Dirk Achenbach, Ingmar Baumgart, Jochen Rill

Die Blockchain im Rampenlicht

Technologie von der Stange – oder besser nach Maß?

Es gibt verschiedene Ausprägungen der Blockchain-Technologie; einige davon wurden in DuD 8/2017 vorgestellt. Sie unterscheiden sich insbesondere in den ihnen zugrundeliegenden (Sicherheits-) Annahmen und Mechanismen. Daher darf die Blockchain nicht als Universaltechnologie gesehen werden – die Gründe dafür diskutieren die Autoren im vorliegenden Beitrag.

1 Einleitung

Mode wird gemeinhin mit Laufstegen in Mailand, Paris, London und New York verbunden. Aber auch in der Informationstechnologie gibt es Moden. Je nach Saison wähnt man in unterschiedlichen Technologien die Antwort auf die Geißeln der Menschheit: Web 2.0, Cloud Computing, RFID, neuronale Netze. Die derzeit angesagte Mode ist die Blockchain. Durch Blockchain-Technologie sollen Finanzmärkte umgekrempelt[1], die Musikbranche neu aufgestellt[2] und der Energiehandel revolutioniert[3] werden.

Die Blockchain ist unbestrittenen eine interessante Technologie mit einem großen Potential, die jedoch in einem sehr frühen Entwicklungsstadium ist. Die Weiterentwicklung der Blockchain-Technologie ist noch nicht an ihrem Ende und uns erwarten noch einige Durchbrüche in der Erforschung der Technologie. Wie bei jeder Technologie, die sich noch in der Entwicklung befindet, ist ihr Einsatz in kommerziellen Anwendungen mit Vorsicht zu empfehlen, insbesondere, wenn Sicherheit ein wichtiger Faktor ist. Dieser Beitrag beleuchtet Annahmen, Maßnahmen und Garantien verschiedener Ausprägungen der Blockchain.

Dr. Dirk Achenbach

leitet das Kompetenzzentrum IT-Sicherheit am FZI Forschungszentrum Informatik in Karlsruhe.

E-Mail: achenbach@fzi.de

PD Dr.-Ing. Ingmar Baumgart

leitet das Kompetenzzentrum IT-Sicherheit am FZI Forschungszentrum Informatik und ist Privatdozent am Karlsruher Institut für Technologie (KIT).

E-Mail: baumgart@fzi.de

Jochen Rill

ist stellvertretender Abteilungsleiter am FZI Forschungszentrum Informatik in Karlsruhe.

E-Mail: rill@fzi.de

2 Vorbemerkung: Modelle, Mechanismen und Sicherheitsgarantien

Um die Sicherheit einer Systemarchitektur strukturiert untersuchen und bewerten zu können, ist es zunächst hilfreich, sich der zugrundeliegenden Modellannahmen bewusst zu werden. Ein Modell ist in diesem Zusammenhang eine Abstraktion der relevanten Systemumgebung. Die gewählte Abstraktionstiefe hat einen direkten Einfluss auf die Qualität der nachfolgenden Sicherheitsaussage: Spielen Speicherkapazitäten eine Rolle? Werden Annahmen über die Netzwerklatenz gemacht?

Teil des Modells ist auch der angenommene Angreifer. Kann er beispielsweise das Netzwerk abhören oder sogar aktiv eingreifen? Kann er Parteien korrumpieren oder Signaturen fälschen? Gibt es einen zentralen Vertrauensanker oder kann potentiell jede Entität eines Systems als Angreifer auftreten?

Hat man sich auf ein Modell festgelegt, können die Mechanismen und Struktureigenschaften des Systems formuliert werden. Die genaue Formulierung der Mechanismen hängt dabei von der Wahl des Modells ab. Ist beispielsweise das Verstreichen von Zeit nicht modelliert, ist es nicht möglich, Zeitüberschreitungen (Timeouts) festzulegen.

Aus dem Modell und der Architekturbeschreibung können nun Sicherheitsaussagen abgeleitet werden. Zum Beispiel also:

1 Tim Kanning, FAZ. Der nächste große Umbruch in der Finanzwelt rückt näher. http://www.faz.net/aktuell/finanzen/digital-bezahlen/finanzwelt-testet-blockchain-fuer-transaktionen-14945304.html. Abgerufen am 25.8.2017.

