S&N INVENT

Die Spreu vom Weizen trennen

Was ist dran am Hype um Bitcoin und Blockchain?

Whitepaper

Dr. Jürgen Lampe

17.07.2020

S&N INVENT

Inhaltsverzeichnis

Vorbemerkung

Was ist dran am Hype um Bitcoin und Blockchain?

Abbildung 1: Die Spreu vom Weizen trennen - Hype um Bitcoin und Blockchain

Die Diskussion von Bitcoin und Blockchain lässt oft den Bezug zur implementierten Realität vermissen. Es wird deshalb versucht, die wesentlichen Grundlagen und Funktionsprinzipien sowie die daraus resultierenden technischen Grenzen verständlich darzustellen.

Einleitung

In den letzten Wochen hat es die Diskussion um Bitcoin und Blockchain erneut und wiederholt bis in die Tagespresse geschafft. Beim genauen Lesen merkt man allerdings schnell, dass sehr oft die reißerische Aufmachung fehlendes Wissen überdeckt. Immer noch sind die im Folgenden widerlegten Mythen, denen jede technische Basis fehlt, im Umlauf.

Das liegt sicher auch daran, dass die Bitcoin-Welt nicht leicht zu verstehen ist. Trotzdem soll der Versuch unternommen werden, die grundlegenden Techniken verständlich darzustellen und dadurch die Diskussion aus der Mythologie auf den Boden der Realität zurück zu holen. Das geht naturgemäß nicht ohne die eine oder andere – auch stärkere – Vereinfachung. Ziel ist es vorrangig, die zentralen Wechselbeziehungen und Abhängigkeiten zu verdeutlichen.

Als Zahlungsmittel stellt Bitcoin praktisch eine unabhängige Währung dar und unterliegt damit neben den technischen Regeln auch nicht-trivialen ökonomischen Gesetzmäßigkeiten. Durch die Beschränkung der Geldmenge mit abnehmender Geldschöpfungsrate ergibt sich beispielsweise, ähnlich wie beim Goldstandard, ein inhärent deflationärer Charakter, der wahrscheinlich langfristig die Liquidität beeinflussen wird. Solche nichttechnischen Gesichtspunkte, zu denen auch das Vertrauen in den Wert der Währung gehört, sind für die Gesamteinschätzung ebenso wichtig, bleiben hier jedoch unberücksichtigt.

1 Grundlagen

Die Bitcoin-Entwicklung stammt aus einer leicht anarchisch geprägten Netzkultur. Jede zentrale Instanz sollte vermieden werden, das Ganze auf einer beliebigen Anzahl von mehr oder weniger dauerhaft teilnehmenden Rechnern laufen. Vollständige Dezentralisierung ist daher das durchgehende Prinzip, das alle weiteren Designentscheidungen geprägt hat. Jeder Bitcoin-Client ist deshalb mit vielen, möglichst zufällig ausgewählten anderen Clients verbunden.

Bitcoin kennt weder Konten noch etwas, das man als Äquivalent für Münzen oder Scheine ansehen könnte. Es gibt nur Überweisungen mit Verrechnungsbeträgen und ein Verzeichnis aller gültigen Überweisungen. Bitcoins existieren nur als Beträge in diesen Überweisungen. Jede Überweisung hat einen eindeutigen Namen (ID), über den sie referenziert werden kann. Der Empfänger des Betrags wird ebenfalls durch eine ID bestimmt. Da es keine Konten gibt, sind die Quellen solcher Überweisungen immer andere Überweisungen. Durch kryptografische Signaturen wird gewährleistet, dass nur der Empfänger einer Überweisung diese als Quelle einer anderen angeben kann.

