# IMMANENTES SYSTEMVERTRAUEN DER BLOCKCHAIN FÜR INTERNET OF THINGS – ERGEBNISSE EINER SYSTEMATISCHEN ÜBERPRÜFUNG

Stefan Tönnissen, Frank Teuteberg
Universität Osnabrück, Katharinenstr. 1, D-49069 Osnabrück

Mehr als 50 Milliarden physische Objekte sollen bis 2020 mit dem Internet verbunden sein. Diese reichen von kleinen und rechenarmen RFID-Systemen bis zu komplexen Geräten wie Smartphones, intelligenten Geräten und Fahrzeugen. Für dieses Internet of Things (IoT) bedarf es eines Systemvertrauens, da die Nutzung intelligenter Dienste über das Internet ohne menschliches Eingreifen geschieht. Heute vorhandene zentrale Vertrauensinstanzen für IoT verlieren aufgrund von Hacker- und Cyberangriffen ihr Vertrauen. Mit der Blockchain existiert eine Vertrauensarchitektur, die es dem Menschen erlaubt, einem System und seinen Komponenten, und nicht einer zentralen Instanz zu vertrauen. Kann die Symbiose von Blockchain und IoT Vertrauen generieren? Dieser Artikel präsentiert eine systematische Literaturübersicht zum Konzept Vertrauen im Kontext der Blockchain-Technologie für das IoT und deren Geschäftsmodelle. Das Ziel dieses Beitrags ist die Darstellung der aktuellen Entwicklungen im Zusammenspiel von Blockchain und IoT, um diese als Blaupause für die Schaffung von Vertrauen in weiteren Anwendungsfeldern nutzen zu können.

More than 50 billion physical devices will be connected to the Internet by 2020. These range from small and rake-poor devices such as RFIDs to complex devices such as smartphones, smart devices and vehicles. This Internet of Things (IoT) requires system trust, as the use of intelligent services over the Internet is done without human intervention. Today's central IoT line of businesses (LOBs) lose their confidence due to hacker and cyber-attacks. Blockchain is a trust architecture that allows people to trust a system and its components, not a central entity. Can the symbiosis of blockchain and IoT generate trust? This article presents a systematic literature review of trust in the context of blockchain technology for the IoT and its business models. The aim of this paper is to present the current developments in the interplay between Blockchain and IoT in order to use it as a blueprint for the creation of trust in other fields of application.

## 1. Einleitung

„Vertrauen ist der Schlüssel für die digitale Wirtschaft“ [43]. Der Economist beschrieb bereits 2015 die Blockchain als eine Technologie zur Schaffung von Vertrauen für Menschen, die kein besonderes oder besonders hohes Vertrauen ineinander haben, jedoch miteinander arbeiten müssen ohne eine neutrale zentrale Instanz zu nutzen. Walterbusch et al. (2014) heben hervor, „…trust is a fundamental cornerstone in the business context“. Die Sharing Economy erfährt eine Verlagerung von einer Infrastruktur, die Menschen voreinander schützt, zu einer Infrastruktur, die Vertrauen zwischen Menschen schafft [16]. In einer aktuellen Studie von Bitkom bestätigen Blockchain-Experten, dass die Blockchain Geschäftsbeziehungen zwischen Unternehmen schaffen kann, die bisher aufgrund fehlenden Vertrauens nicht zustande gekommen wären [4]. In diesem nicht vertrauenswürdigen Umfeld schafft die Blockchain die Voraussetzungen zur Speicherung von Informationen [9]. Die Blockchain als Distributed Ledger Technologie schafft somit Vertrauen in die Funktionalität und Manipulationsfreiheit und gibt dem Nutzer das Vertrauen, dass Inhalte nicht geändert werden. Sie erreicht dies durch eine dezentrale, redundante und manipulationssichere Speicherung von Daten [29]. Jedoch ist Vertrauen zunächst an Personen und Interaktionen zwischen Personen gebunden, daher sprechen wir hinsichtlich des Vertrauens in die Blockchain von Systemvertrauen und damit in die Funktionsfähigkeit von Systemen [5]. Dieses Systemvertrauen lässt sich nach Heidt et al. (2019) in die Dimensionen Vertrauen in Code, Vertrauen in Daten, Vertrauen in die Vision eines Projektes sowie systemisches Vertrauen einteilen.

