Friedrich Thießen

Das Ende der **Blockchain**?

Der Beitrag untersucht, ob es sein könnte, dass die Blockchain die in sie gesetzten Erwartungen nicht erfüllen kann und ausgemustert werden wird. Im Kern ist die Blockchain (welche Variante auch immer gewählt wird) ein Datenspeicher, der durch „cryptographic proof instead of trust" (Nakamoto, 2008) funktioniert. Trotz des Hypes um sie ist die Blockchain aus ökonomischer Sicht nur ein kleiner Baustein, der nur zusammen mit weiteren Bausteinen nutzbare Geschäftsmodelle ermöglicht. Die bisher entwickelten Geschäftsmodelle zeichnen sich durch ein hohes Maß an Unsicherheit aus, die durch den „cryptographic proof"-Mechanismus der Blockchain nicht wesentlich verringert wird.

Verlagerung der Sicherheitsgenerierung von der elektronischen in die reale Welt

Betreiber von Geschäftsmodellen versuchen deshalb, durch ganz traditionelle Instrumente der Sicherheitenschaffung (wie Prüfungen durch Personen, statt durch Software; Befragung Dritter außerhalb der elektronischen Systeme; Checken der „real-world-identity" von Anbietern; Audits durch reputierliche Institutionen; Ersetzung elektronischer durch manuelle Tätigkeiten) die Sicherheit ihrer Leistungen zu erhöhen. Von dieser Verlagerung der Sicherheitsgenerierung von der elektronischen in die reale Welt ist es nur ein kleiner Schritt hin zu einem völligen Verzicht auf Blockchains, denn bei ausreichendem „trust" durch die gezeigten Maßnahmen kann der „cryptographic proof" entbehrlich werden. Die effizienteste Konstruktion eines Geschäftsmodells kann ohne die Blockchain auskommen. Was von der Blockchain bleiben wird, ist die Erkenntnis, dass ein Bedarf (a) an einer elektronischen Repräsentation von Dokumenten und Vermögenswerten (Internet der Dinge), (b) automatischen Ausführungen von Anweisungen (smart contracts), (c) Echtzeittransaktionen und (d) vollständiger Transparenz für alle besteht.

Einleitung und Zielstellung: Jeder kennt das bekannte Bonmot „Alles hat ein Ende, nur die Wurst hat zwei". Der folgende Beitrag befasst sich mit dem ersten Teil dieses Spruches, nämlich dem möglichen Verschwinden der Blockchain-Technologie in die Requisitenkiste der Geschichte. Die Forschungsfrage lautet: Könnte es sein, dass die vielbeschworene Blockchain noch ehe sie so richtig in Fahrt kommt, schon wieder ausgemustert werden wird? Diese Frage wird im Folgenden anhand einer Betrachtung derjenigen Projekte, die derzeit um die Blockchain-Technologie herum verfolgt werden, untersucht.

Im Ergebnis zeigt sich: Die Blockchain-Technologie beeindruckt. Aber sie ist doch ein eher kleiner technologischer Baustein, der nur zusammen mit vielen weiteren Bausteinen sinnvoll ökonomisch genutzt, also in Geschäftsmodelle integriert werden kann. Ausgereifte Geschäftsmodelle benötigen die Blockchain-Technologie aber eher nicht – das zeigen die derzeit laufenden Projekte. In vielen Geschäftsmodellen wird die Blockchain eher ein hinderliches Element sein.

Grundlagen: Die Blockchain-Technologie selbst braucht nicht mehr vorgestellt zu werden. Die bekannteste Variante des Pseudonyms Satoshi Nakamoto (Bitcoin) ist oft genug dargestellt worden. Kern aller Blockchain-Technologien ist ein unfälschbarer, transparenter Speicher entfernt von traditionellen Institutionen, der durch „cryptographic proof instead of trust" (Nakamoto, 2008, Seite 1) funktioniert. Dies ist die zentrale Idee der Blockchain. Nakamotos Entwicklung ist so umwerfend „anders", dass sich niemand der Faszination des Systems entziehen kann. Genau diese Faszination für die Technik ist dann aber Teil der jetzt zu beobachtenden Probleme geworden. Die Technikfokussierung lenkte den Blick weg von den problematischen Aspekten der Innovation.[1)] Denn das, was Satoshi Nakamoto beschrieben hat, oder was in Varianten heute entwickelt wird, sind keine vollständigen Lösungen ökonomischer Probleme. Es sind vielmehr nur Bausteine, die durch weitere Bausteine ergänzt werden müssen, um die Technologie ökonomisch nutzen zu können und die dann eventuell auch entfallen können.

