Wofür also die BlockChain ...

Erfasst am : 25. November 2017 18:05 | Erfasst von : Martin
Verknüpfte Kategorie(n): Internet, Bitcoin, Kommerz

So, nun habe ich mal alle meine Fragen zu BlockChain (BC) ausreichend beantwortet gefunden. Ein einziges Buch half dabei, das nicht mal technisch war. Aber genau das wollte ich. Es ist von Daniel Drescher und lautet "Blockchain Basics" und ist in englisch.

Denn als Kryptografie-Experte war mir das Technische eh klar. Allerdings hatte ich genau deswegen meine knackigen Fragen, die mir zufällige Gesprächspartner nicht beantworten konnten. Weil mir allerdings ein Projekt fehlte, blieben meine Fragen ungeklärt.

Nun, nach Lektüre dieses Buchs, ist das nun nicht mehr so. Es beschreibt in 25 Schritten wirklich ohne eine einzige Zeile Code, geschweige denn Mathematik, worum es sich bei der BC handelt und wieso diese Begriff derzeit so ein Hype ist. Und üblicherweise deswegen, weil die meisten wohl nur vage davon was verstehen. Jeder der 25 Schritte beginnt mit einer Metapher aus der realen, uns allen bekannten sozialen Welt. Danach folgt die daran angelehnte Konzeption in der BC.

Die Kryptografie, die Technik also, ist einfach bzw. wir benutzen sie unter der Haube bei jedem (verschlüsselten) Internetzugriff sowieso schon. Das also kann den Hype nicht ausmachen.

Die BC macht es aus, dass sie konzeptionell viele Punkte adressiert, die eine Datenbank - und mehr ist es nicht - je nach Anwendungsbereich immer adressieren muss. In Merkworten:

1. **Kein Single Point of Failure**
   die BC ist eine verteilte Datenbank, die bei jedem Teilnehmer vollständig vorhanden sein muss. Damit ist sie automatisch dupliziert und redundant. Ist sie einmal in Betrieb mit mehr Teilnehmern als ein Aggressor auf einen Schlag lahmlegen kann, ist sie nicht zu zerstören.

2. **Jeder kann an der BC mitmachen**
   die BC ist ein Computeralgorithmus, so dass jeder netzwerkfähige Computer mitmachen und jede in ihr gepeicherte Transaktion nachkontrollieren kann. Dadurch ist sie in höchsten Masse transparent und bietet keinerlei Privatsphäre zur Geschichte einer Transaktion. Eine Anonymität ist nur dann gegeben, wenn die in der BC zu speichernden Transaktion aus anonymen Daten besteht. Es gibt einen quasi demokratischen Entscheidungsprozess, eine Konsensfindung, die dafür sorgt, dass der Versuch einer Einspeisen von gefälschten Transaktionen umgehend entdeckt wird.

3. **Niemand kann die BC in seinem Sinne manipulieren**
   zumindest fast niemand, Geheimdienste, Google etc. könnten es wohl, denn die BC wird nur sicher, wenn sie eine gewisse Grösse erreicht hat. Die Grösse ist nämlich die Herausforderung, die ein möglicher Manipulator zu meistern hat, wenn er Einträge fälschen möchte. Er muss neben dem zu fälschenden Block alle nachfolgenden Blöcke nachrechnen und er muss das sogar noch schneller tun, als die anderen Teilnehmer, die ja auch an der BC arbeiten und sie legitim verlängern. Ein genug potenter Manipulator kann das aber, erst recht, wenn die BC legitimerweise spärlich genutzt wird. Die Manipulationssicherheit entsteht durch pro Block durchzuführende, resourcenhungrige Berechnung des Hash-Puzzles (dazu später).

4. **Jeder kann an der BC etwas "verdienen"**
   da die BC physische Resourcen braucht, diese nicht gratis sind, ist in der BC ein Mechanismus zur Belohnung für Mitwirkende drin. Eine automatische Bestrafung ist ebenfalls eingebaut, denn es kann passieren, dass erledigte Arbeit eben nicht belohnt wird. Die Belohnung selbst kann wohl aber nur in der "Währung" erfolgen, mit der die BC "handelt", denn der Teilnehmer wird nur an der BC mitmachen, die ihn thematisch interessiert und der er sicher nicht schaden will und seine Belohnung riskieren würde.

5. **die BC kann irgendeine digitale Resource speichern**
   die BC ist ein Programm. So kann sie grundsätzlich auch Programmcode speichern, der revisionssicher und nachvollziehbar ist. Aufgrund der abwesenden Privatsphäre gibt es allerdings keinen Schutz vor unbefugten Einsichten.

