Stephan Wiefling, Luigi Lo Iacono, Frederik Sandbrink

Anwendung der Blockchain außerhalb von Geldwährungen

Die Blockchain ist nicht nur im Bereich der Finanzwelt angekommen, auch andere Branchen versuchen sich an ihrer Anwendung. In diesem Artikel werden Konzepte und Modelle von Blockchain-Anwendungen außerhalb des Finanzbereichs vorgestellt, indem die zugehörigen Veröffentlichungen referiert und diskutiert werden. Die Anwendungsbereiche variieren aktuell über den Schutz persönlicher Daten bis zur Sicherung und Überwachung von Nahrungsmittelproduktionsketten.

1 Einführung

Die Blockchain ist in ihrer Anwendung als Grundlage diverser Krypto-Währungen sehr bekannt geworden und wurde schon als „Wunderwaffe der Finanzwelt“ bezeichnet [1]. Nun springen vermehrt andere Branchen auf den Zug auf und experimentieren oder entwickeln neue Funktionen, welche auf der Blockchain-Technologie basieren. Insbesondere der Energiesektor sieht in der Blockchain einen neuen Weg, der das Energiesystem revolutionieren könnte [2]. Vor allem durch sogenannte Smart Contracts soll das Beziehen von Strom auf ganz neue Weise ermöglicht werden. Dabei soll der Kunde über intelligent geregelte Verträge automatisch immer den günstigsten Strom bekommen. Insbesondere für Verbraucher, die eigenen Strom, zum Beispiel über Photovoltaikanlagen, erzeugen und diesen verkaufen wollen, soll durch das Wegfallen von weiteren Instanzen ein finanzieller Vorteil entstehen [3]. Zu den Smart Contracts muss gesagt werden, dass ihr Verhältnis mit dem Vertragsrecht, ihre AGB-Inhaltskontrolle sowie die Haftung für fehlerhafte Protokolle oder Programmcodes noch überprüft werden müssen [4]. Aber nicht nur der Energiesektor sieht in der Blockchain einen neuen Weg. Auch in anderen Branchen gibt es diese Bestrebungen wie im Folgenden aufgezeigt und untersucht wird.

2 Blockchains

Die Funktionsweise von Blockchain ist mehrfach ausführlich dargestellt worden [5]. Hier ein kurzer Überblick:
Aus theoretischer Sicht können traditionelle Transaktionssysteme als Zustandsübergangssysteme beschrieben werden. Dies bedeutet, dass im Wesentlichen die Übergänge relevant sind und folglich zuverlässig gespeichert werden müssen. Zum Beispiel müssen beim Verkauf eines Gegenstandes nur der Übergang vom Verkäufer zum Käufer angegeben werden. Durch eine Speicherung dieser Information kann zurückverfolgt werden, wer der aktuelle Besitzer eines Objektes ist [6]. Dies muss sich aber nicht nur auf reale Objekte beschränken. Es können auch digitale Daten sein, die zwischen zwei Usern transferiert werden. Auch die Berechtigungen zum Zugriff auf eine Datenbank können in einer Blockchain gespeichert werden, wobei in diesem Kontext der Vergeber und Empfänger der Datenzugriffsrechte die Positionen des Verkäufers und Käufers einnehmen.
Die Blockchain besteht im Allgemeinen aus einer Kette von Blöcken, welche derartige Transaktionen beinhalten. Die Größe der Blöcke, also wie viele Transaktionen pro Block gespeichert werden können, variiert je nach Einsatz der Blockchain. Diese Blöcke werden über eine kryptographische Hashfunktion miteinander unveränderbar verknüpft. Abhängig vom Einsatz der Blockchain ist die Durchführung eines sogenannten Minings [7] zur Verifizierung der Blöcke erforderlich. Zudem stellt sich häufig die Frage, wer das Mining durchführt und welche Anreize es dafür gibt. Darüber hinaus ist noch zu sagen, dass die Blockchain kein anonymer, sondern ein pseudonymer Service ist, denn alle Transaktionen eines Individuums sind einem Blockchain-Account (dem Pseudonym) zugeordnet und können unter Umständen darüber zu dem individuellen Nutzer zurückverfolgt werden [8].