Mindestens drei Bausteine

Die Anwendung der Blockchain-Technologie setzt mindestens drei Bausteine voraus: erstens die Blockchain selbst mit der dazugehörigen Software, zweitens Wallet und drittens Verschlüsselung. Die Blockchain ist der dezentrale Datenspeicher. Wallets sind Softwareprogramme, mit denen Nutzer kommunizieren und Eintragungen in Blockchains veranlassen können. Die Verschlüsselung als Konsequenz der angestrebten Dezentralität ist Voraussetzung für Transaktionen und ohne weitere Softwareprogramme nicht einsetzbar.

Die Geschäftsmodelle, die sich rund um die Blockchain etabliert haben, erfordern weitere zusätzliche Programme. Sie werden nach Schlatt u.a. (2016, Seite 16) nach dem Kriterium der Anwendernähe in die Kategorien Plattformen, Middleware-Software[2], Applikationen und Nebenleistungen gegliedert.

Im Folgenden wird zunächst gezeigt, wie im Hype um die Blockchain-Technologie deren Sicherheits- und Funktionalitätsdefizite oft verschleiernd dargestellt werden. Dann wird darauf eingegangen, wie es mit der Sicherheit tatsächlich beschaffen ist. Anschließend wird erläutert, wie Anbieter von Blockchain-basierten Leistungen zur Verbesserung von Sicherheit und Vertrauen zu ganz klassischen Instrumenten greifen, nämlich zur Nutzung gut regulierter Institutionen und deren Reputation – etwas, das ja eigentlich durch die Blockchain-Technologie entbehrlich werden sollte. Schließlich wird geprüft was von der Blockchain-Technologie in Zukunft noch gebraucht wird, wenn das Prinzip „cryptographic proof instead of trust" nicht funktioniert und „trust" letztlich doch auf klassischen Wegen geschaffen wird.

Die Sicherheit von Blockchains in Wahrnehmung und Wirklichkeit

Übertriebene Euphorie: Nakamoto (2008) hat sich in seinem im Internet veröffentlichten Beitrag vor allem dem Aspekt der Sicherheit durch Kryptografie in einem dezentralen System gewidmet. Genau dieser Aspekt hat wiederum auch in populären Medien den größten Widerhall gefunden. Dabei wird die Sicherheit von Blockchain-basierten Geschäftsmodellen oft auf eine übersteigerte Art und Weise dargestellt. Einige der folgenden Beispiele belegen dies:[3]

– Blockchains ermöglichen Transaktionen ohne die Notwendigkeit gegenseitigen Vertrauens.

– Für Transaktionen mit einer Blockchain wird kein Mittelsmann benötigt. Das System übernimmt die Verifizierung der Transaktion.

– Das Bitcoin-System funktioniert reibungslos.

– Die Öffentlichkeit drückt der Transaktion ihren virtuellen Stempel auf: alles korrekt.

– Damit niemand betrügen kann, sind die Rechner zu einem Netzwerk zusammengeschlossen und kontrollieren gemeinsam.

– Der Nutzer erstellt ein Bitcoin-Wallet. Das ist eine Art Kreditkarte.

Im letzten Fall wurden Blockchain-basierte Zahlungen mit der Sicherheit von Kreditkartenzahlungen verglichen, wobei gerade Wallets häufig erfolgreich angegriffen wurden und man anders als bei Kreditkartenzahlungen gestohlene Gelder gerade nicht zurückfordern kann.

Ausgewählte Risiken: Damit sind einige der verharmlosenden Aussagen zur Sicherheit von Blockchain-Transaktionen genannt. Wie steht es nun um die Sicherheit „realer" Geschäftsmodelle? Anhand einiger Beispiele wird gezeigt, welche Erkenntnisse es in dieser Hinsicht gibt.

– Schlatt u.a. (2016, Seite 7) zeigen, dass zwischen der Blockchain als Datenstruktur und dem zugehörigen Verwaltungssystem unterschieden werden muss. Ersteres ist ohne das Zweite nicht benutzbar, das Zweite kann aber angreifbar und unsicher sein.

– Das Bundesamt für Sicherheit in der Informationstechnik (BSI, 2018) warnt: „Blockchain allein löst keine IT-Sicherheitsprobleme." Außer der Blockchain selbst müsste „gleichzeitig die Sicherheit der verwendeten Hard- und Software sowie der zugrunde liegenden Protokolle gewährleistet werden." Problematisch sind die „externen Schnittstellen der Blockchain, insbesondere für das authentische Einfügen oder Auslesen von Daten".

– Die Blockchain-Technologie verursacht Probleme mit der Langzeitsicherheit, etwa wenn sich Computersprachen ändern, weil das Problem, ob überhaupt irgendein Softwarelieferant und Systembetreiber Interesse hat, langfristig seine Dienste anzubieten und Kundenrechte zu sichern, nicht gelöst ist. Nutzer speichern erhebliche Werte in Blockchains, ohne sicher zu sein, dass sie auch langfristig darauf zugreifen können (BSI, 2018).