Das sind so die Eckdaten. Wieso die Banker etwas Schiss vor der BC haben, ist die Tatsache, dass sie als dezentrales System die Sicherheit von Transaktionen gewährleisten kann für alle irgendwo mitwirkenden Computer. Wenn wir heute zur Bank gehen, damit die für uns einen Betrag von hier nach da überweisen, dann tun wir das, weil es sich nicht lohnt, selbst hinzufahren, weil es unsicher ist etc. etc.

Da Geographie und Distanzen in Computernetzwerken aber keine grossen Sachen mehr sind, fallen die Bank-Services ja weg. Es fallen im Prinzip überall dort die Mittelleute weg, wo es um reine digitale Daten geht - und das ist heute viel: Geldäquivalente, Videos, Musik, Zertifikate, Urkunden, Pläne, Patente, Berechtigungen etc.

Doch die BC hat eben auch eklatante Schwächen: Das Belohnungssystem nützt nur der Teilnehmergruppe. Das kann dazu führen, dass nur wenige Teilnehmer an einer BC mitmachen, was wiederum dazu führt, dass eine Manipulation eines genug potenten Teilnehmers möglich ist, wenn er mit seinen Resourcen die Konsensfindung zu seinen Gunsten beeinflussen kann.

Die BC basiert derzeit auf einem mathematischen Problem, der Einwegfunktion. In der IT heissen diese Digests oder Hashes. Die wohl bekanntesten Hashes sind MD5 und alle Varianten von SHA. Sie berechnen aus einer beliebig grossen Datenmenge einen 128 - 512 Bit langen Wert, eine Zahl also.

Es ist wohl klar, dass man aus nur 512 Bit niemals herausfinden kann, welche 10, 1000, 100000 Megabytes genau einen bestimmten Wert erzeugt haben. Es ist allerdings von der Qualität des Hash-Algorithmus abhängig, wieviele der möglichen Eingangsvarianten man überhaupt durchprobieren muss, bis man einen Hash-Wert findet, der identisch ist zu dem Wert einer anderen Eingangsvariante. Für den bekannte SHA-1 Algorithmus ist das Erzeugen einer sog. Kollision schon gelungen, so dass man dem Spruch "es gibt keine gleichen Ausgangswerte für unterschiedliche Eingangswerte" nicht einfach für bare Münze nehmen kann. Trotz der Kollision ist ein SHA-1 natürlich immer noch gut, denn man kann immer noch nicht in nützlicher Frist eine Eingangsvariante so verändern, dass ein bestimmter Hash-Wert erzeugt wird. Wäre dies möglich, müsste man SHA-1 per sofort also geächtet betrachten.

Google und andere haben aber trotzdem schon begonnen, die Verwendung von SHA-1 in den Web-Protokollen anzumahnen. Man solle mindestens SHA-256 oder den neuen SHA-3 nutzen.

Diese Hashes sind das Fundament der BC. Denn logischerweise kann man auch "Hashes über Hashes bilden" wie der ITler sagt. Das bedeutet, man kann Ketten (Chains) bilden, in der Blöcke zusammengehängt werden, wo jeder Block einen Hash über eine Transaktion beinhaltet. Kann man nachträglich jederzeit die Transaktionsangaben hashen, so kann man den selbst berechneten Hash-Wert auch mit dem im Block gespeicherten Hash vergleichen. Kommt man nicht auf

denselben Wert, wurde irgendwas verändert, die Transaktionsangaben oder/und der Hash-Wert sind also - neutral gesagt - ungültig. Ein Block kann aber nur an den vorherigen angehängt werden, wenn der neue Block den Vorgänger verifiziert hat und in sich selbst den Hash der Verifikation speichert. Mit dieser Regel kann die BC nur wachsen, wenn beim Einspeisen einer neuen Transaktion die BC verifizierbar unverändert geblieben ist. Um das nachzuprüfen, müssen BC-Teilnehmer, die eine neue Transaktion in die BC einspeisen möchten, die ganze Kette bis zur ersten Transaktion rückwärts rechnen.

Diese Fakten bedingen die eingangs erwähnte Transparenz und Unveränderlichkeit aller gespeicherten Transaktionen, also die Integrität.