2 Kai Schwirzke, heise online. Blockchain-Technik: Musikwirtschaft sucht Auswege aus der Datenflut. https://www.heise.de/newsticker/meldung/Blockchain-Technik-Musikwirtschaft-sucht-Auswege-aus-der-Datenflut-3310684.html. Abgerufen am 25.8.2017.

3 Ralph Diermann, Süddeutsche Zeitung. Wie Blockchain-Technik das Energiesystem revolutionieren kann. http://www.sueddeutsche.de/wissen/energie-wie-blockchain-technik-das-energiesystem-revolutionieren-kann-1.3117309. Abgerufen am 25.8.2017.

„Wenn ein Angreifer nur eine Minderheit aller Teilnehmer korrumpieren und Nachrichten im Netzwerk weder verzögern noch unterbinden kann, kann er keine Transaktionen ehrlicher Teilnehmer unterdrücken."

An dieser Stelle ist zu betonen, dass Sicherheitsgarantien grundsätzlich nur im gewählten Modell zu bewerten sind. Ändert sich das Modell, ändern sich die Sicherheitsgarantien, die eine Architektur liefert. Je präziser und vollständiger Modell und Mechanismen formuliert sind, umso genauere Sicherheitsaussagen können getroffen werden.

3 Die Bitcoin-Blockchain

Die Blockchain-Technologie erlangte zuerst Bekanntheit über die kryptographische Währung „Bitcoin".[4] Wenn man über Sicherheitsmechanismen und Sicherheitsgarantien der Blockchain redet, meint man in der Regel die Blockchain, wie sie von Bitcoin benutzt wird. Im Folgenden werden daher die wichtigsten Entwurfsziele von Bitcoin genannt und es wird erklärt, welche Mechanismen der Blockchain zusammen mit welchen Annahmen diese Ziele erreichen.

Das Blockchain-Netzwerk besteht aus einer Menge unabhängiger Teilnehmer, die miteinander über „Rundrufe" (*broadcasts*) kommunizieren. Wesentliche Entwurfsmerkmale der Blockchain-Technologie sind der Verzicht auf zentrale Instanzen, ein Konsensmechanismus und die Unveränderbarkeit der Blockchain.

Im Folgenden werden die wesentlichen Ziele der Bitcoin-Blockchain skizziert:

3.1 Nachvollziehbarkeit

Nachvollziehbarkeit wird in Bitcoin dadurch erreicht, dass alle Bezahlvorgänge als eine *Transaktion* eines gewissen Betrags zwischen einem Sender und einem Empfänger organisiert werden. Diese Transaktionen werden zunächst in Blöcken zusammengefasst und anschließend an alle Teilnehmer des Bezahlsystems übermittelt. Jeder Teilnehmer speichert diese Blöcke lokal in einer stetig wachsenden Liste. Da jeder Teilnehmer über die vollständige Transaktionsliste verfügt, ist die Korrektheit jeder einzelnen Transaktion nachvollziehbar.

3.2 Non-Repudiation

Während es in konventionellen Währungen unmöglich ist, das (Bar-)Geld einer fremden Person auszugeben, ist es in einem System, in dem Zahlungen nur als eine elektronische Transaktion repräsentiert sind, durchaus denkbar, dass Transaktionen in fremdem Namen verfasst werden. Bitcoin löst dieses Problem dadurch, dass alle Transaktionen von dem Sender kryptographisch signiert werden. Teilnehmer werden durch ihren öffentlichen Schlüssel identifiziert. Unter der Annahme, dass kein Angreifer Signaturen fälschen kann, können Teilnehmer nur über Geld verfügen, das sie selbst in Form von Transaktionen erhalten haben.

3.3 Konsistenz

In konventionellen Bezahlsystemen autorisieren Banken als zentrale Institutionen Transaktionen und wachen so darüber, dass ein Kontoinhaber nur das Geld ausgeben kann, über das er verfügt. In einem dezentralen System können Teilnehmer Geld mehrfach ausgeben („*double spending*"), wenn Transaktionen nicht überprüft werden. Um Transaktionen zu autorisieren, prüft sie ein (beliebiger) Teilnehmer auf Richtigkeit und fasst mehrere Transaktionen in einem Block zusammen. Zusätzlich enthält ein bestätigter Block immer die eindeutige Information darüber, welcher Block der Vorgängerblock war – also auf der Basis welchen „Kontostands" aller Teilnehmer die in dem Block enthaltenen Transaktionen bestätigt wurden. Um einen solchen Block in die Blockchain eintragen zu können, muss der Teilnehmer außerdem eine signifikante Menge von Rechenleistung aufbringen und den Beleg dafür – den *Proof of Work* – an den Block anfügen.