Der Besitz von Bitcoins besteht darin, dass es Überweisungen an den jeweiligen Besitzer gibt, die noch nicht wieder als Ausgangspunkt neuer Überweisungen verwendet worden sind. Diese Bedingung wird vor der Aufnahme in das Überweisungsverzeichnis überprüft. Einzelne Überweisungen können dabei mehrere Quellen und Ziele enthalten, um Beträge zu sammeln oder aufzuspalten. Der Eigentümer der Quellen darf dabei durchaus auch Ziel der Überweisung sein, um beispielsweise Einzelbeträge zu kumulieren oder Restbeträge zu behalten. Jede Überweisung wird an das gesamte Netzwerk publiziert.

2 Buchführung

Alle Überweisungen werden in einem gemeinsamen Kontobuch[1], geführt. Durch dauerhafte Aufnahme in dieses Kontobuch wird eine Überweisung gültig und gewissermaßen „ausgeführt“. Das Führen eines Kontobuchs in einer völlig dezentralen Struktur ist allerdings äußerst herausfordernd und bei Bitcoin originell gelöst. Da hierbei zwei unterschiedliche Aufgaben, nämlich die Buchführung und die Konsensfindung, miteinander verschränkt werden, ist diese Funktion die am häufigsten missverstandene.

Das Kontobuch wird von speziellen Knoten gepflegt, die „Miner“ genannt werden. Der Begriff ist irreführend, weil ihre Hauptaufgabe die Buchführung ist, für die sie dann allerdings unter bestimmten Umständen (s. später) mit neu geschaffenen Bitcoins entlohnt werden. Da es im Netzwerk keine Instanz gibt, die korrektes Verhalten erzwingen könnte, wird vorausgesetzt, dass es immer genügend Miner gibt und diese sich überwiegend „gutartig“, d. h. auf die hier beschriebene Art, verhalten[2].

Das Kontobuch kann man sich als eine Sammlung von Blättern vorstellen, zu denen in regelmäßigen Abständen (zehn Minuten) jeweils ein neues Blatt hinzukommt. Jedes Blatt enthält einen Verweis auf das vorangegangene. Da die Blätter im Netzwerk verteilt werden, kann es durch Latenzen, Unterbrechungen usw. vorkommen, dass in einem Intervall neue Blätter mit unterschiedlichen Vorgängern zirkulieren. Wenn ein Miner ein neues Kontobuchblatt erhält, muss er überprüfen, ob es in seinem Kontobuch den referenzierten Vorgänger gibt und die enthaltenen Überweisungen verifizieren. Wenn das Blatt korrekt ist, wird es in die lokale Kontobuchkopie aufgenommen und die Arbeit am eigenen Blatt abgebrochen. Außerdem wird das akzeptierte Blatt an alle verbundenen Knoten (Miner und einfache Clients) weiter geschickt, sodass schließlich alle Knoten alle gültigen Blätter vorliegen haben. Einige davon werden sich im weiteren Verlauf dadurch als verwaiste (orphan) Enden erweisen, dass sie keine Folgeblätter erhalten.

Parallel dazu sammelt jeder Miner alle ihm bekannt werdenden Überweisungen ein, verifiziert sie und fasst sie in einem Puffer zusammen. Zu Beginn des neuen Blattberechnungszyklus wird als Vorgängerblatt das letzte Blatt der längsten Kette ausgewählt. (Das ist das Blatt mit den meisten Vorgängern.) Alle empfangenen Blätter, die nicht in dieser Kette sind, werden ignoriert. Gegen das so abgegrenzte Kontobuch werden die gepufferten Überweisungen validiert und bei Erfolg in das neue, lokal im Entstehen befindliche Blatt übernommen. Abschließend wird eine Prüfzahl über den Inhalt des Blatts einschließlich des Verweises auf den Vorgänger berechnet, die dann im Weiteren als Verweis (ID) auf dieses Blatt benutzt werden kann.