Für bestehende und vertrauensvolle Beziehungen zwischen Geschäftspartnern ist demnach eine Blockchain unnötig, es sei denn, andere Aspekte wie die Schaffung von Transparenz treten in den Vordergrund [52]. „Vertrauen ist gut, Blockchain ist besser.“ [44] Die Blockchain ist jedoch eine komplexe Technologie, die laut einer Studie von pwc aus dem Jahre 2016 nur von 19% der Menschen in Deutschland verstanden wird [39]. Wie kann unter diesen Voraussetzungen die Blockchain das Systemvertrauen herstellen beziehungsweise in welchem Kontext wird das Systemvertrauen hergestellt? Denn das ebenbürtige Äquivalent zu Vertrauen ist Misstrauen, und fordert daher von einem Individuum eine permanente Entscheidung zwischen diesen beiden Möglichkeiten. Dem Misstrauen immanent ist eine geringere Abhängigkeit von Informationen [23]. Neben technischen Aspekten und der Frage der Finanzierung sollten sich erfolgreiche Geschäftsmodelle auch mit dem Aspekt des Vertrauens beschäftigen, um nicht zu scheitern [16]. Sollte das Vertrauen der Öffentlichkeit in ein bestimmtes Unternehmen schwinden, so kann dies „…to an immediate and short-term loss in customers or a dip in the share price“ führen [42]. In einer Untersuchung von Rodig (2017) über IoT-basierte Geschäftsmodelle zeigen 51% der untersuchten IoT-Projekte, dass die Schaffung von zusätzlichen Einnahmen durch neue Services oder Produkte für bereits adressierte Zielgruppen im Vordergrund steht.

Unsere vorherigen Überlegungen führen zu folgen-

den Forschungsfragen (FF), die wir im Rahmen dieses Beitrags anhand eines systematischen Literaturreviews beantworten:

- FF1: Mit welchen technischen oder konzeptionellen Lösungen wird das Systemvertrauen in die Blockchain hergestellt?
- FF2: Welche Dimensionen von Vertrauen werden dabei angesprochen?
- FF3: Welche Muster der Vertrauensgenerierung für IoT-basierte Geschäftsmodelle sind bisher entwickelt worden?

Unser Beitrag ist wie folgt aufgebaut: Zunächst führen wir in die Grundlagen über Vertrauen, die Blockchain-Technologie und das IoT ein, um im nächsten Kapitel die methodische Vorgehensweise unserer Arbeit zu erläutern. Daran schließt sich die Suche nach Literatur und deren Auswertung an, um dann im nächsten Kapitel die Ergebnisse zu präsentieren und die Schlussfolgerungen hinsichtlich unserer Forschungsfragen zu präsentieren. Zum Ende werden Limitationen und ein Ausblick dargestellt.

## 2. Grundlagen

### 2.1 Vertrauen

Vertrauen wird als Enabler für soziale Interaktionen gesehen und hat ihren Ursprung der Forschung außerhalb des Bereichs der Informationssysteme. Seit vielen Jahren nimmt jedoch die Bedeutung des Vertrauens durch den Fortschritt der Technologien, wie zum Beispiel dem elektronischen Geschäftsverkehr, zu. Denn durch virtuelle Teams, Online-Märkten und Plattform getriebenen Geschäftsmodellen nehmen die Interaktionen und der Handel zwischen Fremden zu [50]. Vertrauen ist von besonderer Bedeutung, wenn Unternehmen ihre Prozesse oder Daten in elektronische Märkte oder an Cloud-Computing Anwendungen übergeben [53]. Vertrauen bezeichnet die subjektive Überzeugung von der Richtigkeit, von der Wahrheit von Handlungen, von Einsichten und Aussagen. Es tritt in unsicheren Situationen oder bei Handlungen mit einem risikohaften Ausgang auf, bedingt jedoch immer eine Grundlage [28]. Vertrauen braucht zum einen Grundlagen und muss zum anderen stets über gute Gründe hinausgehen und Ungewissheit aufheben [35]. Es ist darüber hinaus ebenfalls die Erwartung, nicht durch das Handeln anderer benachteiligt zu werden und schafft somit die Grundlage jeder Kooperation [49]. Neben dem interpersonalen Vertrauen zwischen Personen ist das Systemvertrauen als Vertrauen in die Systemzuverlässigkeit zu berücksichtigen. Hierbei wird dem Funktionieren des Systems ein Vertrauen geschenkt, und dies nicht durch ein einzelnes Individuum, sondern durch deren Masse. Des Weiteren ist Kontinuität im Vertrauen an die Funktionsfähigkeit des Systems notwendig, ohne dass das einzelne Individuum verstehen muss, wie das System funktioniert. Dass es funktioniert, reicht für das Vertrauen aus [23].

Im Kontext der Blockchain haben Heidt et al. (2019) folgende Vertrauensdimensionen unterschieden, die wir in unsere Arbeit übernehmen:

• **Vertrauen in Code**: Benutzer vertrauen darauf, dass das System keine schwerwiegenden Programmierfehler enthält.

• **Vertrauen in Daten**: Benutzer vertrauen darauf, dass die in das System eingegebenen Daten korrekt und überprüfbar sind. Dies ist von größter Bedeutung, da Daten direkt die Grundlage für Entscheidungen bilden.