Der Proof of Work bedingt zweierlei. Zum Ersten ist das Erstellen von Blöcken an die Investition von Rechenzeit gebunden: Das Autorisieren von Transaktionen kostet Strom. Zum Zweiten „bremst" der Proof of Work die Erstellung neuer Blöcke: Kein Teilnehmer kann beliebig schnell neue Blöcke erzeugen. Nur dann, wenn ein Angreifer – oder ein Zusammenschluss mehrerer Angreifer – mehr als die Hälfte der gesamten Rechenleistung des Netzwerks kontrolliert, kann er frei diktieren, welche Transaktionen validiert werden und welche nicht. Ist eine Transaktion bereits eine gewisse Zeit in der Blockchain verewigt, ist es fast unmöglich, sie durch eine neue Transaktionsgeschichte zu überschreiben – solange der *Proof of Work* hinreichend „schwer" zu erbringen ist und solange ehrliche Teilnehmer die Mehrheit der Rechenleistung stellen.[5]

3.4 Eindeutigkeit

Da es jedem Teilnehmer prinzipiell möglich ist, einen neuen Block zu schaffen und es ihm freigestellt ist, welche Transaktionen er dazu berücksichtigt, kann es jederzeit dazu kommen, dass unterschiedliche Blöcke mit dem gleichen Vorgängerblock veröffentlicht werden – die Blockkette bekommt also einen neuen Strang. Um zu verhindern, dass der Zustand der Blockchain auf diese Weise divergiert, gilt die einfache Regel, dass neue Blöcke immer am aktuell längsten Strang der Blockchain angehängt werden müssen. Halten sich mehr als 50% aller Clients an dieses Prinzip, ist es einem Angreifer nicht möglich, einen neuen (bösartigen) Strang in der Blockchain zu erzeugen, der von anderen Teilnehmern anerkannt wird.

3.5 Ausgeglichenheit

Das bisher beschriebene System bietet für Teilnehmer keinen Anreiz, sich an der Verifizierung von Blöcken zu beteiligen. Der *Proof of Work* erfordert die Investition von Rechenzeit, die sich nicht lohnt, wenn man nicht eine selbstgemachte Transaktion bestätigt wissen will. Um dieses Problem zu lösen, erhalten Teilnehmer nach der Bestätigung eines Blocks eine Belohnung in Form neu geschaffener („abgebauter") Bitcoins. Zusätzlich ist es dem Sender ebenfalls möglich, für die Bestätigung seiner Transaktion eine Belohnung zu vergeben.

4 Dirk Fox. „Bitcoin". Gateway, Datenschutz und Datensicherheit-DuD 41.8 (2017): 507.

5 Unter bestimmten Voraussetzungen genügt eine ehrliche Mehrheit nicht: Ittay Eyal and Emin Gün Sirer. „Majority is not enough: Bitcoin mining is vulnerable." International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2014.

4 Die Blockchain als Basistechnologie für andere Anwendungen

Bei Bitcoin werden Transaktionen in der Blockchain gespeichert. Grundsätzlich ist die Technologie hinter Bitcoin jedoch dazu geeignet, nahezu beliebige Daten zu speichern, solange ein Mechanismus existiert, nach dem Teilnehmer beurteilen können, ob ein Eintrag korrekt ist und validiert werden kann. Anwendungen, die sich diese Eigenschaft zu Nutze machen, sind vielfältig: Namensserver für ein *Domain Name System*[6], E-Mail[7] oder Grundbucheinträge[8].

Die virtuelle Währung Ethereum[9] geht noch einen Schritt weiter und erlaubt es, sogenannte *Smart Contracts* in die Blockchain zu schreiben.[10] Ein *Smart Contract* ist in Ethereum ein Programm in einer speziellen Programmiersprache, das in der *Ethereum Virtual Machine* ausgeführt wird und selbst wieder Einfluss auf die Blockchain nehmen kann.[11]