3 Verschiedene Einsatzmöglichkeiten

Die Blockchain bietet Einsatzmöglichkeiten in verschiedensten Anwendungsbereichen. Im Folgenden werden beispielhaft einige in wissenschaftlichen Fachzeitschriften oder auf Konferenzen vorgestellte Systeme und Konzepte vorgestellt. Im Anschluss werden diese in Bezug auf die Eigenschaften des technologischen Blockchain-Profils evaluiert, wie sie von Böhme und Pesch [16] in diesem Heft beschrieben werden. Als Eigenschaften sind die *"Nachträgliche Unveränderbarkeit von Daten"* (Immutability), der *Verzicht auf eine zentrale Vertrauensinstanz* (Trustlessness), die *"Widerstandsfähigkeit [...] durch Vermeidung von kritischen Einzelkomponenten"* (Resilence) und die *Transparenz* durch öffentlich einsehbare Daten genannt.

Dies ist die Autorenversion eines in „Datenschutz und Datensicherheit – DuD“ veröffentlichten Artikels.
Die endgültige authentifizierte Version ist online verfügbar unter:
https://doi.org/10.1007/s11623-017-0816-x

3.1 Blockchain zum Schutz von persönlichen Informationen

Mehrere wissenschaftliche Arbeiten haben sich damit befasst, ob die Blockchain ein Mittel zur Sicherung von persönlichen Daten sein kann, wobei die Blockchain selber in diesen Konzepten nicht als Speicher für die Daten dient, sondern nur die Zugriffsberechtigungen speichert.
Von Zyskind et al. [9] wird ein neues Konzept vorgeschlagen, um persönliche Daten von Usern besser zu schützen. Dem Nutzer soll demnach die gesamte Kontrolle über seine Daten gegeben werden. Es soll ihm ermöglicht werden, zu bestimmen, wer auf seine Daten zugreifen darf. Die persönlichen Daten werden in einem Speicher außerhalb der Blockchain (Off-Blockchain) gesichert. Dieser Off-Blockchain-Speicher wird durch eine Key-Value Datenbank realisiert, welche einem Datenindex (Key) jeweils einen Datenwert (Value) zuordnet. Um die Zugangsberechtigung in der Blockchain zu speichern, werden zwei verschiedene Transaktionen genutzt. Die erste Transaktion ist die sogenannte Zugangstransaktion *Access*. Diese Transaktion wird ausgeführt, wenn ein Nutzer einem Dienst die Nutzung seiner Daten erlaubt oder wenn er die Nutzung der Daten untersagt. Die zweite Transaktion namens *Data* wird durchgeführt, wenn ein Dienst auf die Daten eines Nutzers zugreift.