• **Vertrauen in die Vision**, die das Projekt befeuert: Benutzer vertrauen darauf, dass das System genügend Schwung erhält, um ein digitales Ökosystem zu schaffen, das die fragliche Plattform unterstützen kann.

• **Systemisches Vertrauen**: Um auf ein bestimmtes System oder eine bestimmte Plattform vertrauen zu können, müssen mehrere Elemente zusammenwirken. Ob Benutzer einem System oder einer Plattform vertrauen oder ihnen misstrauen, hängt vom erfolgreichen Zusammenspiel der oben genannten Elemente ab [22].

• **Authentifizierung**: Sie sorgt dafür, dass die Identität eines Benutzers gegenüber einem System nachgewiesen und verifiziert werden kann [32].

• **Autorisierung**: Nach der Authentifizierung ist die Identität vom System bestätigt und mit der Autorisierung erfolgt die Zugriffsberechtigung [32].

Vertrauen ist allgemein eine entscheidende Komponente für erfolgreiche Transaktionen, unabhängig davon, ob sie in einem physischen oder virtuellen Raum ausgeführt werden [51].

### 2.2 Blockchain

Die Blockchain als Distributed Ledger ist in ihrer allgemeinen Form eine verteilte Transaktionsdatenbank in einem Peer-to-Peer-Netzwerk, die Transaktionen als digitale Ereignisse aufzeichnet [2]. Die global verteilten Knoten in dem Netzwerk sind mit einer eigenen Protokollschicht für die Kommunikation zwischen den Knoten verbunden. Die Identifizierung geschieht durch die IP-Adresse des Knoten und über die öffentlichen Schlüssel der Benutzer [14]. Innerhalb der Teilnehmer in dem Peer-to-Peer-Netzwerk der Blockchain sind die gespeicherten Transaktionen unveränderlich und werden über einen Konsensmechanismus konsistent gehalten [37]. Jeder Teilnehmer dieser Blockchain kann alle Transaktionen einsehen sowie die chronologische Kette der Blöcke nachvollziehen [2]. Die Blockchain ist eine Kette von Blöcken, von denen jede eine Reihe von Transaktionen eines bestimmten Zeitraumes enthält. Die Unveränderlichkeit dieser Kette von Blöcken geschieht durch die Sicherung der Transaktionsdaten durch kryptografische Hash-Funktionen. Hierbei werden die Blöcke mit dem vorherigen Block dadurch verbunden, dass der Hash des vorherigen Blocks in den Hash des aktuellen Blocks einfließt. Somit ist es praktisch unmöglich, Transaktionen der Blockchain rückgängig zu machen oder zu manipulieren. Alle Teilnehmer eines Blockchain Peer-to-Peer-Netzwerks verfügen über einen

persönlichen Schlüssel zur Signierung der Transaktionen. Aufgrund des über das Netzwerk verteilten Hauptbuches verfügt jeder Teilnehmer über das Wissen, wie die digitalen Assets unter den Teilnehmern verteilt sind. Dieses Wissen verhindert die doppelte Ausgabe oder Weitergabe von digitalen Assets, die Vermeidung des double-spending. Als Mehrbenutzersystem ist die Blockchain konzipiert worden, um kontinuierliche und nicht zentral durch einen Intermediär gesteuerte Interaktionen zwischen heterogenen Teilnehmergruppen zu ermöglichen. Die Blockchain kann entweder als öffentliche oder private Blockchain verwendet werden. Eine öffentliche Blockchain steht jedermann zur Nutzung frei und erlaubt die Einsicht in alle Daten. Die private Blockchain hingegen ist nur für ausgewählte Benutzer zugänglich und bedingt eine entsprechende Berechtigung für den Zugang.

Die systemimmanente Vertrauensgrundlage von Blockchain (siehe hierzu auch Kapitel 2.1 Vertrauen) setzt sich zusammen aus:

a) **Smart Contracts**. Sie fördern die Effizienz, Sicherheit und Unparteilichkeit bei der Ausführung eines Vertrages auf der Blockchain und schaffen somit das Vertrauen zwischen den Parteien [25].

b) Dem Proof-of-work **Konsensmechanismus**, der die Inhalte der Blockchain vor Manipulationen [1] schützt und Transaktionen ohne Konsens ablehnt [29].

c)Die **Unveränderlichkeit** der Daten und die Nachvollziehbarkeit von Änderungen erhöht die Transparenz und schafft somit Vertrauen [46].

d) Dem **Peer-to-Peer Netzwerk**, in dem jeder Teilnehmer im Mining Netzwerk als vertrauenswürdiger Dritter für Clients fungieren kann [3].

e) Dem **Distributed Ledger** zur Vermeidung eines Single Point of Failure [3].

f) Die Gewährleistung der **Integrität** der in der Blockchain gespeicherten Daten [29].

g) Anhand der **Kryptographie** mit öffentlichen Schlüsseln [29].