Wenn der Wertebereich der Prüfzahl, wie bei Bitcoin mit 256 Bit, groß ist und geeignet berechnet wird (Bitcoin verwendet die Hashfunktion SHA-256.), kann mit hinreichender Wahrscheinlichkeit angenommen werden, dass sie das Blatt oder den Datenblock eindeutig kennzeichnet. Jede Abänderung innerhalb eines Blocks, z. B. die einer Überweisung oder auch

[1] Genau genommen müsste das stattdessen „Verzeichnis der Überweisungen“ heißen, da es ja keine Konten gibt. Der Begriff ist aber trotzdem üblich.
[2] An das Verhalten der „normalen“ Clients wird eine solche Forderung nicht gestellt.

des Verweises auf den Vorgänger würde dazu führen, dass die Prüfzahl nicht mehr zum Block passt, wäre also nachweisbar. Eine derartige Verknüpfung von Datenblöcken wird „Blockchain“ genannt. Bitcoin benutzt eine Blockchain für das Kontobuch.

3 Bitcoins-Mining

Außer den aufgesammelten Überweisungen enthält jedes Kontobuchblatt noch genau eine spezielle Überweisung ohne Quelle für die Vergütung des Buchhaltens. Der Betrag ist festgelegt und halbiert sich in größeren Abständen. Das ist der einzige Weg, auf dem neue Bitcoins entstehen. Man muss beachten, dass nur diejenigen Miner in den Genuss dieser Vergütung kommen, deren Blatt in das Konsens-Kontobuch, d. h. die längste Kette von Blättern, aufgenommen wird. Das ist pro Zyklus genau einer. Aber wessen Blatt oder Block landet nun dauerhaft im Kontobuch? In der Theorie reicht es, jeweils zufällig einen Miner auszuwählen. Praktisch ist diese zufällige Auswahl ohne zentrale Instanz schwierig zu erreichen. Wenn es um Geld geht, muss man immer mit Betrugsversuchen rechnen. Deshalb kann man sich auch nicht auf irgendeinen lokalen Zufallsprozess (analog Würfeln) verlassen. Stattdessen – und das ist schon eine geniale Idee – wird jedem Miner eine Aufgabe gestellt, deren Lösung nur durch Ausprobieren einer großen Anzahl von Möglichkeiten zu finden ist, die aber leicht überprüft werden kann. (Ein typischer Vertreter dieser Aufgabenklasse ist die Primzahlzerlegung größerer Zahlen.)

Wer die Aufgabe gelöst hat, darf seine Seite publizieren. Die Wahrscheinlichkeit, dass ein Miner erfolgreich ist, hängt dann von der eingesetzten Rechenkapazität ab. Die Bedingung für korrektes Verhalten muss deshalb von der Anzahl der Miner auf deren eingesetzte Rechenkraft modifiziert werden. Es bleibt aber wichtig, dass diese Ressource nicht monopolisiert wird. (Diese Gefahr ist gegenwärtig nicht ganz auszuschließen.)

Es ist das Lösen dieser Aufgabe, was gemeinhin als Mining bezeichnet wird, weil es zeit- und energieaufwendig ist und heute nur noch mit Spezialhardware erfolgversprechend betrieben werden kann. Tatsächlich stellt es jedoch nur einen – wenn auch nicht leicht zu ersetzenden – Workaround für das Problem der zufälligen Auswahl dar und ist so gesehen kein essentieller Teil des Bitcoin-Systems.

4 Mythen

4.1 Anonymität

Es ist einer der am weitesten verbreiteten Irrtümer, dass Bitcoin vollständige Anonymität gewährleistet. Wahr ist, dass die Teilnehmer sich hinter kryptischen Zeichenfolgen (Adressen) verbergen und jeder beliebig viele solcher Pseudonyme besitzen kann. Doch die wahre Identität lässt sich nicht besser verbergen als bei jeder anderen Aktivität im Internet auch. „Für den Hausgebrauch“ mag das ausreichen, gegenüber den großen Spähern vom Kaliber der NSA sollte man besser keinen Schutz erwarten.