In der Publikation wird zwischen *Nutzern* (User) und *Diensten* (Services) unterschieden. Nutzer sind in diesem Fall Benutzer von Smartphones und von deren mobilen Applikationen. Dienste sind die Betreiber der mobilen Applikationen, welche dafür zusätzlich persönliche Daten benötigen, zum Beispiel für Werbung. Nutzer können sich eine unbegrenzte Menge an Accounts erstellen, jedoch ist der Service nicht anonym, sondern es wird zu jedem Account ein öffentlicher Schlüssel vergeben, welcher zum Pseudonym des Account-Erstellers zurückverfolgbar ist. Zudem wird bei jeder neuen Beziehung zwischen einem Nutzer und einem Service ein neues Schlüssel-Paar generiert, welches zur Ver- und Entschlüsselung der Daten bei Datenübertragungen dient. In der Anwendung soll es wie folgt ablaufen: Ein Nutzer installiert eine neue Anwendung und bestätigt die Richtlinien des Services, dass dieser die Daten des Nutzers benutzen darf. Anschließend wird die Transaktion *Access*, die den öffentlichen Schlüssel des Nutzers beinhaltet, an die Blockchain des Dienstes gesendet. Der Service kann nun die verschlüsselten, persönlichen Daten des Nutzers abfragen. Der Zugriff auf die Daten des Nutzers durch den Service wird durch die Transaktion *Data* protokolliert. Möchte der User nun dem Service den Zugriff auf seine Daten entziehen, wird eine leere Transaktion des Typs *Access* an die Blockchain gesendet.
Das oben beschriebene Verfahren wird im Konzept *"Medrec"* von Azaria et al. [10] aufgegriffen und durch sogenannte Smart Contracts erweitert. Sie befasst sich damit, die persönlichen Daten von Patienten im medizinischen Kontext zu schützen und diese gleichzeitig Institutionen zur Forschung zugänglich zu machen. Sie bemängelt, dass Patienten oftmals wenige Informationen über ihre elektronische Krankenakte haben. Diese wüssten nicht, welche Informationen in den Akten stünden, wer sie in die Akte geschrieben habe und wer die Akte lesen dürfe. Es wird auch darauf hingewiesen, dass es Informationen gebe, die dem Patienten nicht zur Verfügung gestellt werden sollten. Durch das neue Blockchain-basierende Konzept solle dies geändert werden.
Smart Contracts steuern Funktionen zur Veränderung eines Zustandes. Es kommen drei „Smart Contracts" zum Einsatz: „Registrar Contract", „Patient-Provider Relationship" und „Summary Contract". Der „Registrar Contract" wird eingesetzt, wenn ein neuer Patient in das System hinzugefügt wird. Die Smart Contracts „Patient-Provider Relationship" und „Summary Contract" dienen zur Verwaltung der Zugriffsberechtigung und des Speicherorts der Fall-Akte des Patienten. In diesem Ansatz ist das Mining, eingesetzt zur Verifizierung der Blöcke, denjenigen Organisationen überlassen, welche die Daten der Patienten weiterverwenden wollen. Die Weiterverwendung der Daten geschieht nur durch ausdrückliche Erlaubnis des Patienten.
Eine andere Herangehensweise zur Sicherung von Daten mit einer Blockchain wird von Hashemi et al. [11] beschrieben. In der Arbeit werden verschiedene Anwendungsszenarien, zusätzlich zur Speicherung der persönlichen Patienten-Informationen, erläutert. Im Fokus steht das Internet der Dinge (Internet of Things, IoT), wobei nicht auf Geräte im Haushalt eingegangen wird, sondern auf Geräte einer Smart-City in den Bereichen Energiemanagement oder Verkehrsüberwachung. Dabei werden Sensoren, beispielsweise in öffentlichen Verkehrsmitteln, ausgelesen und die gesammelten Daten zu Analysezwecken an Dritte weitergegeben. Die dritte Anwendung, die im Artikel beschrieben wird, ist die Kommunikation zwischen autonomen Fahrzeugen. Die Funktionsweise des von den Autoren beschriebenen Modells unterscheidet sich von denen, die in vorangegangenen Arbeiten beschrieben werden. Die Funktion wird in drei Ebenen aufgeteilt. Die erste Ebene ist das „Data Management Protocol", in dem die unterschiedlichen Teilnehmer kommunizieren. Vier Rollen als Teilnehmer werden in diesem Modell unterschieden. Die erste Rolle nimmt der Daten-Inhaber („Data Owner") ein, der eine Daten-Quelle („Data Source") besitzt, welche ein Sensor oder eine andere Daten-Quelle sein kann und die die zweite Rolle im Modell einnimmt. Der Daten-Inhaber kann die Zugangsberechtigung zu der Daten-Quelle bestimmen. Die dritte Rolle ist der Datenanforderer („Data Requester"). Dieser kann eine Person oder eine Organisation sein, die Daten von einem Daten-Besitzer anfordert. Zusätzlich wird noch die Rolle des „Endorsers" genannt. Dieser stellt eine Autorität dar, die Datenanfragen und die gesendeten Daten validiert. Die zweite Ebene in dem Modell ist das „Data Storage System", welches als dezentrales Blockchain-basiertes Speichersystem beschrieben wird. Die letzte Ebene ist der „Messaging Service", der für die Realisierung des *Publisher-Subscriber-Modells* notwendig ist. Durch das Publisher-Subscriber-Modell müssen die Daten von einem Daten-Inhaber (Publisher) nur einmal an den Service gesendet werden und können dann an die Datenanforderer (Subscriber) verteilt werden. Diese Ebene übernimmt die Kommunikation zwischen dem Daten-Inhaber und dem Datenanforderer.