Während es verschiedene Varianten und Ausprägungen von Blockchain gibt, konzentrieren wir uns in diesem Beitrag auf öffentliche Blockchain mit den nachfolgenden Eigenschaften in Tabelle 1.

Tabelle 1: Eigenschaften einer öffentlichen Blockchain [37]

| *Eigenschaft* | *Erläuterung* |
|---|---|
| Open Source | Jeder kann eine Blockchain einrichten. |
| Dezentralisierung | Es gibt keine zentrale Instanz beziehungsweise Indermediären; die Blockchain ist Teil eines Peer-to-Peer-Netzwerkes. |
| Konsens | Die Aufnahme einer Transaktion geschieht nur durch einen Konsens. Es gibt nur einen Single Point of Truth. |
| Manipulations-sicherheit | Neue Einträge in die Blockchain werden nur akzeptiert, wenn sie auf unveränderten Einträgen basieren. |
| Gültigkeit | Neue Einträge in die Blockchain werden nur akzeptiert, wenn sie einem vordefinierten Protokoll entsprechen. |

### 2.3 Internet of Things

Mit IoT wird die Verknüpfung eines physischen Objekts beziehungsweise Gegenstandes mit einer digitalen Repräsentation verstanden [30], oder auch die Verschmelzung von physischen Produkten und digitalen Services zu hybriden Lösungen [11]. Die Basistechnologie des IoT sind drahtlose Sensornetzwerke [45]. Mit dem IoT wird die Vision verfolgt, das Internet durch die Einbindung physischer Gegenstände in die reale Welt hinein zu verlängern [11]. Das Potential liegt laut Analysten bis 2020 bei mehr als 50 Milliarden Geräten [24]. Mit Hilfe von Minicomputern werden Gegenstände und Orte zu smarten Dingen, die Informationen aus der Umwelt verarbeiten und mit dem Internet kommunizieren [11]. Zahlreiche Gegenstände der täglichen Verwendung werden mit elektronischen Geräten ausgestattet, um sie miteinander und mit dem Internet zu verbinden. Der Datenaustausch erfolgt ohne einen menschlichen Eingriff [20]. Die sich hieraus ergebenden Herausforderungen und Probleme basieren hauptsächlich auf dem allgegenwärtigen Zugang zum Internet, der enormen Menge an verbundenen Geräten sowie der Heterogenität der entsprechenden Komponenten [6]. Aufgrund der Autonomie der Vernetzung als auch des Datenaustausches dieser Geräte liegt eine weitere Herausforderung in der Authentifizierung sowie der Integrität der ausgetauschten Daten [20]. Die heutigen IoT-Systeme sind so konzipiert, dass Sicherheit und Datenschutz einem vertrauenswürdigen Dritten übertragen werden [34]. Der Austausch von Informationen und die Vernetzung der Geräte erfordert in diesem Kontext ein hohes Maß an Vertrauen [26]. Die größte Herausforderung liegt demnach in der Überbrückung der aktuell stark fragmentierten Vertrauensdomänen [38]. Hierbei sind die fünf Wertschöpfungsstufen einer IoT-basierten Anwendung zu beachten, die sich in eine Ebene der physischen Welt als auch eine Ebene der digitalen Welt einteilen lassen (siehe Bild 2). Die physische Welt besteht aus der physischen Ebene auf Ebene 1 und der Sensoren und Aktuatoren auf Ebene 2. Die Verbindung der physischen mit der digitalen Welt des Internets geschieht auf der Ebene 3 mit Konnektoren. Darauf baut die Ebene 4 mit der Analytik der Daten sowie Ebene 5 mit den Webservices oder mobilen Applikationen auf [11].

## 3. Methodische Vorgehensweise

### 3.1 Ablauf

Für die Beantwortung unserer Forschungsfrage führten wir zunächst ein Literaturreview mit 369 Treffern durch (siehe Abbildung 1). Diese Treffer wurden dann einer Konformitätsprüfung anhand der Merkmale Kontext, Zweck und praktischer Beitrag unterzogen, um nur die für unsere Forschungsfragen relevanten Beiträge bestimmen zu können. Das Ergebnis sind 79 Treffer, die anhand der Vertrauensdimensionen (siehe Kapitel 2.1) sowie der systemimmanenten Vertrauenseigenschaften der Blockchain (siehe Kapitel 2.2) analysiert wurden. Mit dem Ergebnis können wir die Forschungsfragen FF1 und FF2 beantworten. Für die Beantwortung der Forschungsfrage FF3 führten

wir zunächst auf der Grundlage der zuvor erhobenen Daten eine hierarchische Cluster-Analyse mit der Ward-Methode durch, um anhand der unterschiedlichen Cluster die Muster der Vertrauensgenerierung ableiten zu können.