– Die Handelsplattform Bitfinex warnt vor "unusual activities", welche bei der


Foto: Christine Kornack

Prof. Dr. Friedrich Thießen

Professur für Finanzwirtschaft und Bankbetriebslehre, Technische Universität Chemnitz

Der Untersuchungsgegenstand des Autor klingt überraschend. Während in den Medien und der Praxis in der Kreditwirtschaft geradezu ein Hype um das Schlagwort Blockchain ausgebrochen ist und fast nur noch über das Ausmaß der Veränderungen gesprochen wird, die diese Schlüsseltechnologie in vielen Branchen haben könnte, wirft der Autor die Frage auf, ob sie nicht schon wieder ausgemustert werden könnte, bevor sie so richtig in Schwung geraten ist. Seine eher zurückhaltende Sicht der Dinge: Die Blockchain-Technologie übt auf viele Branchen eine große Faszination aus. Aber in der praktischen Anwendung ist doch ein eher kleiner technologischer Baustein, der nur zusammen mit vielen weiteren Elementen sinnvoll ökonomisch genutzt, also in Geschäftsmodelle integriert werden kann. Solange Geschäftsmodelle als Maßnahmen der Vertrauensschaffung die Rolle externer Institutionen bemühen müssen, kann die Blockchain sich eher als ein hinderliches Element erweisen. Den Bedarf an einer elektronischen Repräsentation von Dokumenten, Vermögenswerten und sonstigen Objekten, automatische Ausführungen von Anweisungen, Echtzeittransaktionen sowie vollständiger Transparenz für alle sieht er gleichwohl und schließt deshalb eine Weiterentwicklung der Blockchain nicht aus. (Red.)

Blockchain-Technologie grundsätzlich nicht ausgeschlossen werden könnten. „Session Hijacking" sei ein Sicherheitsproblem. Die Börse gibt den Rat, ergänzende Analysesysteme einzusetzen. Außerdem wird geraten: „Instantly freeze your account if you suspect malicious activity". Und weiter: "Limit access to your account based on IP address." Oder: "Define an address whitelist to ensure no withdrawals can go anywhere else." Weiter wird geraten: „Add an extra layer of security to your account and protect sensitive operations such as logging in."[4)]

Signifikante Differenzen

Wenn man diese Probleme und Ratschläge mit den oben zitierten euphorischen Aussagen zur per se vorhandenen Sicherheit aus den Medien vergleicht, erkennt man signifikante Differenzen.[5)]

Fehlende Haftung: Das Problem verstärkt sich, weil die Bereitschaft der Anbieter, für ihre Dienstleistungen einzustehen und zu haften, gering ist. Die Anbieter kennen die Risiken selbstverständlich und versuchen, sich von allen Ansprüchen freizuhalten. Die Allgemeinen Geschäftsbedingungen von Bitfinex enthalten überwiegend Formulierungen wie „assumes no liability or responsibility". Das gilt für „any claim, application, loss, injury, delay, accident, cost, business interruption cost or any other expenses". Eingeschlossen sind auch Kernaspekte der Dienstleistungen wie „data loss, computer failure or malfunction". Wer die Services dieser Börse nutzt, muss erklären, dass er Bitfinex und seine Mitarbeiter von allen „liabilities for any and all losses" entbindet.[6)]

Es gibt zwei Internetseiten, die eine besondere Reputation in der Blockchain-Community besitzen. Das ist zum einen die von Satoshi Nakamoto selbst ins Leben gerufene Seite www.bitcoin.org sowie die Seite des sogenannten Bitcoin Wiki.[7)]

Die Seite www.bitcoin.org weist – ganz im Gegensatz zu euphorischen Medien – auf vielerlei Gefahren der Blockchain-Technologie hin. Ausdrücklich werden korrupte Wallets und falsch strukturierte Transaktionen genannt sowie auch das heikle Problem, dass selbst in einem der Herzstücke der Blockchain-Technologie, dem sogenannten „Mining", Sicherheitsprobleme auftreten.

Sicherheits- und Funktionsprobleme nicht ausgeschlossen

In den Medien heißt es zum Mining: "Jeder gefundene Block wird zur Prüfung ausgerufen und von den anderen Rechnern gecheckt – alles in Ordnung". Die Realität sieht dagegen so aus: "Unfortunately, it turned out that roughly half the network hash rate was mining without fully validating blocks."[8)] Und weiter: „Some miners are currently generating invalid blocks" und "almost all software will accept these invalid blocks under certain conditions."[9)]

Das bedeutet letztlich, dass es in allen dreien der oben genannten Grundbausteine der Blockchain-Technologie Sicherheits- und Funktionsprobleme geben kann. Dazu gehört die Blockchain und die damit zusammenhängende Software selbst, Wallets und Verschlüsselung. Das erschüttert die These von einem sicheren System durch Dezentralisierung und Kryptografie (distributed ledger, cryptographic proof).