Wenn eine Organisation Zugriff auf die Daten eines Gerätes haben möchte, muss sie erst den Besitzer um Erlaubnis fragen. Ist dies geschehen, wird eine Nachricht an die Blockchain gesendet, die eine neue Transaktion erstellt. Diese enthält das Zugriffsrecht sowie die Identitäten des Gerätebesitzers und des Unternehmens, welches Zugriff auf die Daten haben möchte. Hiermit soll zurückverfolgbar sein, auf wie viele Geräte ein Unternehmen Zugriff hat, und nicht, welche Geräte von einem Nutzer Daten an Unternehmen senden. Dieses Modell ist ein weiteres Beispiel dafür, dass die Blockchain sich als Speicher für Zugriffsrechte eignet und die Daten in einem dezentralen Speichersystem gut gespeichert werden können.

Wie in Tabelle 1 zu sehen ist, werden die erwarteten Blockchain-Eigenschaften von den drei vorgestellten Konzepten nur in Teilen erfüllt. Im Off-Blockchain-Speicher können die Nutzerdaten nachträglich verändert werden, wodurch die geforderte *Unveränderbarkeit* (Immutability) in diesem Bereich nicht gegeben ist. Bei Medrec wird die Blockchain ausschließlich von "medical stakeholders" (Forscher, Gesundheitsorganisationen, etc.) [10] betrieben. Folglich muss den wenigen Betreibern der Blockchain vertraut werden. Aufgrund der wenigen Blockchain-Betreiber wird die *Widerstandsfähigkeit* (Resilence) geringer als bei öffentlichen Blockchains ausfallen. Da die Nutzerdaten bei allen drei Konzepten verschlüsselt gespeichert werden, ist das Kriterium der *Transparenz* in diesem Bereich nicht erfüllt.

3.2 Blockchain im Medienvertrieb mit digitaler Rechteverwaltung

Ein weiteres Cluster von Anwendungsbereichen der Blockchain ist die Verteilung von digitalen Inhalten, welche über eine digitale Rechteverwaltung abgesichert werden.

Im Konzept *"BRIGHT"* von Fujimura et al. [12] wird der Prototyp eines Online-Verwaltungssystems für digitale Rechte vorgestellt. Die Blockchain kommt bei diesem Modell als Speicher für kryptographische Schlüssel zur Entschlüsselung medialer Inhalte wie Video oder Audio, zum Einsatz. Um die Verschlüsslung von Mediendaten effizient zu gestalten wird nur der Header der Datei verändert, denn die Behandlung der Nutzdaten wäre, laut den Autoren, bei einer immer weiter steigenden Datenrate nicht mehr praktikabel. In diesem Modell wird zwischen drei Teilnehmertypen unterschieden: Dem Anbieter des Inhaltes, dem Kunden und dem Mining-Server. Der Anbieter stellt den Inhalt zur Verfügung und bestimmt, ob der Inhalt nur temporär vom Kunden genutzt werden darf oder ob dieser in den Besitz des Nutzers übergeht. Der Kunde muss, um die Inhalte nutzen zu können, in diesem Konzept immer online sein, damit die Anwendung den Rechtebesitz des Nutzers überprüfen kann. Der Mining-Server dient zur Aufnahme neuer Schlüssel in die Blockchain. Wer in der Anwendung das Mining übernimmt, ist nicht festgelegt. Es besteht die Möglichkeit, dass entweder der Kunde dies übernimmt und als Gegenleistung Inhalte bekommt, oder dass der Rechteinhaber dies übernimmt und als Gegenleistung seine Inhalte verteilt werden.