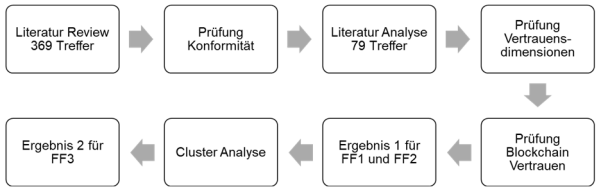


Bild 1: Ablauf der Forschung

### 3.2 Literaturreview

Das Literaturreview der Beiträge und Artikel wurde unter Verwendung der in Tabelle 2 und Tabelle 3 angegeben Quellen im Juli 2019 durchgeführt.

Die Suche nach relevanten Beiträgen ist in zwei Stufen durchgeführt worden:

1.Stufe: Suche nach Beiträgen zu „Blockchain Trust IoT“, „Blockchain Trust Internet of Things“ sowie „Blockchain Vertrauen IoT“ und „Blockchain Vertrauen Internet of Things“.

2.Stufe: Suche nach Beiträgen zu „Blockchain Trust“ sowie „Blockchain Vertrauen“. Manuelle Sichtung der zusätzlichen Beiträge anhand des Titels und des Abstracts und Entscheidung für eine Aufnahme in unsere Analyse.

Der Grund für diese Vorgehensweise ist, dass wir auch Beiträge wie zum Beispiel „BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs” in unsere Analyse einbeziehen wollen, obwohl der Begriff IoT oder Internet of Things fehlt. Jedoch sind Vehicular Ad Hoc Network (VANet) ein Teil von Internet of Things und damit relevant für unsere Analysen.

Die Auswertung von Journals führt zu der in Tabelle 2 aufgeführten Ergebnisse.

Tabelle 2: Ergebnisse unserer Literaturanalyse in Journals

| *Quelle:* | *Ergebnis* |
|---|---|
| IEEE Xplore, | 58 Treffer, davon 28 als relevant eingestuft. |
| Web of Science | 37 Treffer, davon 10 als relevant eingestuft. |
| Google Scholar | 26 Treffer, davon 21 als relevant eingestuft. |
| Springer Link | 220 Treffer, davon 29 als relevant eingestuft. |
| Science Direct | 21 Treffer, davon 5 als relevant eingestuft. |

Neben den Journalen haben wir drei gemäß Verband der Hochschullehrer für Betriebswirtschaft (VHB) Jourqual3 Rating hoch bewertete und renommierte Konferenzen der Wirtschaftsinformatik und deren Proceedings nach relevanten Beiträgen mit folgendem Ergebnis durchsucht (siehe Tabelle 3).

Tabelle 3: Ergebnisse unserer Literaturanalyse in Konferenzen

| *Quelle:* | *Ergebnis* |
|---|---|
| ICIS | 3 Treffer, davon 0 als relevant eingestuft. |
| ECIS | 4 Treffer, davon 0 als relevant eingestuft. |
| WI | 0 Treffer, davon 0 als relevant eingestuft |

Nach der Bereinigung der Ergebnisse anhand von Doppelungen (14 Beiträge) konnten wir 79 Beiträge zur Beantwortung unserer Forschungsfragen selektieren.

Die Konformität der ausgewählten Beiträge wurde anhand der Titel und der Abstracts nach den folgenden Einschlusskriterien untersucht:

- **Kontext**: Die Studien sollten ihre Beiträge im Kontext der Blockchain-Technologie definieren, die in den Anwendungsbereich von IoT zielen.
- **Zweck**: Der Zweck dieser Studien muss sich auf konkrete Lösungsvorschläge zur Generierung von Vertrauen durch die Blockchain-Technologie im Kontext von IoT beziehen.
- **Praktischer Beitrag**: Die Studien sollten mindestens eines der folgenden Elemente von Design Science Research enthalten: praktische Umsetzung, Tests, kritische Analyse, Bewertung oder Diskussion [13].

Die wichtigsten extrahierten Merkmale sind die Eigenschaften des systemimmanenten Vertrauens der Blockchain (siehe Kapitel 2.2) sowie die Dimensionen des Vertrauens (siehe Kapitel 2.1).

### 3.3 Verwandte Arbeiten

Anhand des zuvor durchgeführten Literaturreviews konnten wir die nachfolgenden thematisch verwandten Arbeiten finden (siehe Tabelle 4).

