Weitere Gedanken zur BlockChain und BitCoin

Erfasst am : 6. Dezember 2017 15:43 | Erfasst von : Martin
Verknüpfte Kategorie(n): Gedankenspiele, Beobachtungen, Internet, Kommerz

Im meinem letzten Artikel habe ich erklärt, dass mir die BC (BlockChain) nun klar ist, weil ich dank des erwähnten Buchs vor allem die Konzepte zur "Fehlerbehandlung" dargelegt bekommen habe.

Weitere Punkte, die ich zur Betrachtung anbiete, die ich nicht ausreichend geklärt oder noch nicht behandelt fand, möchte ich hier kurz darlegen.

- Die Datenmassen einer BC, speziell der BTC (BitCoin)
  Hier fokussiere ich auf die Datenmengen: Es ist mir immer noch nicht klar, wie die BTC ihre zu erwartenden Datenmengen speichert / speichern wird. Sagen wir mal, dass in der Bankenwelt die heutige IT pro Tag 1 Milliarde Transaktionen machen, so fallen da doch einige Daten an pro Jahr. Da die Transaktion zwei Partner hat, fallen die Datenmengen bei zwei Teilnehmern an - Banken eben. Die haben genug Kohle, um die Daten sicher und schnell zu verstauen - eben WEIL sie gross und stark sind. Die BTC hingehen soll solche Peers unnötig machen. Das tut sie ja auch in autoritativer Hinsicht. Aber: Sie tut es nicht bezüglich der Resourcen: Da die BTC alle Transaktionen vorhalten muss für das Kontrollieren der Integrität der BTC, müssen also alle Transaktionen bei jedem Teilnehmer der BTC gespeichert sein. Die BTC ist global. Es gibt keinen BTC-Teilnehmer mit weniger Datenmassen.

  Gemäss Statistik habe die BRD in 2016 etwas mehr als 6 Milliarden Bank-Transaktionen gemacht, so liege ich mit der täglichen 1 Mia. für die ganze Welt nicht ganz falsch, ich runde das mal auf ca. 500 Milliarden pro Jahr. Wenn wir mal mit einer Transaktionsgrösse von 1000 Bytes ausgehen, dann sind das also 500 TBytes pro Jahr an Zuwachs. Das ist natürlich nicht so schlimm, das schaffen die Banken schon, das schafft auch eine Firma. Aber wie gesagt, jeder Teilnehmer der BTC muss das tun. Ist das nachhaltig? Zusammen mit der "Geschwindigkeit" der Transaktionen, ist das Speichern das kleinste Problem, eine BC hat ja gerade das Paradigma, dass sie nicht schnell sein kann, weil das zur Integritätskonzeption gehört.

So also noch etwas zur Transaktionen / Sekunde Zahl: Es gibt eine News-Meldung, die die Unverträglichkeit mit High-Speed-Transaktions schon mal mehr als nur andeutete und das schon im März 2016 ...
https://www.heise.de/newsticker/meldung/Kapazitaetsgrenze-erreicht-Bitcoin-Transaktionen-in-der-Warteschlange-3132893.html

Diese Meldung veranlasste jemanden, die weltweite Transaktionsgeschwindigkeit auf 7 TpS zu berechnen. Das ist natürlich ein mehr als lächerlicher Wert. Es ist schlichtweg ein absolutes NoGo.

- Geschwindigkeit des Commits
  In der Welt der RDBMS ist ein abgeschlossener Commit das Zeichen des Systems, dass etwas verarbeitet und gespeichert wurde - mit allen Konsequenzen und Nebeneffekten. Für den Entwickler ist eine Speicherung damit abgeschlossen. Der Programmierer darf sich also guten Gewissens weiteren Dingen zuwenden. Doch wie erklärt, die BC kennt keine zentrale Stelle, die ein Commit ausgeben könnte. Im Gegenteil, es kann konzeptionell eigentlich beliebig lange gehen, denn wenn die BC Diskrepanzen aus der Welt schaffen muss, bedeutet das, dass ein Quorum der Teilnehmer sich einig werden muss, welchen Ast einer Verzweigung sie nun als autoritativ ansehen will. Für den Programmierer heisst das, dass er Programme schreiben muss, die sich rückwirkend(!) mit einer Annullierung der Transaktion und deren Konsequenzen rumschlagen müssen. Es ist sogar noch schlimmer: Es könnte zu einem Totalausfall kommen, wenn die BC es nicht schafft, einen autoritativen Ast zu finden.