4.1 Der DAO-Vorfall

Erlaubt man das Beschreiben und die automatische Ausführung von Verträgen in einer Programmiersprache, erbt man den Segen frei programmierbarer Systeme, aber auch deren Fluch: Die Verifikation von Computerprogrammen ist bis heute Forschungsgegenstand.[12] Generell ist bei Programmen nicht zwischen beabsichtigtem und unbeabsichtigtem (oder gar bösartigem) Verhalten zu unterscheiden, solange keine Spezifikation vorliegt und der Code dahingehend verifiziert wird. Selbst für menschliche Experten ist das Auffinden von Fehlern in Programmcode sehr schwer.[13]

Die „dezentrale autonome Organisation" *The DAO* war eine dezentral organisierte Investmentfirma, die ihre Investmententscheidungen ausschließlich durch die Auswertung eines *Smart Contracts* in der Ethereum-Blockchain traf. Teilnehmer, die mit einer Investmententscheidung der DAO nicht einverstanden waren, konnten ihr Investment wieder abziehen. Aufgrund einer Sicherheitslücke im Code der DAO war es einem Angreifer möglich, nicht nur seine eigenen Anteile an der DAO zurückzuholen, sondern beliebig viel Geld zu transferieren. Auf diese Weise gelang es ihm, 53 Millionen Dollar Kapital zu veruntreuen.[14] Die Ethereum-Entwickler entscheiden sich daraufhin, über ein Software-Update einen „Hard Fork" der Blockchain durchzuführen, der den Angriff ungeschehen machen sollte. Damit so ein Vorgehen erfolgreich ist, muss sich die Mehrheit der Teilnehmer dazu entschließen, einen neuen Strang der Blockchain als korrekt zu akzeptieren. Dieser Konsens stellt jedoch die Sicherheitsannahme der bedingungslosen Integrität der Blockchain grundlegend infrage: Die Verbindlichkeit der Blockchain ist keine kryptographische Garantie, sondern Gegenstand öffentlicher Debatte.

5 Die Probleme der Blockchain und potentielle Lösungen

Für die Erstellung eines *Proof of Work*, der die Grundlage der Sicherheit des Bitcoin-Netzwerks darstellt, muss eine große Menge elektrischer Arbeit aufgewendet werden. Konservative Schätzungen gehen davon aus, dass jede Transaktion mindestens 26 kWh elektrischer Arbeit verbraucht.[15] Aktuell liegt der geschätzte Gesamtenergieverbrauch der Bitcoin-Blockchain bei 16 TWh pro Jahr.[16]

Zusätzlich ist der *Proof of Work* auch dafür verantwortlich, dass es sehr lange dauert, bis eine Transaktion in die Blockchain eingetragen wird. Aktuell beträgt die maximale Transaktionsgeschwindigkeit in Bitcoin sieben Transaktionen pro Sekunde. Die durchschnittliche Wartezeit, bis eine Transaktion von dem Netzwerk bestätigt wird, hängt von der aktuellen Nutzung des Netzwerks ab und kann zwischen 22 Minuten (Juni 2016 bis November 2016) und 300 Minuten (Juni 2017 bis Juli 2017) reichen.[17] Die Tatsache, dass alle Teilnehmer der Blockchain die vollständige Transaktionsliste speichern müssen, macht deren Größe ebenfalls zu einem Problem: Die Bitcoin-Blockchain ist im Moment 130 GB[18] groß, was für mobile Geräte aktuell eine nicht zu bewältigende Datenmenge und selbst für normale Desktop-Computer eine Herausforderung darstellt. Die Verwendung von *Thin Clients*, die die Blockchain nur nutzen, aber selbst keine Validierung vornehmen, ist zwar grundsätzlich möglich, jedoch sinkt die Sicherheit der Blockchain mit der Anzahl der *Thin Clients*.

5.1 Der „Proof of Stake"

Ein alternativer Mechanismus zur Validierung von Blöcken, der neuerdings in viele Blockchain-Varianten Einzug hält (z. B. in Ethereum[19]), ist der sogenannte *Proof of Stake*. Die Idee dabei ist, dass Clients zum Erstellen von Blöcken keinen Beweis ihrer investierten Rechenzeit mehr brauchen. Stattdessen gibt es eine festgelegte Gruppe von autorisierten Clients, die Blöcke validieren dürfen. Jeder hat die Möglichkeit, dieser Gruppe beizutreten, indem er einen Teil seines Guthabens in einen dafür vorgesehenen Account einzahlt, aus dem er es erst nach einem längeren Zeitraum wieder abrufen kann. Das System wählt nun zufällig einen Teilnehmer aus dieser Gruppe und erlaubt ihm, einen neuen Block zu erzeugen – ohne *Proof of Work*. Die Auswahl wird dabei nach der Höhe des eingezahlten Guthabens gewichtet. Clients, die einen

6 Namecoin, https://namecoin.org/

7 Martin Grottenthaler und Jürgen Fuß. „MailCoin." Datenschutz und Datensicherheit-DuD 41.8 (2017): 487-491.

8 Joon Ian Wong, Quartz. "Sweden's blockchain-powered land registry is inching towards reality." https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/. Abgerufen am 25.8.2017.