Aufgrund der Tatsache, dass die Blockchain von wenigen ausgewählten Netzwerkteilnehmern betrieben werden soll, können die erwarteten Eigenschaften *Resilence* und *Trustlessness* bei diesem Konzept nicht erfüllt werden (siehe Tabelle 1). Da alle Schlüssel öffentlich einsehbar sind und die umgesetzte Blockchain auf Bitcoin basiert, können die Eigenschaften *Transparenz* und *Immutability* als erfüllt betrachtet werden. Es sei allerdings erwähnt, dass die Blockzeit in dem Konzept von 10 Minuten auf fünf Sekunden verringert wurde, wodurch die Blockchain tendentiell anfälliger für Manipulationen sein könnte, da folglich die Rechenzeit für den Arbeitsnachweis deutlich geringer ist [8, 16].

3.3 Blockchain als Verbesserung des Domain Name Service

Der Manipulationsschutz der Blockchain beruht darauf, dass sie gleichlautend bei allen Teilnehmern gespeichert und verwaltet wird. Daher eignet sie sich besonders für Systeme, bei denen viele Teilnehmer die gleichen Informationen besitzen müssen. Dies wird in einer Arbeit über den Domain Name Service (DNS) genutzt. Der DNS dient grundsätzlich dazu, IP-Adressen einen Domain-Namen, der sowohl maschinen- als auch menschenlesbar ist, zuzuordnen. Dabei muss jeder Teilnehmer wissen, ob ein Domain-Name schon an einen anderen Teilnehmer vergeben ist, oder noch zu erwerben ist. Ebenso muss jedem Teilnehmer die Zuordnung von Domain-Namen zu IP-Adresse bekannt sein.

In [13] wird ein Modell beschrieben, das als Zusatz für den DNS-Standard dienen kann. Es wird deutlich gemacht, dass das hier vorgeschlagene Modell den DNS auf Grund seiner weiten Verbreitung nicht ersetzen kann, sondern nur als Zusatz dient. Den größten Schwachpunkt im bestehenden DNS sehen die Autoren dieser Arbeit darin, dass er von wenigen Zentren aus organisiert ist und daher leicht von Regierungen gesteuert werden kann, zum Beispiel indem sie mit ihrem Einfluss den Zugriff auf Webseiten sperren. Durch das vorgestellte Modell namens *Distributed Decentralized Domain Name Service* (D^3NS) soll dies mit Hilfe der Blockchain auf ein dezentralisiertes System erweitert werden, auf das eine Regierung nur schwer Einfluss nehmen kann.

In dem Modell werden die Informationen in einer Blockchain und einer verteilten Hashtabelle gespeichert. In der Blockchain wird die Information über den Besitzer einer Domain und in der verteilten Hashtabelle die weiteren zugehörigen Informationen (DNS Records) gespeichert. Der Besitz einer Domain wird mit einem kryptographischen Schlüssel-Paar verifiziert, dem die Identität eines Besitzers zugeordnet ist. Der öffentliche Schlüssel dient dabei zur Verifizierung der in der Hashtabelle vom Domaininhaber signierten Domaininformationen. Bei einer übertragenen Domain wird der öffentliche Schlüssel des neuen Besitzers als Domaininhabereintrag in die Blockchain geschrieben und die Transaktion mit dem privaten Schlüssel des *alten* Besitzers unterschrieben. Um Anspruch auf eine Domain zu bekommen, muss ein Nutzer einen Block „mi-

