Jahre Gold geben und dann findet man etwas Neues? Oder kann es nicht hunderte Jahre den Schweizer Franken geben und dann wieder etwas Neues? Ich will die Massentauglichkeit für Bitcoin erreichen. Der Einzelne soll die Möglichkeit erhalten, andere zu bezahlen ohne Beteiligung von Dritten, möglichst sofort und möglichst ohne Gebühren. Meine Vision ist es, das gesamte Zahlungssystem loszulösen von irgendwelchen Mittelinstanzen. ‹

Jonas Schnelli
ist als Maintainer von Bitcoin einer von vier Menschen weltweit, die das Recht haben, Änderungen in den Kerncode der Kryptowährung einzuspielen. Schnelli lebt in Basel.

Ronnie Grob
ist Redaktor dieser Zeitschrift.