So einen einzigen Block einer Transaktion zu fälschen, ist natürlich Peanuts. Wenn an eine Transaktion nun eine weitere anhängt, weil beispielsweise eine Geldüberweisung von A nach B von diesem B aufgeteilt an C, D und E weitergeleitet wird, so ist die Kette auch noch nicht schwierig zu berechnen, denn man hat ja alle Eingangsdaten: Die ursprüngliche Transaktion, die einen ersten Block ergab - Die Überweisung von A nach B. Sollen nun Blöcke angehängt werden für die Transaktionen BC, BD, BE, so wird bei jedem Anhängen der zuvor letzte Block (Kopf der BC) versiegelt. Eine Manipulation der Ausgangstransaktion wird also nicht nur die Berechnung dieses Blocks auslösen, sondern auch diejenige aller nachfolgenden Blöcke. Der Manipulator rennt also dem Kopf der BC hintennach und muss erst noch die anderen Teilnehmer von seinen Berechnungen überzeugen.

Die Hash-Funktion hat nun als Eigenschaft, dass sie sehr schnell berechnet werden kann. Im Wesentlichen ist die Berechnungszeit nur von der Grösse der Eingangsdaten abhängig. Ein SHA-256 kann auf einem handelsüblichen PC heute durchaus schon knapp 10 MByte pro Sekunde durchrechnen, oder andersrum: Wenn die Eingangsmenge etwa 100 Bytes sind, sind das etwa 100'000 Hashes pro Sekunde. Die genauen Daten sind da gar nicht so wichtig, es geht nur um die Veranschaulichung der Grössenordnungen.

Die Fälschung der Überweisung von A nach B wäre also wohl in wenigen Mikrosekunden gemacht - wenn da nicht noch etwas wäre: Das Hash-Puzzle. Das ist das Geniale an der BC: Für einen gültigen Block muss noch ein Wert gefunden werden, der von der Transaktion gar nicht betroffen ist. Das ist die Lösung des oben erwähnten Hash-Puzzles. Da jede Hash-Funktion eben die Eigenschaft hat, dass man nicht von ihrem Resultat auf den Eingabewert schliessen kann, gilt natürlich auch das andere: Man kann nicht wissen, was man der Hashfunktion füttern muss, um einen bestimmten Wert herauszubekommen. Wollte man das, muss man halt fast unendlich viele Varianten als Eingaben durchprobieren und jedesmal das Resultat auf die gewünschte Wert-Kategorie prüfen.

Unendlich ist ja schon viel. Kleine rechnerische Betrachtung: Selbst wenn also Spezialhardware zum Mining benutzt wird, die pro Sekunde (derzeit) 100 Billionen Hashes (10^{14}) rechnen kann, so ist das immer noch wenig, denn ein SHA-256 Wert ist irgendeine Zahl zwischen 0 und 10^{77} ... das Jahr hat 31'536'000 Sekunden, das Universum ist ca. 500 Billiarden Sekunden alt, aufgerundet also nicht mal 10^{18}. Mal die 10^{14} Hashes pro Sekunde, gibt also schlappe 10^{32} Hashes für das Alter des Universums bei aktueller Hardware. Da ist 10^{77} immer noch 10^{45} mal mehr. Beim "unsicheren" SHA-1 wären es immer noch 10 Universumsalter.

Gemäss einer Info haben die Chinesen derzeit etwa 15 Exahash (15×10^{18}) pro Sekunde zur Verfügung. Das macht den Braten immer noch nicht feiss, denn bei SHA-256 ist es dann halt nur noch 10^{41} mal so viel die das gegenwärtige Universumsalter ... Wie auch immer, man kann also getrost sagen, dass man niemals für einen bestimmten Hash-Wert durch reines Variieren der Eingangsdaten diese herausfinden kann. Man kann also nur Variieren und das Resultat begutachten. Herauskommen tut immer nur eine simple Zahl. Könnte sogar mal 42 sein ...

Das Hash-Puzzle verlangt nun, dass der Hash-Wert ein bestimmtes Kriterium erfüllt. Es sagt: "Zu den Eingangsdaten für die Hash-Funktion nimm noch eine davon unabhängige Zahl (Nonce = number used once) hinzu, und hashe das. Der Hash-Wert muss dabei einfach kleiner als 1 Quadrillion sein. Wenn du eine Nonce gefunden hast, die gehashed mit dem Block einen Hash-Wert unter 1 Quadrillion ergibt, dann darfst Du diesen Block an die BC anhängen.".

