Digitales Vertrauen

Nachhaltige Blockchains

Der rasante Aufstieg von Bitcoin hat viele Problemstellungen zum verteilten Vertrauensmanagement, dem Energieverbrauch und dem Schutz der Privatsphäre von interessanten Forschungsfragen zu wichtigen Herausforderungen für nachhaltige wirtschaftliche und gesellschaftliche Entwicklung werden lassen.

Von Rüdiger Weis

Eine Blockchain besteht technisch betrachtet aus einer verketteten Liste von Blöcken mit Hash-Zeigern und gehört zu den einfachsten Datenstrukturen der Informatik. Hashfunktionen sind Verfahren, welche kurze Prüfsummen für Daten berechnen. Sie sind zentrale und gründlich untersuchte Bausteine in allen in der Praxis weitverbreiteten Signaturprotokollen. Die grundlegenden Methoden zur Erzeugung einer kryptografisch gesicherten Buchführung wurden in der Forschung schon seit vielen Jahrzehnten diskutiert (Merkle 1990, Haber/Stornetta 1991, Anderson 1996, Donnerhacke 1997).

Große Beachtung gewannen Blockchains, nachdem mit Bitcoin eine kryptografische Währung erschaffen wurde, welche die hashverkettete Liste mit Verfahren der verteilten Datenbanktechnik kombinierte.

Bitcoin, welches grundlegend auf einem öffentlich verteilt gespeicherten, gegen Veränderung gesicherten Transaktionsbuch beruht, generiert konstruktionsbedingt völlig neue Herausforderungen bezüglich des Schutzes der Privatsphäre. Konstruktionsbedingt ist ein „Recht auf Vergessen" in Blockchain basierten Systemen zunächst nicht möglich.

Innerhalb Bitcoin hat jede private oder juristische Person Zugriff auf die gesamten Transaktionsdaten. Dies ist im Vergleich zu normalen Bankdaten, auf die nur nach klar definierten Grundlagen von staatlichen Stellen zugegriffen werden darf, eine signifikante Verschlechterung hinsichtlich des Schutzes gegenüber rechtswidrigen Angriffen von Geheimdiensten und Kriminellen.

Bitcoin versucht, durch die Verwendung von Pseudonymen einige der Datenschutzprobleme zu adressieren. Moderne Analysetechniken mithilfe von recht einfacher Graphentheorie reduzieren jedoch in beträchtlichem Ausmaß den Schutz durch pseudonyme Konten. Es gibt bereits mehrere Firmen auf dem Markt, die das Durchleuchten von Bitcoin-Flüssen als Dienstleistung anbieten. Auch alternative Systeme, die einen erweiterten Schutz der Privatsphäre bieten, sind gegen derartige Analysemethoden nicht vollständig abgesichert.

Ohne Pseudonyme wäre Bitcoin aus datenschutzrechtlicher Perspektive ein Alptraum, aber selbst mit Pseudonymen ist es immer noch äußerst problematisch. Hier besteht ein starker Forschungs- und Entwicklungsbedarf.

Herausforderungen aktueller Konsensverfahren

Spannende Herausforderungen bestehen darin, sich in einem Netzwerk von gleichberechtigten Rechnern auf einen gemeinsamen Konsens über den Zustand der Blockchain zu einigen. Hierzu gibt es verschiedene Vorschläge. Am weitesten verbreitet und wegen des großen Energieverbrauchs am meisten kritisiert sind sogenannte Prove-of-Work-Protokolle, mit denen auch innerhalb eines sogenannten Miningprozesses neue Währungseinheiten generiert werden.

Die Ursprungsidee von Bitcoin war ein demokratisches System, in dem alle teilnehmenden Rechner jeweils eine Stimme haben. Einige zu wenig durchdachte Designentscheidungen führten jedoch dazu, dass sich inzwischen eine starke Zentralisierung herausgebildet hat. Die Kontrolle über die Blockchains konzentriert sich in der Praxis auf wenige Mining-Pools. Dies widerspricht nicht nur der Grundidee der Dezentralisierung, es bringt auch einige gewichtige praktische Probleme mit sich.

Bei der zugrunde liegenden Funktion für das Mining neuer Bitcoin handelt es sich um die kryptografische Hashfunktion Secure-Hash-Algorithm SHA-256. Diese Hashfunktion wurde gezielt in einer Form entworfen, die eine möglichst einfache Hardwarerealisierung ermöglicht. Dies führt dazu, dass diejenigen, die die bessere Hardware und billigeren Strom nutzen können, den Markt kontrollieren. Hätte man hier die aktuelle kryptografische Forschung verfolgt, hätte diese problematische Entwicklung zumindest abgebremst werden können.

Die kryptografische Forschung hat sich im Zusammenhang mit Password-Hashing schon sehr lange damit beschäftigt, Funktionen zu entwickeln, welche möglichst schlecht auf Spezialhardware zu realisieren sind. Viele alternative Kryptowährungssysteme verwenden derartige Verfahren, zum Teil allerdings nicht mit ausreichend sicheren Parametern.