nen“, also verifizieren. Die Gegenleistung für diese rechen- und energieaufwändige Arbeit ist der Besitz eines noch nicht vergebenen Domainnamens. Ein Problem dieses Modells ist das Folgende: Wenn der Besitzer seinen privaten Schlüssel verliert, ist es nicht möglich, die Domain weiter zu übertragen. Wie der Besitzer sich beim erstmaligen Teilnehmen an dem D^{3}NS-Ansatz verifiziert, ist in der Arbeit nicht beschrieben. Es wird nur festgestellt, dass ihm durch die Teilnahme an der Blockchain vertraut werden kann. Da dieses Modell als Zusatz zum bisherigen DNS gedacht ist, wird die Kommunikation zwischen den beiden Systemen so beschrieben, dass D^{3}NS nur Informationen an den Standard-DNS weitergibt, aber keine Informationen vom DNS übernimmt. Die Autoren beschreiben, dass die Zusammenarbeit von Blockchain und verteilter Hashtabelle nicht alle Probleme im Bereich DNS lösen kann, aber eine Lösung für viele andere Webservices sein kann.

Die in [16] geforderten Blockchain-Eigenschaften können von D^{3}NS größtenteils erfüllt werden. Lediglich die *Immutability* ist durch die veränderbaren DNS-Records in der verteilten Hashtabelle nicht vollständig erfüllt (siehe Tabelle 1).

3.4 Blockchain als dezentraler Speicher von Informationen in einer Community

Auch im Bereich der Community-Systeme existieren Ansätze zur Anwendung von Blockchain-basierten Lösungen. Wie gewohnt wird dabei der Vorteil genutzt, dass die Blockchain nicht veränderbar ist und dass es durch die Dezentralität keine Autorität gibt, die Einfluss auf die Community nehmen kann.

In [14] wird beschrieben, wie in einer Peer-to-Peer (P2P) Community mit Hilfe der Blockchain ein sicheres System zur Bewertung von Usern aufgebaut werden kann. In der Arbeit wird festgestellt, dass es im Internet schwierig ist, einem Unbekannten zu trauen. Deshalb gibt es in vielen Communities, in denen Handel oder ein Austausch von realen oder virtuellen Objekten betrieben wird, ein Bewertungssystem, das zeigt, ob der jeweilige User vertrauenswürdig ist oder nicht. Zusätzlich zu einem sicheren und dezentralen Bewertungssystem sollen auch verschiedene Arten von Angriffen auf Bewertungen verhindert oder erschwert werden. Zu diesen Attacken gehört z.B. eine unfaire Bewertung des Beteiligten, obwohl die Transaktion erfolgreich war. Es könnten in den traditionellen Systemen auch mehrere Accounts erstellt werden, um die Bewertung eines Nutzers unfair zu verbessern oder zu verschlechtern.

Eine Übermittlung von Dateien in einer P2P Community läuft in dem Verfahren wie folgt ab: Der erste Schritt ist, dass der Sender eine angeforderte Datei mit seinem privaten Schlüssel signiert und an den Empfänger sendet. Der Empfänger überprüft die Korrektheit der Datei und sendet dann eine Nachricht an die Mining-Server mit dem aktuellen Stand der Bewertung der jeweiligen Beteiligten. In der Nachricht sind ebenfalls ein Zeitstempel und der Hashwert der gesendeten Datei enthalten. Diese Informationen werden nun von den Mining-Servern als Transaktion in die Blockchain angehängt. Damit wird von den Mining-Servern die Transaktion verifiziert und die Bewertung des Senders um einen Punkt erhöht. Die Beteiligten der Übertragung müssen bis zur Verifizierung der Übertragung online bleiben. Da die Blockchain bei vielen Transaktionen pro Sekunde sehr schnell anwachsen kann, wird die Blockchain im ganzen Umfang nur auf den Mining-Servern gespeichert. Um zum Beispiel die oben genannten Attacken zu verhindern, wird die Identität eines Nutzers an seine IP-Adresse gebunden. Dadurch soll die Erstellung mehrerer Accounts erschwert werden. Durch die automatische Bewertung des erfolgreichen Ablaufs einer Übertragung, kryptographisch nachgewiesen durch die sender- und empfängerseitige Signierung einer tatsächlich angeforderten Datei, kann der Nutzer keine unfaire Bewertung abgeben.