  Das kann je nach Anwendungszweck natürlich verschieden gravierend sein. In der NoSQL-Welt sagt man dann "eventually committed" und meint, dass es schon Dinge gibt, die man nicht per sofort committed haben muss, dass sich ein Commit aber einstellt. Tja, aber es gibt Konfliktfälle. Ob diese ein Showstopper für den Anwendungsfall der BC sein könnte, ist wohl eben von eben diesem abhängig.

  Was wäre, wenn ein Angreifer, der die BC einfach lahmlegen will, sich also als Teilnehmer anmeldet, bei der Kontrolle von errechneten Blöcken einfach an die anderen meldet: "ich habe was anderes" ... und das via Botnet nicht einfach von nur einem Teilnehmer, sondern von Tausenden? Er muss sich ja nicht mit der Historie der BC rumschlagen, er will ja nur stören, also hat er nicht einmal eine grosse Rechenlast zu bewältigen.

  Die Datenmengen müssen bewältigt werden, denn nur so ist garantiert, dass die BC im Problemfall eine Chain total durchrechnen kann. Eine Art von Caching des letzten als absolut gültig betrachteten Block kann natürlich jeder bei sich vorhalten. Er könnte sagen, dass dieser Referenzblock immer dem aktuellen Tagesdatum um eine Woche hinterher läuft, um eine Verzweigung der BC optimal schnell handhaben zu können. D.h. die Validierung der von anderen errechneten Blöcken ist einfach und schnell. Sicher ist es ja auch, denn wenn die gesamte BC an eigenen, vertrauenswürdigen Orten gespeichert ist, ändert sie dort niemand und man könnte sie jederzeit komplett nachrechnen, um den Referenzblock zu validieren. Es könnte also sein, dass der Commit einer Transaktion konzeptionell schon recht schnell erreicht werden kann.

- Wegelagerei, sprich Transaktion-Fees
  Das führt dazu, das die Miners, die ja eine Belohnung fürs Betreiben der BC bekommen wollen, sich bei den vielen Transaktionen die auswählen, die ihnen am wahrscheinlichsten eine Belohnung einbringen. Im Ethereum-Projekt nennen sie das Gas. Der Ersteller einer Transaktion gibt da eine Obergrenze an Gas mit, die er den Minern als Belohnung zur Berechnung des BC-Blocks für seine Transaktion anbietet. Ein Ethereum-BC-Teilnehmer kann sich also entscheiden, ob er diese Transaktion rechnen will. Und er kann sich sogar entscheiden, wieviele Resourcen er dafür einsetzen will, denn das Gas gibt ihm ja ein Entscheidungskriterium mit.

  Für den Transaktionserzeuger hat das diese Konsequenzen: Er weiss nicht, wie schnell seine Transaktion in die BC gelangt. Und es kostet ihn was und er weiss nicht einmal, wie sicher der Block nun ist ... denn wie erklärt, die BC kann manipuliert werden, es ist nicht unmöglich. Wenn er also einen Zahlungsvorgang über diese BC einspeisen möchte, und das in Real-Time, so kann ihm die BC diese garantierte Antwortzeit nicht erbringen. Wie im realen Leben kann er aber ein "Guter Kunde" werden, wenn er zuviel Gas anbietet. Das kann zu einer bevorzugten Behandlung führen. Ein Widerspruch zur Konzeption der BC.

- Ökologie und Geldwäsche
  Wie es sich trifft, hat auch André Kramer im Editorial der c't einen Punkt aufgegriffen, der mir natürlich schon seit Anbeginn der BC ein Dorn im Auge ist: Die Ökobilanz der BCs. Das Mining kostet ja aufgrund des Hash-Puzzles enorme Mengen an Energie, denn wer schnell sein will, muss klotzen, nicht kleckern. Kramer:

  “Denn der Stromverbrauch des Bitcoin-Mining ist immens. Die Nachrichtenseite Digiconomist hat eine einzige Bitcoin-Transaktion mit 215 Kilowattstunden Strom berechnet, dem Jahresverbrauch eines Kühlschranks. Einer Studie zufolge entsprach der Stromverbrauch für Bitcoin-Mining im Jahr 2017 dem von 159 Ländern. Die Rechnung ist kaum überprüfbar; ihr Kern bleibt aber wahr: Bitcoin-Mining trägt in hohem Umfang zur Klima-Erwärmung bei.