9 https://www.ethereum.org/

10 Siehe auch Christian Sillaber, Bernhard Waltl. „Life Cycle of Smart Contracts in Blockchain Ecosystems." Datenschutz und Datensicherheit-DuD 41.8 (2017): 497-500.

11 Vgl. die Dokumentation zur Sprache Solidity: https://solidity.readthedocs.io/en/develop/. Angerufen am 24.8.2017.

12 Bhargavan, Karthikeyan, et al. "Short Paper: Formal Verification of Smart Contracts." https://www.cs.umd.edu/~aseem/solidetherplas.pdf

13 Der *Underhanded C Contest* macht das Verstecken von Fehlern in Code zu einem Spiel: http://www.underhanded-c.org/

14 Max Biederbeck, WIRED.de: Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen. https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde. Abgerufen am 24.8.2017.

15 Christopher Malmo, VICE Motherboard: https://motherboard.vice.com/en_us/article/ypkp3y/bitcoin-is-still-unsustainable. Abgerufen am 25.8.2017.

16 Bitcoin Energy Consumption Index: https://digiconomist.net/bitcoin-energy-consumption. Abgerufen am 21.8.2017.

17 Blockchain.info, Average Confirmation Time. https://blockchain.info/de/charts/avg-confirmation-time?timespan=2years&daysAverageString=7. Abgerufen am 25.8.2017.

18 Blockchain.info, Blockchain Size. https://blockchain.info/de/charts/blocks-size. Abgerufen am 25.8.2017.

19 Philipp Giese, BTC-ECHO. Proof of Stake dank Casper: die Zukunft vom Ethereum. https://www.btc-echo.de/proof-of-stake-dank-casper-die-zukunft-vom-ethereum/. Abgerufen am 25.8.2017.

Block an einen Strang der Blockchain anhängen, der nicht weitergeführt wird, werden bestraft: Sie verlieren einen Teil des eingezahlten Geldes. Dadurch soll wie beim *Proof of Work* sichergestellt werden, dass sich die längste Kette immer durchsetzt. Trotz verändertem Sicherheitsmechanismus werden Blockchains, die einen *Proof of Stake* einsetzen, häufig die gleichen Sicherheitseigenschaften zugesprochen, die auch Bitcoin besitzt. Die genaue Beurteilung der Sicherheitseigenschaften gestaltet sich jedoch für beide Sicherheitsmechanismen als sehr schwierig. Ob der *Proof of Stake* tatsächlich bessere (oder gar schlechtere) Sicherheitseigenschaften besitzt, ist noch Gegenstand einer Debatte in der Blockchain-Community[20, 21]. Der Grund dafür ist, dass die durch *Proof of Work* und *Proof of Stake* erreichten Sicherheitseigenschaften auf ökonomischen Annahmen beruhen. Zum einen soll es für einen Angreifer (finanziell) nicht möglich sein, mehr als 50% der Rechenleistung des Netzwerks auf sich zu vereinigen und zum anderen soll Fehlverhalten (z. B. das Anhängen von Blöcken an einen falschen Strang der Kette) ökonomisch nicht sinnvoll sein. Diese Annahmen unterscheiden sich grundlegend von den Annahmen, die bei konventionellen Sicherheitsmechanismen gemacht werden, was die Beurteilung von deren Korrektheit schwierig macht.