Interessant im Sinne der Nachhaltigkeit ist, dass im Zuge der Hardwareentwicklung für Mining-Berechnungen viel Aufwand für eine energiesparende Implementierung der benötigten Verfahren betrieben wurde. Es gibt Überlegungen, alterna-

*Ökologisches*Wirtschaften 4.2018 (33) | DOI 10.14512/OEW330427

„Die Möglichkeit, mittels Blockchain-Technologien digitale Vertrauensstrukturen aufzubauen, schafft interessante Perspektiven für sich entwickelnde Volkswirtschaften."

tive Miningverfahren vorzuschlagen, welche als Nebenaspekt eine energieeffizientere Implementierung von auch anderweitig benötigten Verfahren mit sich bringen könnten.

Nachhaltiges Mining

Wünschenswert wäre ein Mining, welches mit sozial nützlichen Beiträgen arbeitet, anstatt der bei Bitcoin verwendeten Berechnung von Zufallsfunktionen, welche außer der Sicherung des Mininigprozesses keine nützlichen Ergebnisse mit sich bringen. Andere Systeme, welche beispielsweise das sichere verteilte Speichern von Dateien belohnen (Prove-of-Space), liefern direkt einen interessanten Mehrwert. Die momentan stark diskutierten Prove-of-Stake-Ansätze wiederum vermeiden oder reduzieren zumindest im Fall von hybriden Verfahren den problematischen Energieverbrauch.

Am einfachsten integrierbar in bestehende Systeme wären Lösungen, welche zwar weiterhin auf einem Prove-of-Work-Ansatz beruhen, die Rechenzeit allerdings für nützliche Probleme nutzen. Hier bieten sich Fragestellung an, welche als Beispielprobleme für verteiltes Rechnen seit Längerem benutzt werden, wie die Berechnung von Proteinfaltungen. Diese aufwendigen Berechnungen sind notwendig, um Heilungsmethoden zu bestimmten Krankheiten zu entwickeln (Folding@home, 2000). Das Suchen von Cunningham-Ketten – also bestimmten Folgen von Primzahlen, die interessant für mathematische Forschung sind – wurde innerhalb von Primecoin genutzt (Primecoin 2013). Neben der guten verteilten Berechenbarkeit bilden auch die Anforderungen an ein sicheres und faires Mining ein weites Feld für zukünftige Forschungen.

Vielversprechende Ansätze sind sogenannte Proof-of-Space-Verfahren. Hierbei wird das Speichern von Daten anstatt der Berechnung von Zufallsfunktionen belohnt. Ein interessanter Vorschlag in diesem Kontext ist Permacoin (Miller et al. 2014). Ein Initial Coin Offering (ICO) im niedrigen dreistelligen Millionenbereich gelang Filecoin im August 2017 (Filecoin, 2014).

Ein fundamentaler Ansatz, den Energieverbrauch von Kryptowährungen drastisch zu reduzieren, ist ein Wechsel von Prove-of-Work-Systemen zu Prove-of-Stake-Systemen. Bei der Verwendung von Prove-of-Stake-Systemen entstehen jedoch völlig andere Währungseigenschaften. Interessante Ideen finden sich in der Ethereum Community mit dem hybriden Ansatz namens Casper (Buterin/Gruffith, 2017).

Mining und erneuerbare Energiequellen

Die Eigenschaft, dass die benötigte Energie für das Mining über längere Zeitabschnitte nicht so stark schwankt wie der normale Energieverbrauch von Volkswirtschaften, bietet interessante Möglichkeiten für die Verwendung einiger regenerativen Energiequellen. Sonnen- und Windenergie haben die Eigenschaft, dass sie stark schwankende Einspeisungen generieren. Zudem befinden sich häufig zur Energiegewinnung günstige Orte weit entfernt von den Hauptabnehmern. Sowohl Transport als auch Speicherung von größeren Strommengen führen zu nicht unerheblichen Energieverlusten. Die gerade innerhalb des Netzes nicht benötigte Energie direkt in Bitcoin umzusetzen, scheint eine spannende Idee zu sein.

Autonome Systeme könnten in sonnenreichen, infrastrukturarmen Gebieten eingesetzt werden, dort eigenständig mit Solarenergie betriebene Meshnetze aufbauen und mit dem Minen von kryptografischen Coins beginnen. Für die Teilnahme an einer Blockchain-Ökonomie reicht zunächst eine Außenverbindung mit dem GSM-Mobilfunkstandard oder über Satellitentelefon. Für das gesamte Meshnetz wird nur eine geringe Bandbreite benötigt. Die Rechnung für die mobile Verbindung könnte mit den aus Sonnenenergie gewonnenen Coins beglichen werden. Analog könnte bei einer späteren Anbindung an das konventionelle Stromnetz tagsüber Solarstrom eingespeist und für den nachts benötigten Strom die Rechnung mit kryptografischem Geld bezahlt werden.