Unter der Annahme, dass das Bewertungssystem unter *allen* Teilnehmern einer P2P Community, wie z.B. die Netzwerkteilnehmer von BitTorrent, verwendet werden würde, könnte dieser Ansatz alle geforderten Blockchain-Eigenschaften erfüllen, wie in Tabelle 1 zu sehen ist.

3.5 Blockchain zur Überwachung von Lebensmittelproduktionen

Auch im Bereich der Produktion, besonders der von Lebensmitteln, gibt es Konzepte für einen Einsatz der Blockchain.

In [15] wird ein Konzept beschrieben, das ein Zusammenspiel von Blockchain als Speicher und RFID-Chip (Identifizierung von Objekten mit Hilfe von elektromagnetischen Wellen) zur Identifizierung und Sammlung von Daten beschreibt. Die Autoren sehen als Vorteile in diesem System, dass in jedem Produktionsschritt alle Daten sicher und unveränderlich gespeichert werden. In dem Artikel wird besonders auf die häufigen Lebensmittelskandale in China verwiesen. Das Modell ist so gestaltet, dass in jedem Produktionsschritt die wesentlichen Informationen in der Blockchain gespeichert werden. In der Fleischerzeugung werden z.B. in der Aufzucht der Hof und die zugehörigen Mitarbeiter notiert und welcher Mitarbeiter in der Verarbeitung das Produkt bearbeitet hat und wie lange es sich in der Lagerung befand. Die Identifizierung des Nahrungsmittels soll über den RFID-Chip geschehen, da dies schon ein in der Nahrungsmittelerzeugung eingesetztes Mittel ist. Durch die Unveränderbarkeit der Blockchain kann zu keinem Zeitpunkt der Produktionskette eine Veränderung der Informationen vorgenommen werden. Dies könnte möglichen Lebensmittelskandalen vorbeugen.

Aufgrund fehlender Spezifizierung der Blockchain-Node-Betreiber im Artikel kann keine Aussage über die Eigenschaften *Trustlessness* und *Resilence* in diesem Ansatz getroffen werden. Die Eigenschaften *Immutability* und *Transparenz* können jedoch als erfüllt betrachtet werden (siehe Tabelle 1).

4 Zusammenfassung und Ausblick

	Immutability	Trustlessness	Resilence	Transparenz
Private Daten [9]	✓ (Schlüssel) × (Daten)	? (Betreiber unklar)	?	✓ (Schlüssel) × (Daten)
Medrec [10]	✓ (Schlüssel) × (Daten)	× ("medical stakeholders" muss vertraut werden)	× (weitgehend private Blockchain)	✓ (Schlüssel) × (Daten)
IoT [11]	✓ (Schlüssel) × (Daten)	✓	✓ (Schlüssel) ? (Daten)	✓ (Schlüssel) × (Daten)
BRIGHT [12]	✓	× (Betreibern muss vertraut werden)	× (weitgehend private Blockchain)	✓
D³NS [13]	✓ (Schlüssel) × (DNS-Records)	✓	✓	✓
Bewertungssystem [14]	✓	✓	✓	✓
Lebensmittel [15]	✓	? (Betreiber unklar)	?	✓

Tabelle 1: Vergleich der vorgestellten Konzepte im Bezug auf die Eigenschaften des technologischen Blockchain-Profils aus [16]

Durch ihre Unveränderbarkeit kann die Blockchain besonders in Bereichen eingesetzt werden, die Wert darauf legen, dass ihre Daten dezentral gesteuert werden, dass sie korrekt sind und dass niemand von innen oder außen die Daten verändern kann. Es gibt viele Domänen, die deshalb Anwendungen mit der Blockchain-Technologie erforschen,. Bis auf den Finanzsektor hat es die Blockchain jedoch noch in keinem Bereich zum Durchbruch geschafft.