5.2 Kryptographische Sicherheitsannahmen versus Cryptoeconomics

Um verlässliche Aussagen über die Sicherheit der Blockchain machen zu können, müssen zwei grundverschiedene Disziplinen vereint werden: Kryptographie und Ökonomie. Ökonomische Überlegungen bilden nun die Grundlage kryptographischer Sicherheitsannahmen und -garantien. Sicherheitsmechanismen werden aufgrund spieltheoretischer Überlegungen entworfen und haben zum Ziel, Angriffe und Manipulationen unwirtschaftlich zu machen. In der Community wird vom Feld der Krypto-Ökonomie („*cryptoeconomics*") gesprochen.[22]

Wirtschaftliche Anreizsysteme zu nutzen, um Menschen zu einem Verhalten zu motivieren, ist keine neue Idee. Das Mining bei Bitcoin selbst stellt einen solchen Anreizmechanismus dar. Dadurch, dass Teilnehmer für das Erstellen von Blöcken belohnt werden, besteht ein finanzieller Anreiz dazu. Ohne diesen Anreiz würden nur Altruisten Transaktionen verifizieren. Der (oder die) pseudonyme Schöpfer (in) von Bitcoin, Satoshi Nakamoto, schreibt: „[A greedy attacker] ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."[23]

Im Gegensatz dazu basiert die Sicherheit von vielen konventionellen kryptographischen Sicherheitsmechanismen, wie beispielsweise von Verschlüsselungsverfahren, auf der Schwierigkeit eines algorithmischen Problems. Nimmt man an, dass solch ein Problem schwierig zu lösen ist, kann man nachweisen, dass das darauf basierende Verschlüsselungsverfahren nur mit erheblichem Rechenaufwand zu knacken ist. Das Problem wird durch den Einsatz von mehr Rechenleistung nicht leichter – man kann mögliche Schlüssel der Verschlüsselung nur schneller durchprobieren. Durch Erhöhen der Schlüssellänge kann man die Zeit, die solche Angriffe benötigen, drastisch erhöhen, ohne die Nutzer des Systems in ebenso starkem Maß einzuschränken.

Bei ökonomischen Sicherheitseigenschaften ist das anders. Zwar lässt sich die Schwierigkeit des *Proof of Work* erhöhen, um es für Angreifer teurer zu machen, den Großteil der gesamten Rechenleistung des Netzwerks zu stellen. Das beeinträchtigt jedoch auch unmittelbar die ehrlichen Benutzer der Blockchain, und damit deren Anteil.

Darüber hinaus könnte es eine Fehlannahme sein, dass die Mehrheit der Teilnehmer ausschließlich ökonomisch motiviert handelt. Für einen Angreifer, dem vor allem daran gelegen ist, das System zu stören, ist es möglicherweise bedeutungslos, wenn er dabei einen großen wirtschaftlichen Verlust erleidet.

Schließlich kann die Blockchain nicht als wirtschaftlich geschlossenes System betrachtet werden. Das ist insbesondere dann der Fall, wenn in der Blockchain nicht Währungen gehandelt werden, sondern Güter der realen Welt. Der Wert der Blockchain-internen Währung (wie z. B. BTC oder ETH) ist von dem Wechselkurs in eine „reale Währung" abhängig. Dieser Kurs steht in unmittelbarem Zusammenhang zu der Anzahl der Teilnehmer des Systems. Je mehr Geld sich mit der Validierung von Blöcken verdienen lässt, desto mehr Leute sind bereit, die dafür notwendige Rechenleistung zu investieren. Wäre es von heute auf morgen unmöglich, Bitcoins in Dollar zu tauschen, ist es fraglich, ob die Bitcoin-Blockchain weiter existieren würde. Dieser Zusammenhang wirkt sich auch auf die Sicherheit des Systems aus: Verliert eine *Proof-of-Stake*-Währung an Wert, wird es einfacher, einen großen Teil des Stakes zu erwerben. Gewinnt sie an Wert, erhalten Teilnehmer, die früh einsteigen, größere Anteile für den gleichen Einsatz.

Durch die Verwendung von ökonomischen Mechanismen wird die Sicherheit von Blockchains abhängig von vielen komplexen, äußeren Einflussfaktoren und kann nicht mehr isoliert betrachtet werden. Ein kryptographischer Sicherheitsnachweis auf der Basis präzise formulierter und wohluntersuchter Annahmen, den man von traditionellen Sicherheitsmechanismen erwartet, ist so nahezu unmöglich zu erbringen.