Weitere Angriffspunkte ergeben sich, wenn Bitcoins für das Bezahlen von nicht-digitalen Leistungen benutzt werden, zum Beispiel beim Umtausch in konventionelle Währungen, oder beim Kauf von Waren. Nicht vergessen sollte man auch, dass nach dem Enttarnen einer Identität alle jemals damit vorgenommenen Transaktionen, die ja in der Blockchain unlöschbar gespeichert sind, zurückverfolgt werden können.

4.2 Schnelligkeit

Man kann immer wieder lesen, dass Bitcoin schnelle Bezahlvorgänge erlaubt. Das betrifft jedoch nur das Starten einer Überweisung. Als sicher ausgeführt gilt diese erst dann, wenn sie im Kontobuch auf einer Seite dokumentiert ist, die bereits mindestens fünf Nachfolger hat. Bei einem Zehn-Minuten-Intervall kann das frühestens nach einer Stunde soweit sein. Dazu kommt, dass in Zeiten hoher Belastung manchmal einige Zeit (bis zu mehrere Stunden) vergeht, bis eine Überweisung überhaupt in die Bearbeitung kommt. Es gibt Ansätze dieses Manko zu beheben, indem Beträge bei vertrauenswürdigen Treuhändern, sogenannten „Green Addresses“, geparkt werden, die dann für die Bezahlung bürgen. Da es sich dabei um zumindest teilweise zentrale Agenten handelt, widerspricht dieses Vorgehen den ursprünglichen Grundsätzen und hat sich bisher nicht weit verbreitet.

4.3 Betrugssicherheit

Prinzipiell ist das Vorgehen sehr sicher gegen Betrugsversuche. Wenn das System stark ausgelastet ist und die Beteiligten nicht bis zur sicheren Bestätigung warten, gibt es allerdings die Möglichkeit, Überweisungen ungültig zu machen. Das liegt daran, dass die Miner das Recht haben, Überweisungen, die ihnen eine Bearbeitungsgebühr zuweisen, bevorzugt zu behandeln. Man kann also eine Leistung per Überweisung bezahlen und, während diese auf ihre Bearbeitung wartet, in einer weiteren Überweisung den gleichen Quellbetrag abzüglich einer (höheren) Bearbeitungsgebühr für den Miner wieder einem eigenen Empfänger zuweisen. Mit hoher Wahrscheinlichkeit wird dann diese zweite Überweisung zuerst ins Kontobuch aufgenommen, während die ursprüngliche Bezahlung als ungültig (ein Betrag darf nur einmal verwendet werden) verworfen wird.

Des Weiteren sind natürlich alle vom Online-Banking her bekannten Angriffe denkbar, um an die Schlüssel und damit die Bitcoins eines Teilnehmers zu kommen.

4.4 Verbesserbarkeit

Bitcoin ist eine rundum integrierte Implementierung einer virtuellen Währung. Genau das macht eine generelle Verbesserung oder Weiterentwicklung jedoch extrem schwierig. Alle Komponenten sind so aufeinander abgestimmt, dass jede größere Änderung das Gesamtkonzept beeinträchtigt. Zudem ist es durch das Fehlen einer zentralen Instanz extrem schwierig, Konsens über Modifikationen zu erreichen. Schließlich muss auch bedacht werden, dass jede Weiterentwicklung Auswirkungen auf den Wert der bestehenden Guthaben und damit auf das Vertrauen in die Währung haben kann.

5 Grundsätzliche Fragen

5.1 Blockchain

Einige Protagonisten sehen in der Blockchain schon den Untergang der bisherigen Banken. Tatsächlich handelt es sich um eine clevere Technik, Daten nachvollziehbar unveränderlich zu speichern. Auf die Dauer hat eine solche Unveränderlichkeit aber auch Nachteile. Da die Blockchain nur wächst, wird der zu beachtende Datenbestand immer umfangreicher. Außerhalb von Bitcoin ergibt sich bei dezentraler Organisation zusätzlich die Frage, wie Miner in genügender Anzahl gewonnen und honoriert werden können.