Tabelle 4: Verwandte Arbeiten

| *Titel des Beitrags* | *Autoren* |
|---|---|
| The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. | Hawlitscheka, F. et al. (2018) |
| Vertrauen ist gut, Blockchain ist besser – Einsatzmöglichkeiten von Blockchain für Vertrauensprobleme im Crowdsourcing. | Schütz, A.E. et al. (2018) |
| The issue of user trust in decentralized applications running on blockchain platforms. | Bracamonte, V. und Okada, H. (2017) |
| Blockchain-Based Traffic Event Validation and Trust Verification for VANETs. | Yang, Y.-T. et al. (2019) |
| Blockchain based trust & authentication for decentralized sensor networks. | Moinet, A. et al. (2017) |
| TrustChain: Trust Management in Blockchain and IoT supported Supply Chains. | Malik, S. et al. (2019) |
| Research on trust mechanism of cooperation innovation with big data processing based on blockchain. | Liu, Q. und Zou, X. (2019) |

| *Titel des Beitrags* | *Autoren* |
|---|---|
| Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions. | Iqbal, R. et al. (2019) |

Hawlitscheka et al. (2018) untersuchen in ihrem Beitrag anhand einer Literaturrecherche das Potenzial der Blockchain-Technologie zur Lösung des Vertrauensproblems in einer Sharing Economy. Sie stellen fest, dass das Konzept des Vertrauens zwischen der Blockchain-Technologie und der Sharing Economy erheblich variiert, die Blockchain-Technologie jedoch bis zu einem gewissen Grad geeignet ist, dass Vertrauen in Plattformanbieter zu ersetzen. Schütz et al. (2018) setzen ihren Fokus auf das Crowdsourcing und deren aktuellen Vertrauensprobleme und entwickeln ein Reputationssystem auf Basis der Blockchain-Technologie. Mit Hilfe von Smart Contracts auf der Ethereum Blockchain werden Profile von Auftraggebern und Arbeitnehmern mit einem Reputationsscore verknüpft, um dadurch die notwendige Vertrauensgrundlage für die Geschäftsbeziehung zu erreichen [44]. Bracamonte und Okada (2017) untersuchen in ihrem Beitrag das Thema Vertrauen und vertrauensbezogene Faktoren im Zusammenhang mit dezentralen Anwendungen, die auf öffentlichen Blockchain-Plattformen ausgeführt werden. Sie differenzieren Vertrauen in soziales und technologisches Vertrauen und analysieren, inwieweit diese Anwendungen als von Dritten nicht kontrollierbar angesehen werden. Ihre Ergebnisse zeigen, dass die Websites dezentraler Anwendungen zwar auf die Konzepte Dezentralisierung, Vertrauenswürdigkeit und Autonomie verweisen, diese jedoch nicht in gleicher Weise definieren [7]. Yang et al. (2019) entwickeln ein Vertrauensmodell mit Hilfe der Blockchain-Technologie und einem Proof-of-event Konsensmechanismus, um die Legitimität und das Verhalten anonymer Knoten in einem Fahrzeugnetz zum Austausch von Verkehrsinformationen zu bewerten. Für die Sicherstellung der Integrität von kryptografischen Authentifizierungsdaten in Sensornetzwerken schlagen Moinet et al. (2017) ein Blockchain-basiertes Protokoll zur Gewährleistung eines Peer-Trust Levels vor. Auf der Grundlage der Blockchain-Datenstruktur entwickeln sie ein Modell zur dezentralen Authentifizierung. Malik et al. (2019) sehen ein Vertrauensproblem hinsichtlich der Daten in einem Audit-Trail für Lieferkettenereignisse und die Lösung in einem Reputationssystem. Sie entwickeln ein dreistufiges Trust-Management-Framework auf der Grundlage einer Konsortium-Blockchain, um die Interaktionen zwischen den Lieferkettenteilnehmern zu verfolgen und dynamisch Vertrauens- und Reputationswerte zu generieren. Liu und Zou (2019) stellen die neuesten Forschungsergebnisse des Vertrauensmechanismus in einem Peer-to-Peer Netzwerk der Blockchain vor. Der Blockchain Vertrauensmechanismus basiert auf der Beteiligung aller Mitglieder an der Überwachung, Kontrolle und Prüfung des Vertrauenswertes für den gesamten Lebenszyklus von Adressen, Schlüsseln und Daten [31]. Der Beitrag von Iqbal et al. (2019) stellt die Schlüsselfaktoren für die Konzeptionierung eines Vertrauensmodells für „…social Internet of vehicles“ (SIoV) vor. Diese sind Reputation, Kontext, Umfeld, Ziele, Nutzererwartungen, soziale Beziehungen, Verbindungsbereitschaft und zeitnahe Bewertung. Sie zeigen in ihrem Beitrag, dass die Blockchain-Technologie zur Lösung der heute vorhandenen Probleme mit diesen Schlüsselfaktoren geeignet ist.