  Der Großteil davon findet in China statt, das seinen Energiebedarf aus fossilen Energien speist. Miner der Währung Ethereum haben Boeings des Typs 747 gechartert, um Grafikkarten an ihren Einsatzort zu fliegen. Wer sich solche Stunts leistet, betreibt höchstwahrscheinlich Geldwäsche, nicht Geldanlage.”

Mit dem letzten Satz reisst er an, wofür die BC natürlich ideal geeignet ist - um so mehr, je mehr Business an einer BC wie der BTC hängt, denn dann ist die BC fast ideal geeignet, Geldwäsche zu betreiben. Und wenn man die Kursexplosion von BTC beobachtet, so ist das Spekulieren bei ihr angekommen und im gleichen Masse wohl auch die ebenso massive Geldwäscherei. Beide schrauben sich wohl in die Höhe.

Denn die BTC ist zwar voll transparent, aber es war auch noch nie so leicht, ein Portemonnaie zu erzeugen - vollautomatisch von einem Computer, der im Darknet auf seinen Besitzer wartet, den er nicht mal kennt. Da muss man sagen, dass die Strafverfolgungsbehörden ja immer noch nach der "Folge dem Geld" Regel verfahren können, denn irgendwann muss das virtuelle Geld in reales gewechselt werden - für reale Genussfreuden. Noch. Wenn BTC eine von den Staaten und Gesellschaften akzeptierte Währung würde, fällt auch das weg. Das wird die Geldflussverfolgung sicherlich noch um 1-2 Grössenordnungen schwieriger und vielleicht aus ökonomischen Gründen unmöglich machen.

Es gibt ja den Text, dass je komplizierter ein System ist, es um so anfälliger sei. Die BC ist konzeptionell einfach, aber die Implementationen sind anfällig.

Hacker müssen sich ja nicht um die Konzeption kümmern, sondern sie kümmern sich um die jeweiligen Implementationen: Wenn sie da reinkommen, dann kann alles noch so gesichert sein, wenn sie im Code sind, ist alles möglich, was die Konzeption zulässt.

Die BTC-Börsen und andere wurden schon oft um mehrere Tausend BTC erleichtert. Von Hackern. Während das Geldwäschern vielleicht egal sein kann, so ist der Verlust des Portemonnaies einem Geschäftstreibenden überhaupt nicht egal. Und da es in der BC konzeptionell keinen Verantwortlichen gibt ... keine Kulanz von niemandem ... keine Schuldigen ... Schwarzpeter-Rumgeschiebe ... denn jeder wird eine Walletsoftware nutzen müssen. DAS Angriffsziel für Hacker und Malware-Programmierer ... eventuell grad schon auch grad geliefert mit Hintertüren für Geheimdienste, Finanzamt, Hacker etc. etc. In Zeiten von schnellem Internet - wer ist schon in der Lage, den Verkehr zu inspizieren, zu verstehen und Gegenmassnahmen zu ergreifen? Die Masse sicherlich nicht. Schöne neue Welt.

Gerade aktuell wieder ein BC-Hack:
https://www.heise.de/newsticker/meldung/Kryptogeld-Mining-Marktplatz-Nicehash-gehackt-und-bestohlen-3913041.html

Ist die BC also einfach eine Spielwiese für Technik-Nerds, IT-Profilierer, Real-Geld-Spekulanten, Geldwäschern? Es hiess ja schon beim Gold-Rush: "Reich werden nicht die Schürfer, sondern die Verkäufer von Equipment wie Schaufeln etc."

Wir werden sehen ...

PS: Ich bin derzeit kein aktiver Benutzer von BCs. Ich habe mich nur schlau gemacht und etwas weniges probiert. Gerne lese ich Korrekturen von Euch zu meinen Gedanken, sollten diese falsch oder unstimmig sein. Danke dafür.

PPS: Noch was zur Übertragungssicherheit von BTC. Eine Transaktion ist ja de facto dann auch eine Benachrichtigung an eine Email-Adresse, an ein anonymes Wallet. Kein Wunder, gibt es bereits Malware, die solche Transaktionen erkennen und auf andere Wallets umleiten:
https://www.heise.de/security/meldung/Schnueffeltrojaner-Evrial-tauscht-im-Windows-Clipboard-Bitcoin-Adressen-aus-3947596.html