5.2 Skalierbarkeit

Das größte Problem des Bitcoin-Projekts ist die mangelnde Skalierbarkeit. In der aktuellen Form können maximal drei bis sieben Überweisungen pro Sekunde verarbeitet werden (weltweit!). Nach glaubwürdigen Ausführungen ließe sich diese Grenze durch technische Anpassungen zwar noch bis in den Bereich 25 bis 30 verschieben, aber das ist immer noch um Größenordnungen zu wenig. Der Grund ergibt sich aus der beschränkten Größe der Kontobuchseiten und deren Berechnungsintervall. Beide Werte können nicht beliebig variiert werden, wenn das System funktionsfähig bleiben soll.

6 Zusammenfassung

Bitcoin ist ein beeindruckendes Beispiel dafür, wie man mit aktueller Technologie und sinnvollen Kompromissen eine schwierige Aufgabe überzeugend lösen kann. Geradezu vorbildlich ist die Einbeziehung von Sicherheitsaspekten in alle Designentscheidungen. In Zeiten des „Internet of Things“ sollte man darüber nachdenken, ob nicht auch Software in anderen Bereichen diese Sorgfalt verdient hätte.

Die Geschlossenheit der Lösung ist andererseits ein großer Stolperstein, wenn es darum geht, die verwendeten Konzepte auf andere Anwendungsfelder und Größenbereiche zu übertragen. Bisher gibt es zwar einen Hype um das Thema „Blockchain“, aber überzeugende Konzepte für besser skalierende Systeme fehlen nach wie vor. Es bleibt also spannend zu beobachten, ob Bitcoin eine zwar rundum perfekte Nischenlösung für kleine Probleme bleibt oder das Potential hat, die Prozesse rund um den Geldverkehr tatsächlich stark zu verändern.

Weiter interessante Artikel zum Thema:

BBC: We looked inside a secret Chinese bitcoin mine

Gartner: The CIO's Guide to Blockchain

Märchenkette: Blockchain zwischen Marketing und Forschung

Autor

Dr. Jürgen Lampe ist IT-Berater bei der S&N Invent GmbH. Er ist promovierter Mathematiker und war u. a. als Hochschuldozent tätig. Seit mehr als 20 Jahren befasst er sich mit Design und Implementierung von Java-Anwendungen, hauptsächlich im Bankenumfeld. Sein spezielles Interesse gilt effizienten anwenderorientierten Softwarearchitekturen und domänenspezifischen Sprachen.

Neben seiner Tätigkeit als Senior-Berater schreibt er Whitepaper und Artikel für Fachzeitschriften und spricht auf Konferenzen. Er ist Autor des Buches „Clean Code für Dummies“.

Über S&N Invent

S&N Invent ist ein bundesweit tätiges IT-Unternehmen mit einem umfassenden Leistungsportfolio über die gesamte Wertschöpfungskette des IT-Lifecycles. Wir entwickeln gemeinsam mit unseren Kunden Lösungen, setzen Projekte um und schaffen damit digitale Mehrwerte.

Das Leistungsspektrum reicht von klassischen Mainframe-Architekturen über moderne Java/JEE Web- und Portalarchitekturen bis hin zu neuesten Technologien im Cloud- und Mobile-Bereich. Agile Projekte mit hohem Qualitätsanspruch, gewährleistet durch modernes Continuous Quality Management, sind für uns in zahlreichen Projekten gelebter Standard.

Die S&N Invent GmbH ist ein Unternehmen der S&N Group. Insgesamt sind in den Gesellschaften der S&N Group ca. 380 feste Mitarbeiterinnen und Mitarbeiter an acht Standorten in Deutschland sowie dem Nearshore-Standort Budapest beschäftigt. Damit können wir unsere Kunden mit umfassender Kompetenz und regionaler Nähe bestens betreuen. Gleichzeitig sind wir so in der Lage, große und komplexe Projekte in Time und Budget erfolgreich umsetzen zu können.