5.3 Mehr Kontrolle über die Blockchain durch Berechtigungsmanagement

Die Blockchain-Technologie wird heutzutage als Lösung für eine Vielzahl von Problemen beworben. Die Reichweite ist dabei von der Absicherung von Atomwaffen[24] bis zu der Realisierung eines digitalen Grundbuchs[25]. Bitcoin ist jedoch eine „public" und „permissionless" Blockchain. Das bedeutet, dass jedermann Zugriff auf die in der Blockchain gespeicherten Informationen hat und auch jedermann neue Transaktionen hinzufügen und validieren kann. Diese Eigenschaften sind für bestimmte Anwendungsfälle jedoch ungewünscht. Verwaltete man beispielsweise die Standorte von Atomwaffen in einer Blockchain, würde man nicht wollen, dass jedermann diese Informationen abrufen kann („private"). Ebenso möchte man im Fall des digitalen Grundbuchs nicht,

20 Ethereum Proof of Stake FAQ. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ. Abgerufen am 25.8.2017.

21 Paul Sztorc. Mining – Threat Model and Equilibrium Analysis. http://www.truthcoin.info/blog/mining-threat-equilibrium/. Abgerufen am 25.8.2017.

22 Nick Tomaino. Cryptoeconomics 101. https://thecontrol.co/cryptoeconomics-101-e5c883e9a8ff. Abgerufen am 24.08.2017.

23 Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. (2008).

24 Stefan Krempl, heise online. Pentagon-Forschungsarm will mit der Blockchain Militärsysteme absichern. https://www.heise.de/security/meldung/Pentagon-Forschungsarm-will-mit-der-Blockchain-Militaersysteme-absichern-3349197.html. Abgerufen am 25.8.2017.

25 Siehe oben.

dass jeder, der das Grundbuch lesen darf, auch Grundbucheinträge vornehmen kann („permissioned").

Um die Blockchain auch in diesen Anwendungsfällen einsetzbar zu machen, wird versucht, die Technologie um ein Berechtigungsmanagement zu erweitern – mit dem Zweck, feingranular einschränken können, wer Zugriff auf die Blockchain hat, wer Blöcke validieren und wer Transaktionen eintragen darf. Selbst zwei Realisierungen der Blockchain, die beide einen *Proof of Work* verwenden, funktionieren also nicht notwendigerweise gleich. Bei der Entwicklung von neuen und bei der Nutzung von bereits existierenden Blockchain-Anwendungen muss sorgfältig geprüft werden, welches Berechtigungsmodell sinnvoll ist. Bei der Umsetzung der Zugriffseinschränkung ist allerdings Vorsicht geboten: wird diese über einen zentralen Dienst realisiert, kann das die dezentrale Architektur und die Sicherheitseigenschaften des Gesamtsystems in Frage stellen.

5.4 Durchführen von Transaktionen „Off-Chain"

Die Transaktionsgeschwindigkeit einer auf einem *Proof of Work* basierten Blockchain ist für viele Anwendungen nicht ausreichend. Im Bitcoin-Umfeld haben sich daher Dienstleister gebildet, die bestimmte Transaktionen außerhalb der Blockchain durchführen („Off-Chain"). Beispielsweise bietet Coinbase[26], ein Anbieter für den Wechsel von digitalen Währungen in Fiat-Währungen, die Möglichkeit, Transaktionen zwischen zwei bei ihm registrierten Bitcoin-Nutzern außerhalb der Blochchain abzuwickeln. Coinbase schlüpft hier also in die Rolle eines Finanzdienstleisters, ähnlich wie Paypal.

Die wesentliche Errungenschaft der Blockchain ist jedoch die Gewährleistung von Funktionalität und Sicherheit ohne eine zentrale Vertrauensstelle. Bei dem Entwurf eines Systems stellt sich immer zunächst die Frage, welche Vertrauensbeziehungen zwischen dem Nutzer eines Dienstes und den weiteren beteiligten Entitäten (z. B. den Dienstanbietern) bestehen. Viele der heutigen Dienste im Internet (wie beispielsweise Paypal) sind so konzipiert, dass vollständiges Vertrauen in eine zentrale Instanz vorausgesetzt wird. Die zentrale Instanz ist hier entweder der Dienstanbieter selbst oder aber eine vertrauenswürdige dritte Partei („*trusted third party*", kurz *TTP*), die als zentraler Vertrauensanker fungiert.

Die Nutzung einer TTP hat sich in der Praxis jedoch als problematisch erwiesen. So ist es in einer globalisierten Welt kaum praktikabel, dass ein einzelnes Unternehmen oder eine einzelne Organisation das vollständige Vertrauen aller Nutzer weltweit genießt. In der Realität kann somit lediglich von partiellem Vertrauen in die Entitäten eines Systems ausgegangen werden. Dies gilt insbesondere, wenn in Betracht gezogen wird, dass einzelne Entitäten von einem Angreifer korrumpiert werden können.