Mittlerweile sind die Sicherheitsprobleme der Blockchain-Technologie nicht mehr ganz unbekannt, und Anbieter von Blockchain-basierten Leistungen fangen an, zusätzliche Mechanismen einzubauen, welche Vertrauen schaffen. Im Folgenden wird überprüft, welche vertrauensbildenden Maßnahmen und Mechanismen dabei Verwendung finden.

Bevor aber diese vertrauensbildenden Maßnahmen näher beleuchtet werden, wird noch einmal aufgezeigt, womit das Blockchain-System angetreten ist: Von der Idee her sind zusätzliche vertrauensbildende Maßnahmen systemfremd. Denn das System basiert, wie Nakamoto selbst formuliert, auf „cryptographic proof instead of trust".[10)] Das ist die zentrale Idee. Die Blockchain-Community war immer besonders stolz darauf, dass das Blockchain-System unabhängig von Institutionen auskomme. Niemandem müsse getraut werden. Jedelsky und Wiegelmann (2018, Seite 34f.) fassen diese Sichtweise so zusammen: „Blockchains sind … Datenbanken … ohne eine zentrale Kontrollinstanz, ohne die Notwendigkeit gegenseitigen Vertrauens der Parteien … Keine Institution muss als Vertrauen stiftender Partner zwischen misstrauischen Händlern vermitteln." Demgegenüber findet man aber, dass Blockchain-basierte Dienstleister zunehmend auf Institutionen hinweisen, die als Vertrauensgeber fungieren. Immer weniger wird dem reinen Prinzip des „cryptographic proof" vertraut. Dies kann an einigen Beispielen beleuchtet werden:

Rückgriff auf traditionelle Sicherheitsprüfungen

Laut dem Handelssystem Bitfinex können Vermögenswerte in „cold wallets" (offline) oder in „hot wallets" (online) deponiert werden. Ersteres sei sicherer, weil „the funds in offline cold storage require manual intervention by several members of our management to access."[11)] Das ist hervorzuheben, denn wenn es von einem Börsenbetreiber selbst für sinnvoll gehalten wird, dass mehrere Personen manuell über eine Transaktion schauen, dann kann das Versprechen der Sicherheit allein durch „cryptographic proof" im Rahmen rein elektronischer Prozesse nicht stimmen. Mehrere Personen, die sich gegenseitig kontrollieren, sind ein ganz klassisches, herkömmliches Instrument, Sicherheit zu schaffen. Erstaunlicherweise empfiehlt die größte mit Blockchain-Technologie arbeitende Börse, genau dieses alte beziehungsweise uralte Instrument zu nutzen.

Im Bitcoin-Wiki wird empfohlen, Software erst dann zu nutzen, wenn man in Nutzerkreisen positive Empfehlungen dazu gefunden habe: „Before trusting or sending your bitcoins to any website you should always search on additional community resources to see what other users are saying about the service."[12)] Auch das ist hervorzuheben: Man soll sich also auf die Urteile von „other users" stützen,

statt allein auf „cryptographic proof“ der Blockchain. Auch dies, also die Befragung von Dritten, ist ein sehr altes, klassisches, herkömmliches Instrument, Sicherheit zu schaffen.

Es geht weiter: Im Bitcoin-Wiki findet man den Hinweis, dass man aus der elektronischen Welt herausgehen sollte, um die „real-world-identity“ von Verantwortlichen zu erkunden: „When sending money to an exchange or seller you are trusting that the operator will not abscond with your funds and that the operator maintains secure systems that protect against theft – internal or external. It is recommended that you obtain the real-world identity of the operator.“[13] Der Verweis auf die „real-world identity“ ist besonders interessant. Denn eine solche Überprüfung macht nur dann Sinn, wenn in der realen Welt mehr Sicherheit und Vertrauenswürdigkeit vorhanden ist als in der elektronischen, und das ist nur deshalb der Fall, weil es dort anders als in der virtuellen Welt Institutionen des Vertrauens (etwa Unternehmen mit Reputation, Regulierung, Gesetze, Staatsanwälte, Polizei, Haftung) gibt.[14]

Institutionen mit Reputation

Noch einen Schritt weiter geht die Internetbörse Kraken. Sie wirbt damit, sich als eine der ersten Institutionen der Blockchain-Welt extern überprüft haben zu lassen: „Kraken is an exemplary institution that the rest of the Bitcoin world should look up to. [It is] one of the first exchanges to pass an independent audit.“[15] Das Zitat zeigt, dass Kraken die externe Auditierung sogar als richtungsweisend ansieht („should look up to“).