Man kann das Puzzle sogar in der Schwierigkeit variieren, indem man diese Regel einfach weiter oder enger schnürt. Das passiert bei der BC alle ca. 14 Tage und nennt sich Difficulty Adjustment So sorgt die BC dafür, dass es keine Inflation von Blöcken gibt, nur weil die Hash-Rate aus irgendwelchen Gründen steigt oder sinkt.

Die BC hat also diese Regeln. Wieso soll sich diese Rechnerei überhaupt ein Teilnehmer antun, wenn es doch wohl absolut zufällig ist, ob er jemals einen Block anhängen darf? Das ist eben unter anderem abhängig vom Belohnungssystem. Und eben, die Regel kann ja so gestaltet werden, dass es immer etwa dieselben Chancen pro Zeit gibt.

Diese ganze Rechnerei ist das, was man Mining nennt, was also sehr, seeehr, seeeeeehr resourcenintensiv ist. Rechnen kostet ja auch Strom und anderes. Mining ist also weder gratis, noch einfach noch von jedermann erfolgreich zu betreiben. Da spielt es auch keine Rolle, wenn sich mehrere Miner zu Gruppen zusammenschliessen.

Man sieht, die Einspeisung von Transaktionen in eine BC ist beileibe nicht schnell. High-Speed Trading wie es die Banken vorantreiben, ist so m.E. kein Thema für die BC. Es ist daher unwahrscheinlich, dass eine BC vorhersehbar in der Lage ist, ein aktuelles Buchungssystem zu ersetzen.

Die Hashing-Power ist als jederzeit in der Lage, alle 10 Minuten einen neuen Block zu finden. Der Block beinhaltet natürlich nicht nur eine Transaktion, sondern mehrere, etwa 3-4000. Derzeit sei die Blockgrösse in der BTC 1 MByte. Das macht die BC natürlich langsam, zu langsam für die Menge an Transaktionen, die ein leistungsfähiges Transaktionssystem bearbeiten können muss in der heutige Zeit.

Die Vergrösserung der Blockgrösse wäre ein Weg da raus, aber nur sehr kurzfristig und vor allem zur Idee von Bitcoin kontraproduktiv. Denn grosse Datenmengen verlangen nach potenter Hardware. Irgendwann zuviel für kleine BC-Teilnehmer. Die Folge wäre, dass weniger Leute mitmachen könnten, oder wenn doch, die Hardware mieten - in Rechenzentren von Amazon, Google, Microsoft etc. Ein Ausfall so eines Rechenzentrums aus welchen - gerne auch sehr gewollten - Gründen legte dann zu grosse Teile der BC lahm.

Zudem ist die BC so, dass es noch lange kein Garant auf Einspeisung gibt, wenn meine Computeranlage einen gültigen Block berechnen kann. Denn, wenn mich niemand kontrolliert, berechne ich den ganzen Kram auch nicht, sondern sage einfach "der Hash-Wert ist xyz, basta.".

Nun kommt eben eine andere BC-Konzeption hinzu, die Kontrolle durch die anderen. Wenn ich einen Block für eine Transaktion gefunden (=errechnet) habe, dann muss ich das den anderen BC-Teilnehmern mitteilen, die meinen Block natürlich nicht einfach "glauben". Sie werden die Berechnung prüfen. Das ist ja nun einfach und schnell, denn es geht nicht mehr ums Finden einer Hash-Puzzle-Lösung, sondern nur noch ums Nachrechnen, ob alle Hashes seit der ersten Transaktion zu den Blockdaten passen.

Wenn ich also die BC bescheissen möchte, die Daten einer bereits in die BC eingehängten Transaktion ändern möchte, so muss ich aufgrund der Dezentralisierung der BC allen Teilnehmern meine Blöcke ab der manipulierten Transaktion bekanntmachen. Und diese Blöcke müsste ich ja zuerst berechnen, also pro Block eine Nonce finden. Und wie schwer das sein kann, habe ich oben

ja gerade dargelegt.

Dass es zu Differenzen bezüglich der Hashes unter den Teilnehmern kommen kann, ist in der BC miteinbezogen. Die Gründe für der Erscheinen der Differenzen ist völlig unerheblich für die BC, die muss nur einen klaren Weg haben, Diskrepanzen zu bereinigen. Und die hat sie.