Die Forschung beschäftigt sich schon seit Jahrzehnten mit Verfahren, die das absichtliche Fehlverhalten einer Reihe von Teilnehmern eines Systems tolerieren können („*Byzantine Fault Tolerance*", kurz BFT).[27] Solche BFT-Protokolle haben jedoch einen hohen Kommunikationsaufwand und skalieren schlecht bezüglich der Anzahl an Teilnehmern. Aufgrund dessen konnten sich BFT-Protokolle somit lange Zeit in der Praxis nicht durchsetzen. Zudem sind sogenannte Sybil-Angriffe möglich, bei denen ein Angreifer unter mehreren Identitäten auftritt und dadurch Verfahren wie z. B. Mehrheitsentscheide zu seinen Gunsten beeinflusst kann. Mit der Bitcoin-Blockchain wurde erstmals eine praxistaugliche Technologie entwickelt, die alle diese Probleme adressierte.

Nutzt man Dienstleister wie Coinbase um Off-Chain-Transaktionen durchzuführen, gibt man die Vorteile des dezentralen Blockchain-Systems auf und muss erneut einer zentralen Instanz vertrauen. Wenn eine solche zentrale Vertrauensinstanz jedoch existiert, stellt sich unmittelbar die Frage, wieso das System überhaupt dezentral entworfen wurde und ob diese Instanz nicht das komplette System bereitstellen kann. Insbesondere weisen dezentrale Systeme durch den Verzicht auf zentrale Instanzen eine erhöhte Komplexität auf und erfordern aufwändige Verfahren zur Selbstorganisation. Das führt dazu, dass diese Verfahren hinsichtlich der Skalierbarkeit in Bezug auf die Anzahl an Teilnehmern, die Anzahl an Transaktionen sowie die Größe der abgelegten Daten klassischen verteilten Datenbanken (mit zentralem Vertrauensanker) deutlich unterlegen sind.

6 Fazit

Die aktuell weit verbreitete Begeisterung für Anwendungen der Blockchain ist grundsätzlich sehr positiv zu bewerten. Die Blockchain-Technologie ist zweifellos ein hochinnovatives, zukunftsträchtiges Konzept. Sie hat das Potential, in einigen Bereichen einen technologischen Umbruch zu bewirken.

Bei der Verwendung der Technologie ist jedoch Vorsicht geboten. Zunächst muss geklärt werden, ob die Verwendung der Blockchain sinnvoll ist. Existiert eine zentrale Instanz, oder macht das Einführen eines Berechtigungsmanagements eine solche notwendig, ist der Einsatz eines dezentralen Systems nicht immer sinnvoll. Möchte man ein dezentrales System entwerfen, das nur gegen Ausfall gesichert werden muss, stellen moderne verteilte Datenbanksysteme[28] eine signifikant effizientere Lösung zur Datenablage dar.

Die Sicherheitsannahmen vieler Blockchain-Mechanismen basieren auf ökonomischen Überlegungen, die sich von klassischen Sicherheitsannahmen unterscheiden. Für den Einsatz in einer sicherheitskritischen Anwendung muss daher sorgfältig geprüft werden, ob diese Annahmen in der konkreten Situation zutreffen – insbesondere, wenn die Anwendung kein geschlossenes System darstellt. Die Blockchain ist keine Universaltechnologie. Ihr Einsatz und ihre Ausprägung muss für den jeweiligen Anwendungsfall sorgfältig abgewogen werden.

Die Weiterentwicklung der ursprünglichen Idee hinter der Blockchain-Technologie steckt noch in den Anfängen. Damit zukünftige Anwendungen auf der Basis neuartiger Blockchain-Konzepte sicher umgesetzt werden können, lohnt sich die Investition nicht nur in die interdisziplinäre Erforschung von Anwendungen der Blockchain, sondern auch ihrer Grundlagen.

Dank

Die Autoren danken: Ard Kastrati für die Eingebung zu einer systematischen Herleitung der Designziele der Blockchain und allen Teilnehmern des TeleTrusT-Informationstags „Blockchain" für die Inspiration zu diesem Beitrag.

26 https://www.coinbase.com/?locale=de

27 Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401.

28 Ggf. auch zur Erhöhung der Verfügbarkeit und Performanz als verteilte Datenbank auf mehreren Rechnern.