Zusammenfassend zeigen diese Beispiele ganz deutlich, wie die geringe Sicherheit der Blockchain-basierten Geschäftsmodelle zunehmend durch ganz klassische, herkömmliche Instrumente der Sicherheits- und Vertrauensschaffung verbessert wird. Ohne Institutionen mit Reputation geht es offenbar nicht. Mehrfachkontrolle durch unabhängig voneinander agierende Personen, manuelle statt rein elektronische Dienstleistungsausführungen, Befragung von Dritten, Reale-Welt-Identität und unabhängige Audits – alles klassische Instrumente der Sicherheitsschaffung – werden für sinnvoll erachtet.

Welche Folgen hat die zunehmende Verwendung solcher klassischen Instrumente der Sicherheitenschaffung? Es liegt die Überlegung sehr nahe, dass eine verbesserte Anwendung der klassischen Instrumente den „cryptographic proof“ der Blockchain-Technologie entbehrlich oder überflüssig machen könnte, weil die Sicherheit ausreichend ist und eventuell sogar effizienter bereits durch die klassischen Sicherheitsmaßnahmen gewährleistet werden kann. Das wäre dann das „Ende der Blockchain“.

Überprüfung von Anwendungsfeldern der Blockchain

Unter diesem Blickwinkel werden Anwendungsfelder der Blockchain überprüft. In der Literatur findet man Hinweise zu folgenden geplanten Anwendungen:[16]

– Speicher von Immobiliendaten von der Planung über den Bau und Betrieb bis zum Rückbau, etwa mit Lageinformationen, Grundbuchdaten, Technikinformationen und Mieterhistorie.

– Abbildung der Transaktionshistorie von Immobiliengeschäften.

– Unbestechliches Grundbuch (in korrupten Ländern).

– „Tokenization“ von Immobilien (Handel von Immobilien).

– Zentrales Register einer unfälschbaren Buchhaltung. Echtzeitbuchführung.

– Eintragung von steuerrelevanten Einnahmen unter einer Steuernummer.

– Notariatsservice (proof of existence von Dokumenten, zum Beispiel Ehedokumente, Testamente, Geburtsurkunden, Versicherungsnachweise).

– Repräsentation von Lizenzen und deren Versteigerung.

Zeitschrift für das gesamte
KREDITWESEN

Verlag und Redaktion:

Verlag Fritz Knapp GmbH
Aschaffenburger Str. 19, 60599 Frankfurt,
Postfach 70 03 62, 60553 Frankfurt.

Telefon: (0 69) 97 08 33 - 0, Telefax: (0 69) 7 07 84 00
E-Mail: red.zfgk@kreditwesen.de
Internet: www.kreditwesen.de

Herausgeber: Klaus-Friedrich Otto

Chefredaktion: Dr. Berthold Morschhäuser (Mo), Philipp Otto (P.O.)

Redaktion: Swantje Benkelberg (sb), Philipp Hafner (ph), Hanna Thielemann (ht), Frankfurt am Main

Redaktionssekretariat und Layout: Patricia Appel

Verlagsleitung: Philipp Otto

Anzeigenleitung: Timo Hartig

Anzeigenverkauf: Hans-Peter Schmitt,
Tel. (0 69) 97 08 33-43

Zurzeit ist die Anzeigenpreisliste Nr. 60 vom 1.1.2018 gültig.

Zitierweise: KREDITWESEN

Erscheinungsweise: am 1. und 15. jeden Monats.

Bezugsbedingungen: Abonnementspreise inkl. MwSt. und Versandkosten: jährlich € 610,49, bei Abonnements-Teilzahlung: ½-jährlich € 313,67, ¼-jährlich € 160,00. Ausland: jährlich € 632,81. Preis des Einzelheftes € 25,00 (zuzügl. Versandkosten).

Verbundabonnement mit der Zeitschrift »bank und markt«: € 930,63, bei Abonnements-Teilzahlung: ½-jährlich € 488,62, ¼-jährlich € 256,27. Ausland: jährlich € 957,98.

Studenten: 50% Ermäßigung (auf Grundpreis).

Der Bezugszeitraum gilt jeweils für ein Jahr. Er verlängert sich automatisch um ein weiteres Jahr, wenn nicht einen Monat vor Ablauf dieses Zeitraumes eine schriftliche Abbestellung vorliegt. Bestellungen direkt an den Verlag oder an den Buchhandel.

Probeheftanforderungen bitte unter
Tel.: (069) 97 08 33-25.