Ein Manipulator könnte die BC manipulieren, wenn er die Power hätte, schneller neue Blöcke zu berechnen als die legitimen BC-Teilnehmer die BC selbst erweitern, denn eines der Kriterien ist, dass im Zweifelsfalle (Teilnehmer berechnen verschiedene Hashes zu einer Transaktion, was einer Verzweigung der BC gleichkommt) der längere BC-Ast als der autoritative gilt. Denn die BC erachtet mit der Zeit denjenigen Ast als wohl korrekt, in dem mehr Rechenpower steckt - ganz einfach deshalb, weil dort mehr Teilnehmer dieselben Daten berechnet haben.

Der langen Rede kurzer Sinn ist also, dass die BC sowohl im Fundament wie auch im Eskalationsprozess auf dem Kriterium der Rechenpower beruht.

Nach heutigem Ermessen ist das ausreichend. Dennoch: Was auch der Drescher nicht behandelte, ist die mögliche Gefahr der Quantencomputer. IBM hat erst grad neulich eine Maschine mit 50 QBits in Betrieb genommen. Wenn die Quantencomputer wirklich so sind, dass sie Hash-Geschichten auf einen Schlag unsicher machen, dann fällt die gesamte BC in sich zusammen. Nicht für uns, aber für diejenigen, die sich einen Quantencomputer leisten können. Und wenn die das können, dann verlieren auch wir das Vertrauen in die BC. Und Vertrauensverlust kann eine Technologie abwürgen oder gar nicht erst aufkommen lassen. Mathematiker seien zwar dran, sich Quantencomputer-resistente Algorithmen zu überlegen.

Nun, die Möglichkeiten der Quantencomputer sind derzeit noch etwas Spekulation. Sollten diese dennoch gerade hier zuschlagen, dann ist die BC natürlich gefährdet, mit ihr allerdings die gesamte andere angewandte Kryptografie auch.

Drescher hat aber die anderen Schwächen der BC angesprochen und die möglichen Lösungsansätze. Interessant ist das, was er meint, was die Geschichte dereinst zeigen könnte: Dass die BC per se zwar nur ein Hype war, dass aber die Konzeptionen sich schon irgendwie festsetzen.

Er nimmt dazu ein Zitat von Tim Berners-Lee heran, der ein demokratisches, unkontrolliertes Internet vor sich sah. Heute wissen wir, dass das Internet nicht demokratisch ist, dass die Netzneutralität gefährdet ist, dass Staaten die physischen Transportkanäle sehr wohl unter Kontrolle haben, dass NSA und andere den Verkehr abhören etc.

Die BC soll auch ein unkontrolliertes, demokratisches, selbst-regulierendes System sein. Die BC kann das sein, aber nicht offen für jedermann, nicht offen für die gigantischen Massen an Transaktionen. Sektorspezifische BCs können jedoch sicher eine überregionale Bedeutung kriegen. Die IT pusht das schon ... denn wenn man mal die prominenteste BC, Bitcoin (BTC), heranzieht, so könnte man sagen, dass BTC die digitale Version von alternativen Lokalwährungen ist. Davon gibt es auch viele, die funktionieren auch, weil sie eben regional sind, weil Produzenten und Nutzniesser im selben Perimeter damit umgehen und weil sich keine Staaten da einmischen, die juristische Lage ist klar.

Interessant ist an BTC ja auch, dass der Kurs erst durch die Decke ging, als die BTC für diejenigen mit jetzigem, überflüssigem Realgeld zum Spekulationsobjekt wurde. BTC hat noch keinen realen Einfluss, aber die Emotionen pushen schon den Kurs. Ist das nicht grad entgegen des heeren Zieles, demokratisch zu sein ...

Wenn Facebook einen FaceCoin entwickelt, so wird diese Währung innerhalb der Community Facebook funktionieren. Da diese gross ist, wird sie eine gewisse Attraktion ausstrahlen, weil viele mit FB interagieren. Doch Brot und Butter, kann ich die beim Bauer mit FaceCoin bezahlen? Es ist

also das bekannte Henne-Ei Problem.

Solange Staaten die Oberhoheit haben über Geldflüsse, die Gesetzeslage etc. und sie sich nicht mit BTC beschäftigen, solange wird BTC eben nur eine lokale Währung sein, die der Net-Citizens. Für die allerdings in der gesamten physischen Welt, für die digitalen Nomaden also.

Für mich war das Lesen von Dreschers Buch jedenfalls sehr klärend. Dafür bin ich dankbar. Der lange Artikel jetzt ... eine Art Lernkontrolle ... :-)

PS: Wer mal im Browser mit etwas SHA-xxx rumspielen will, hier geht's sehr einfach, bequem und mit etwas Erklärung:

https://www.freeformatter.com/sha256-generator.html