## 4. Ergebnisse

Die Analyse der Beiträge erfolgte auf der Grundlage eines ausführlichen Coding Handbuches, in dem sowohl die Vertrauensdomänen nach Heidt et al. (2019) sowie die systemimmanenten Vertrauenseigenschaften der Blockchain ausführlich und mit Beispielen dokumentiert wurden. Anhand dieses Coding Handbuches wurde zunächst der Abstract des Beitrags analysiert, und darüber hinaus bei Unklarheiten der gesamte Beitrag. Für jede in dem Beitrag angesprochene Vertrauensdomäne als auch Vertrauenseigenschaft der Blockchain wurde jeweils eine 1 notiert. Beispielsweise wird für den Beitrag „BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network“ von Rathore et al. (2019) eine 1 für die Vertrauenseigenschaft Integrität der Blockchain notiert, da die im Beitrag adressierte Lösung anhand der drei Kerntechnologien Software Defined Networking (SDN), Blockchain, Fog und Mobile Edge Computing die Gewährleistung der Integrität der Daten erreichen soll. Die durch den Beitrag angesprochene Vertrauensdomäne ist Vertrauen in Daten, hierfür wird ebenfalls eine 1 notiert.

Die nachfolgende Statistik (siehe Tabelle 5) zeigt das Ergebnis unserer Zuordnung der Beiträge zu den angesprochenen Vertrauensdomänen (siehe Kapitel 2.1) sowie den involvierten systemimmanenten Vertrauenseigenschaften der Blockchain (siehe Kapitel 2.2). Mit diesen Ergebnissen beantworten wir unsere Forschungsfragen FF1 und FF2.

Tabelle 5: Anzahl der Zuordnungen zu Vertrauensdomänen und Vertrauenseigenschaften

| *Vertrauensdomäne* | *Anzahl der Beiträge* | *Vertrauenseigenschaften der Blockchain* | *Anzahl der Beiträge* |
|---|---|---|---|
| Vertrauen in Code | 4 | Smart Contracts | 9 |
| Vertrauen in Daten | 12 | Konsensmechanismus | 6 |
| Vertrauen in die Vision | 0 | Unveränderlichkeit | 3 |
| Systemisches Vertrauen | 11 | Peer-to-Peer Netzwerk | 19 |
| Authentifizierung | 41 | Distributed Ledger | 34 |
| Autorisierung | 34 | Integrität | 10 |
| | | Kryptographie | 24 |

Die Summen übersteigen die Anzahl der Beiträge von 81, da Mehrfachzuordnungen möglich waren. Im Bereich der Vertrauensdomänen wird deutlich, dass der Fokus der Beiträge und der avisierten Lösungen hinsichtlich der Authentifizierung und Autorisierung liegt.

Singh et al. (2018) beschreiben in ihrem Beitrag das Problem einer sicheren Kommunikation für intelligente Fahrzeuge und sehen wie Guo et al. (2019) die Lösung in einer sicheren Authentifizierung mit Hilfe der Blockchain. Das Distributed Ledger Konzept der Blockchain-Technologie ist die dominierende Eigenschaft für die Bildung von Vertrauen, gefolgt von den Eigenschaften Kryptographie und dem Peer-to-Peer Netzwerk. Auffällig ist, dass im Kontext von Internet of Things die Unveränderlichkeit der Daten in einer Blockchain anscheinend für die Bildung von Vertrauen keine gravierende Rolle spielt. Ebenso scheint der Konsensmechanismus in diesem Kontext eine eher untergeordnete Rolle zu spielen.

### 4.1 Deskriptive Statistik und Clusteranalyse

Die Clusteranalyse ist eine Gruppe multivariater Techniken, deren Hauptzweck darin besteht, Objekte auf der Grundlage ihrer Eigenschaften zu gruppieren [19]. Nach Eckstein (2016) besteht die Grundidee einer Clusteranalyse darin, eine definierte Menge von Objekten so zu gruppieren, dass die Objekte innerhalb einer Gruppe möglichst homogen bezüglich der Menge der Clustermerkmale und die Objekte unterschiedlicher Gruppen möglichst heterogen bezüglich der Menge der Clustermerkmale sind. Die Verwendung der Clusteranalyse hat in den letzten Zeiträumen erheblich zugenommen und ist weit verbreitet [27].

Bevor wir die Clusteranalyse durchführen, untersuchen wir die Pearson-Korrelation zwischen unseren Merkmalen (siehe Tabelle 7). Die Ergebnisse lassen aufgrund ihres niedrigen Niveaus eine weitere Clusteranalyse zu. Hierfür nutzen wir IBM SPSS Version 24 und verwenden die hierarchisch-agglomerative Klassifikation des Ward-Verfahrens. Diese Varianz-Methode arbeitet mit dem kleinsten Zuwachs der Fehlerquadratsumme bei einer Clusterfusion [8]. Als Abstandsmaß in der Clusteranalyse wurde der quadratische euklidische Abstand gewählt, der für binäre Variablen verwendet werden kann. Für die Bestimmung der besten Anzahl an Clustern „gibt es keine „harten“ Regeln, die für eine statistisch und sachlogisch plausible Deutung der erzielten Ergebnisse hilfreich sind“ [8]. Daher haben wir zunächst mit Hilfe des Dendrogramms eine Bestimmung der Anzahl der Cluster durchgeführt. In einem weiteren Schritt haben wir die Entscheidungsregel von Eckstein (2016) angewandt. Dazu wird der Fusionsschritt gesucht, der sich durch eine übermäßige Steigerung des Heterogenitätskoeffizienten auszeichnet. Die optimale Anzahl der Cluster ist dann die Anzahl der Fusionsschritte gesamt abzüglich des Fusionsschritts mit der übermäßigen Steigerung des Heterogenitätskoeffizienten. In unserem Fall ergeben 78 Fusionsschritte abzüglich dem 75. Fusionsschritt, der eine übermäßige Steigerung des Heterogenitätskoeffizienten zeigt, 3 Cluster. Damit wird das Ergebnis von drei Clustern der visuellen Analyse des Dendrogramms bestätigt.