Bei Nichterscheinen ohne Verschulden des Verlags oder infolge höherer Gewalt entfallen alle Ansprüche.

Bankverbindung: Frankfurter Sparkasse,
IBAN: DE68 5005 0201 0200 1469 71, BIC: HELADEF1822.

Druck: Hoehl-Druck Medien + Service GmbH, Gutenbergstraße 1, 36251 Bad Hersfeld.

ISSN 0341-4019

– Verwalten und Nutzen von Musikrechten.

– Verwaltung von Hotelkontingenten (unabhängig von booking.com).

– Repräsentation und Handel von Diamanten mit genauen Informationen über Herkunft und Qualität.

– „Internet der Dinge“: Repräsentation jeder Art von Geräten, Programmen, Werten in Blockchains. Handel und Steuerung der „Dinge“.[17)]

– „Internet der Verträge“: Abbildung aller Arten von bi- und multilateralen Verträgen und automatische Überwachung von Bedingungen und Ausführung von Anweisungen.

– Banken ohne Banklizenzen (sicher wegen Blockchain) zum Beispiel in unsicheren, korrupten Schwellenländern.

– Diverse ICOs (Initial Coin Offerings).

– Digital Trade Chain (Handelsfinanzierung). Forderungsverwaltung und -handel.

– Repräsentation von Schuldscheinen beziehungsweise Schuldscheindarlehen, Geldmarktwertpapiere mit integriertem Handel und Abwicklung unter Ersparung zusätzlicher Clearingsysteme.

– Repräsentation von Wertpapieren. Handel und Verbuchung von Wertpapieren in Echtzeit.

– Emission von Wertpapieren: Konsortiums-Blockchains.

– Repräsentation und Handeln von Unternehmensbeteiligungen.

– Emission von Geld durch Zentralbanken (EZB).

– Emission von goldgedecktem Zentralbankgeld in korrupten, instabilen Ländern (Venezuela).

Die Projekte erlauben einen Blick in die grundlegenden gewünschten Eigenschaften. Nach Buhl u.a. (2017, Seite 33) sowie Schlatt u. a. (2016, Seite 15ff.) zeigen die vorhandenen Projekte, dass insbesondere die folgenden sechs Aspekte auf Interesse stoßen:

– Verzicht auf traditionelle Autoritäten,

– unveränderbare Daten,

– vollständige Transparenz für alle,

– Echtzeittransaktionen,

– Internet der Dinge: Elektronische Repräsentation von Dokumenten und Vermögenswerten zur elektronischen Weiterverarbeitung,

– automatische Ausführung von Anweisungen (smart contracts).

Bedarf bisher nicht erkannt

Es ist leicht einzusehen, dass diese Aspekte bei den meisten oben genannten Vorhaben und Einsatzgebiete auch ohne Blockchain erfüllt werden können. Wenn zum Beispiel Depotbanken Echtzeittransaktionen mit sofortiger universeller Transparenz bisher nicht angeboten haben, dann liegt das nicht daran, dass es grundsätzlich nicht ginge, sondern daran, dass der Bedarf nicht erkannt wurde. Erst durch Bitcoin ist man auf viele neue Möglichkeiten und die Nachfrage danach aufmerksam geworden. Zum Realisieren dieses Neuen braucht man aber nicht zwingend die Blockchain, sondern kann vielerlei Wege beschreiten.

Braucht man zum Beispiel sowieso einen Trustee, um ein Blockchain-basiertes Geschäftsmodell zu auditieren (siehe Blockchain-Börse Kraken), dann ist es kein großer Gedankensprung mehr, diese intendierte Leistung gleich durch einen Trustee erbringen lassen – es muss nicht unbedingt die anonyme Blockchain sein.

Die langfristige, dauerhafte Repräsentation von etwa von Dokumenten, Wertpapieren und sonstigen Verträgen, also das Internet der Dinge, kann eine Depotbank mit ihrem Renommee und ihrer Regulierung sicherlich besser bewerkstelligen als

eine anonyme Blockchain-Struktur. Die Blockchain mit den vielen Problemen der dezentralen Verifizierung wird in vielen Projekten eher hinderlich sein, eine Leistung adäquat und effizient zu erbringen – Sicherheit schafft sie, wie oben gezeigt, sowieso nicht ausreichend.