Wie Tabelle 1 zeigt, sind die angedachten und vorgeschlagenen Ansätze bisher noch unausgegoren. In vielen Fällen werden wesentliche Eigenschaften nicht berücksichtigt oder gar erbracht. Dazu lassen die wissenschaftlichen Arbeiten praxisrelevante Metriken, wie z.B. die Wachstumsfunktion des Speicherbedarfs und Mininganreize, außer Acht. Dem Hype folgt die Ernüchterung, dass sehr genau geprüft und analysiert werden muss, bevor es zum Einsatz der Blockchain-Technologie kommen kann.

Literatur

[1] https://www.heise.de/newsticker/meldung/Bitcoin-Technik-Blockchain-als-Wunderwaffe-der-Finanzwirtschaft-2699919.html, abgerufen am 21.02.2017

[2] http://www.sueddeutsche.de/wissen/energie-wie-blockchain-technik-das-energiesystem-revolutionieren-kann-1.3117309#redirectedFromLandingpage, abgerufen am 21.02.17

[3] http://www.verbraucherzentrale.nrw/blockchain, abergerufen am 21.02.2017

[4] https://anwaltsblatt.anwaltverein.de/files/anwaltsblatt.de/Rubriken/news/2016/AnwBl%202016,%20612_Blocher.pdf, abgerufen am 21.02.17

[5] Böhme R, Christin N, Edelman B, Moore T (2015) Bitcoin: Economics, Technology, and Governance. J Econ Perspect 29:213–238. Siehe auch den Beitrag von Böhme und Pesch in diesem Heft.

[6] https://fahrplan.events.ccc.de/congress/2016/Fahrplan/system/event_attachments/attachments/000/003/123/original/handout.pdf, abgerufen am 21.02.17

[7] Gervais, A., Karame, G., Capkun, S., Capkun, V.: Is Bitcoin a Decentralized Cur-rency?. IEEE Security & Privacy 12, no. 3 (May 2014), 54–60.

[8] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org (2008).

[9] Zyskind, G., Nathan, O.und Pentland , A. S. Decentralizing privacy: Using blockchain to protect personal data. Security and Privacy Workshops (SPW), 2015 IEEE (July 2015)

[10] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. Medrec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD) 1 (August 2016), 25–30.

[11] Hashemi, S. H, Faghari, F., Rausch, P., Campbell, R.H. World of empowered IoT users. Internet-of-Things Design and Implementation (IoTDI), 2016 IEEE First International Conference on (April 2016).

[12] Fujimura, S., Watanbe, H., Nakadaira, A., Yamada, T., Akutsu, A., Kishigami, J. J. BRIGHT: A concept for a decentralized rights management system based on blockchain. Consumer Electronics - Berlin (ICCE-Berlin), 2015 IEEE 5thInternational Conference on (September 2015).

[13] Benshoof, B., Rosen, A., Bourgeois, A.G., Harrison, R.W. Distributed decentral-ized domain name service. Parallel and Distributed Processing Symposium Work-shops, 2016 IEEE International (August 2016).

[14] Dennis, R., Owen, G. Rep on the block: A next generation reputation system based on the blockchain. International Conference for Internet Technology and Secured Transactions (December 2015).

[15] Tian, F. An agri-food supply chain traceability system for china based on RFID & blockchain technology. Service Systems and Service Management (ICSSSM), 2016 13th International Conference on (August 2016).

[16] Böhme, R. und Pesch, P. Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, Datenschutz und Datensicherheit (August 2017)

Stephan Wiefling ist wissenschaftlicher Mitarbeiter in der Gruppe für Daten- und Anwendungssicherheit der TH Köln. Die Forschungsschwerpunkte liegen in den Bereichen Cloud Computing und Blockchain.

Luigi Lo Iacono ist Professor an der Fakultät für Informations-, Medien- und Elektrotechnik der TH Köln und Leiter der Gruppe für Daten- und Anwendungssicherheit.

Frederik Sandbrink ist Masterstudent der Medientechnologie an der Fakultät für Informations-, Medien und Elektrotechnik der TH Köln.