Setzt man innerhalb des solarbetriebenen Blockchainsystems bei der Konsensfindung auf sozial nützliches Mining, etwa die Bereitstellung von Speicherplatz für Dateien, könnte dies eine Grundlage für ökologisch verantwortungsvoll realisierte und lokal kontrollierte Clouddienste darstellen.

Potenziale der Blockchain in sich entwickelnden Volkswirtschaften

Die Möglichkeit, mittels Blockchain-Technologien digitale Vertrauensstrukturen aufzubauen, welche nur geringe Anforderungen an die analoge Welt stellen, schafft interessante Perspektiven für sich entwickelnde Volkswirtschaften. In einigen Ländern Afrikas gibt es spannende Entwicklungen von mobiltelefonbasierten Bezahlungssystemen, besonders in Ländern mit nur gering entwickeltem Bankwesen. Auch wenn es in einigen Fällen zahlreiche Probleme im Bereich der Privatsphäre und den teilweise unakzeptabel hohen Transaktionsgebühren gibt, sehen viele sehr positive Entwicklungen. Blockchain-Lösungen, etwa im Bereich von Grundbucheintragungen, bieten Chancen für Volkswirtschaften mit noch schwach ausgeprägtem Notariatswesen, gleich mit einem modernen, digitalen Verwaltungswesen zu beginnen.

Schneller als andere Technologien haben sich Blockchain-basierte Systeme in den Wirtschaftsprozess eingegliedert. Der Schutz der Privatsphäre bei öffentlichen Blockchain-Systemen stellt neue Herausforderungen an den kryptografischen Schutz der Teilnehmenden. Ein Design basierend auf kryptografischem Halbwissen führt schnell zu einer Entdemokratisierung der grundlegenden Prozesse und einem starken Zuwachs des Energieverbrauches. Die Nutzung von regenerativen Energiequellen und die Möglichkeit, Vertrauenssysteme ohne staatliches Mitwirken zu erstellen, bietet schon aktuell interessante Perspektiven für nachhaltige Entwicklungen. Die kryptografische Forschung bietet darüber hinaus eine Reihe von Ideen, nachhaltigere Blockchain-Systeme zu entwickeln. Hilfreich wäre in jedem Falle ein stärker fächerübergreifender Dialog über Techniken zur Unterstützung Digitaler Souveränität (Weis 2016, Weis et al. 2017).

Literatur

Merkle, R. C. (1990): A certified digital signature. In: Lecture Notes in Computer Science – Crypto '89/435: 218–238.

Haber, S./Stornetta, W. S. (1991): How to Time-Stamp a Digital Document. In: Lecture Notes in Computer Science – Advances in Cryptology – Crypto '90/537: 437–455.

Anderson, R. J. (1996): The Eternity Service. In: In Proceedings of Pragocrypt '96.

Donnerhacke, L. (1997): Ewiges Logfile. Im Internet unter: http://altlasten.lutz.donnerhacke.de/mitarb/lutz/logfile/

Filecoin (2014): Filecoin. Im Internet unter: https://filecoin.io/filecoin-jul-2014.pdf

Folding@home (2000): Diseases. Im Internet unter: https://foldingathome.org/diseases/

Nakamoto, S. (2009): Bitcoin: A Peer-to-Peer Electronic Cash System. Im Internet unter: https://bitcoin.org/bitcoin.pdf

Miller, A./Juels, A./Shi, E./Parno, B./Katz, J. (2014): Permacoin: Repurposing bitcoin work for data preservation. In: Proceedings of the 2014 IEEE Symposium on Security and Privacy: 475–490.

Buterin, V./Gruffith, V. (2017): Casper the Friendly Finality Gadget. Im Internet: https://arxiv.org/pdf/1710.09437.pdf

Primecoin (2013): Primecoin. Im Internet unter: http://primecoin.io

Weis, R. (2016): Technische Sicherung der Digitalen Souveränität. In: Friedrichsen, M./Bisa, P.-J. (Hrsg.): Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft. Wiesbaden: Springer Fachmedien. 53–66.

Weis, R./Lucks, S./Grassmuck, V. (2017): Techniken für und wider Digitale Souveränität. Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen. ISSN 2365-843. Im Internet unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/Weis_Lucks_Grassmuck_Studie_.pdf

AUTOR + KONTAKT

Dr. Rüdiger Weis ist Professor für Informatik mit dem Schwerpunkt Systemprogrammierung an der Beuth-Hochschule in Berlin. Er ist seit 1997 regelmäßiger Vortragender auf dem Chaos Communication Congress des Chaos Computer Clubs und Gründungsmitglied des Vereins Digitale Gesellschaft e. V.

E-Mail: rcw@cryptolabs.org