Geschäftsmodelle haben viele Angriffspunkte

Der vorliegende Beitrag untersuchte die Frage, ob es sein kann, dass die Blockchain-Technologie schnell zu einem vorzeitigen Ende gelangt. Das Prinzip der Blockchain ist „cryptographic proof instead of trust" (Nakamoto, 2008). Es konnte gezeigt werden, dass die Blockchain nur ein kleines Element im Rahmen von Geschäftsmodellen darstellt, die in der Regel so viele Angriffspunkte bieten, dass von „trust" überhaupt keine Rede sein kann. Es konnte weiter gezeigt werden, dass die Blockchain-Community mittlerweile selbst dazu übergeht, ganz traditionelle Instrumente der Sicherheits- und Vertrauensschaffung zu nutzen, wie unter anderem Prüfungen durch Personen, statt durch Software, Befragung Dritter außerhalb der elektronischen Systeme, Checken der „real-world-identity" von Anbietern, Audits durch reputierliche Institutionen.

Außerdem werden elektronische durch manuelle Tätigkeiten ersetzt. Von dieser Verlagerung der Sicherheitsgenerierung auf Institutionen der realen Welt ist es nur ein kleiner Schritt hin zu einem völligen Verzicht auf Blockchains, denn bei ausreichendem „trust" durch die gezeigten Maßnahmen kann der „cryptograhic proof" entbehrlich werden. Die effizienteste Konstruktion eines Geschäftsmodells kann ohne die Blockchain auskommen.

Damit soll nicht gesagt werden, dass sich die Blockchain-Technologie nicht weiterentwickeln kann. Es sind enorme Bemühungen in dieser Hinsicht festzustellen. Niemand weiß, was noch alles erfunden werden wird. Aber derzeit kann es nicht als ausgeschlossen gelten, dass die Blockchain-Technologie zu einem vorläufigen Ende gelangt. Was von der Blockchain bleiben wird, ist die Erkenntnis, dass ein Bedarf an einer elektronischen Repräsentation von Dokumenten, Vermögenswerten und sonstigen Objekten (Internet der Dinge), automatische Ausführungen von Anweisungen (smart contracts), Echtzeittransaktionen und vollständige Transparenz für alle besteht. Projektbetreiber sollten versuchen, diese Eigenschaften in ihren Vorhaben zu realisieren mit genau den Instrumenten, die dafür effizient sind, ohne krampfhafte Fokussierung auf die Blockchain.

Für wertvolle Unterstützung bedankt sich der Autor vor allem bei MA Jan Justus Brenger.

Fußnoten

1) Nakamoto (2008) war vorrangig an den technischen, insbesondere kryptografischen Prozessen interessiert. Dies kann aus den Quellen geschlossen werden, die er seinem Internetbeitrag hinzufügte. Er hat der Frage, was ein funktionsfähiges ökonomisches Geschäftsmodell ausmacht, weniger Beachtung geschenkt. Es ist aber nicht so, dass Nakamoto ökonomischen Aspekten gar keine Wichtigkeit beimaß. Nakamoto hat sein Paper 2008/2009 veröffentlicht – das heißt nach der Subprimekrise, also nach dem Zusammenbruch und Beinahezusammenbruch namhafter Banken. Die Idee, beim Speichern wichtiger Daten auf solche unsicheren Institutionen verzichten zu können, ist eine ökonomische und traf den Nerv der Zeit. Aber sein Paper ist bei solchen ökonomischen Überlegungen deutlich weniger ausgearbeitet als bei den technischen Aspekten.
2) Als Verbindung von Plattformen und Applikationen.
3) Vgl. zum Beispiel die Zusammenfassungen in Behrens, 2017; Bolesch, Mitschele (2016); Schilder (2017) und Schilder (2018).
4) Vgl. www.bitfinex.com
5) Weitere Risiken: Bei Lisk kann jedermann smart contracts mit JavaScript erstellen, die dann „auf ewig" in einer Blockchain gespeichert werden. In der Realität werden wichtige Verträge von erfahrenen Notaren und Rechtskundigen geschrieben und von vielerlei Augen kontrolliert. Der Unterschied und die Risiken brauchen nicht ausgeführt zu werden.
6) Vgl. www.bitfinex.com. Interessant sind auch die Versuche, Haftung und Aufsicht auch in Zukunft zu verhindern. Die Brüder Cameron und Tyler Winklevoss, die höchstwahrscheinlich sehr viel dazu beigetragen haben, den Kurs von Bitcoins nach oben zu manipulieren, wollen eine Aufsicht mit allen Mitteln verhindern und plädieren für „self-regulatory organisations to oversee the emerging crypto-currency industry". Eine ideale SRO in ihren Augen würde sich aus Vertretern derjenigen Unternehmen zusammensetzen, die eigentlich überwacht werden sollten. Als Alternative wird in den USA „a rationalized federal framework" diskutiert. Die Antwort der Lobby ist eine SRO, die zwar aus Unternehmensvertretern besteht, die aber wenigstens „the most independence from its membership" aufweisen. Ein Strolch, wer Böses bei solchen Vorschlägen denkt; vgl. Rennison, 2018.
7) Es heißt: „Dies ist ein Community Wiki, in welchem alle Informationen über Bitcoin von der Bitcoin Community frei zusammengetragen werden können." Vgl. https://de.bitcoin.it.
8) Vgl. https://en.bitcoin.it.
9) Vgl. https://en.bitcoin.it.
10) Nakamoto, 2008, S. 1
11) Vgl. www.bitfinex.com.
12) Vgl. https://en.bitcoin.it.
13) Vgl. https://en.bitcoin.it.
14) Weiter findet sich: "Exchanging or storing significant amounts of funds with third-parties is not recommended." Das ist ein wirkliches Armutszeugnis, weil die Blockchain-Community ja angetreten war mit der Idee u.a. Depotbanken überflüssig zu machen.
15) Vgl. www.kraken.com.
16) Vgl. u.a. Backhaus, 2017; Bank, 2017; Buhl, u.a., 2017; Dentz, 2017; Jedelsky, Wiegelmann, 2018; Mizrahi, 2015; Paulus, 2017; Preithnner, 2017; Schlatt u.a., 2016; Weber, Gruber, 2017.
17) Wichtig sind hierbei die Überlegungen von Mizrahi (2015). Er zeigt, dass der Start einer neuen Blockchain, die werthaltige Objekte repräsentiert (etwa Geld, Dokumente, Schuldscheine, Grundbücher), ohne externe, vertrauenswürdige Personen nicht möglich ist, weil man sonst nicht sicher sein kann, dass die werthaltigen Objekte überhaupt vorhanden sind. Keine Blockchain kann in diesem Sinne aus sich selbst heraus starten. Wenn man etwa Grundstücke, Dokumente, Schuldscheindarlehen abbilden will – was viele Blockchain-Projekte vorhaben, braucht man vertrauenswürdige Lieferanten und regelmäßig vertrauenswürdige „Bestätiger", die sicherstellen, dass die Objekte überhaupt noch da sind. Die Blockchain-Technologie kann nicht per se für die Existenz der abgebildeten Dinge garantieren.

Literatur

Backhaus, D. (2017), Daimler platziert Schuldschein via Blockchain, in: Der Treasurer v. 19.7.2017
Bank (2017), Aus dem Hype wird langsam Ernst, in: Die Bank, Heft 8, Seiten 26 bis 29
Behrens, C. (2017), Kampf um die Seele von Bitcoin, Süddeutsche Zeitung vom 2. August 2017
Bolesch, L., Mitschele, A. (2016), Revolution oder Evolution? Funktionsweise, Herausforderungen und Potenziale der Blockchain-Technologie, in: Zeitschrift für das gesamte Kreditwesen, Heft 22, Seite 35
BSI (2018), Blockchain sicher gestalten – Eckpunkte des BSI, Bundesamt für Sicherheit in der Informationstechnik, Bonn
Buhl, H., Schweizer, A., Urbach, N. (2017), Blockchain-Technologie als Schlüssel für die Zukunft, in: Zeitschrift für das gesamte Kreditwesen, Heft 12, S. 30 bis 33.
Dentz, M. (2017), Treasurer Kurt Schäfer über Daimlers Blockchain-Deal, in: Der Treasurer v. 27. September 2017
Jedelsky, A., Wiegelmann, T. (2018), Die Blockchain-Technologie und ihr Potenzial für die Immobilienwirtschaft, in: Immobilien und Finanzierung, Heft 3-2018, Seiten 34 bis 36
Mizrahi, A. (2015), A blockchain based property ownership record system, verfübar im Internet unter http://chromaway.com
Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, o.O.
Paulus, S. (2017), Commerzbank und KfW steigen in Blockchain-Wettlauf ein, Der Treasurer vom 27. September 2017
Preithnner, M. (2017), Building Information Modeling – ein Informationspool für Immobilienbewerter?, in: Immobilien und Finanzierung, Heft 23, Seiten 14 bis 17
Rennison, J. (2018), Treasury must fill regulatory `vacuum` on crypto assets, says top CFTC official, in: Finanical Times vom 15. März 2018
Schilder, R. (2017), Bitcoin – wundersame Geldvermehrung, in: Freie Presse Chemnitz vom 11. August 2017
Schilder, R. (2017), Das nächste große Ding, in: Freie Presse Chemnitz vom 19. Juli 2017
Schlatt, V., Schweizer, A., Urbach, N., Fridgen, G. (2016), Blockchain: Grundlagen, Anwendungen und Potenziale, Fraunhofer FIT, Projektgruppe Wirtschaftsinformatik, Universität Augsburg, Augsburg
Weber, V., Gruber, V. (2017), Immobilienbewertung in Zeiten des technologischen Wandels, in: Immobilien und Finanzierung, Heft 23, S. 25 bis 26