Tabelle 6: Ergebnis der Cluster-Analyse

| *Cluster* | *Frequency* | *Percent* | *Cumulative Percent* |
|---|---|---|---|
| 1 | 30 | 38,0 | 38,0 |
| 2 | 32 | 40,5 | 78,5 |
| 3 | 17 | 21,5 | 100,0 |
| Total | 79 | 100,0 | |

Die unterschiedlichen Cluster zeigen in Tabelle 8 die Muster der Komposition der Vertrauensdomänen mit den Vertrauenseigenschaften der Blockchain.

Tabelle 8: Vertrauenseigenschaften und –domänen je Cluster

| *Anzahl der Vertrauenseigenschaften der Blockchain sowie Vertrauensdomänen je Cluster* | *Cluster 1* | *Cluster 2* | *Cluster 3* |
|---|---|---|---|
| Smart Contracts | 8 | 0 | 1 |
| Konsensmechanismus | 6 | 0 | 0 |
| Unveränderlichkeit | 2 | 0 | 1 |
| Peer-to-Peer Netzwerk | 0 | 10 | 9 |
| Distributed Ledger | 4 | 14 | 16 |
| Integrität | 6 | 2 | 2 |
| Kryptographie | 6 | 18 | 0 |
| *Vertrauenseigenschaften der Blockchain - Teilsumme :* | 32 | 44 | 29 |
| Vertrauen in Code | 1 | 0 | 3 |
| Vertrauen in Daten | 12 | 0 | 0 |
| Vertrauen in die Vision | 0 | 0 | 0 |
| Systemisches Vertrauen | 7 | 0 | 4 |
| Authentifizierung | 3 | 29 | 9 |
| Autorisierung | 5 | 28 | 1 |
| *Vertrauensdomänen - Teilsumme :* | 28 | 57 | 17 |
| *Gesamtsumme:* | 60 | 101 | 46 |

Die Vertrauenseigenschaften Smart Contracts, Konsensmechanismus, Integrität und Kryptografie führen im Cluster 1 zu einer Aktivierung der Vertrauensdomänen „Vertrauen in Daten“ und „Systemisches Vertrauen“. Im Vergleich zu den anderen Clustern ist die Bedeutung von Smart Contracts, dem Konsensmechanismus sowie der Integrität hervorzuheben. Dies begründet sich darin, dass der Konsensmechanismus der Blockchain-Technologie dessen Inhalte vor Manipulationen schützt, und damit die Vertrauensdomäne „Vertrauen in Daten“ aktiviert. Mit Smart Contracts werden Sicherheit und Unparteilichkeit bei der Ausführung von vereinbarten Transaktionen gewährleistet. Die Blockchain gewährleistet sowohl die Ausführung dieser Transaktionen als auch deren Protokollierung und schafft somit Vertrauen. Die hierauf aufbauenden Geschäftsmodelle, wie zum Beispiel im Kontext von Industrie 4.0, enthalten als wesentliche technische Grundlage die Übertragung von Daten zwischen Kunden und Anbietern über das Internet [11]. Aufgrund der hohen Automatisierungen in diesen Geschäftsmodellen ist ein systemisches Vertrauen des Kunden unabdingbar. Sowohl der Konsensmechanismus als auch Smart Contracts schaffen hierfür die notwendigen Grundlagen.

Der Cluster 2 zeigt einen deutlichen Schwerpunkt bei den Vertrauenseigenschaften Peer-to-Peer Netzwerk, Distributed Ledger sowie Kryptographie, und

führt zu einer Fokussierung auf die Vertrauensdomäne Authentifizierung und Autorisierung. Dieses Muster der Vertrauensgenerierung spricht Geschäftsmodelle an, die die Vernetzung von cyber-physischen Systemen und Menschen wie zum Beispiel mit Konsumentenelektronik im Fokus haben [40]. Mit dem Peer-to-Peer Netzwerk der Blockchain wird die Vertrauenswürdigkeit jedes Teilnehmers erreicht, verbunden mit der Vermeidung eines Single-point of failure durch die Distributed Ledger Konzeptionierung. Der dezentrale und mobile Einsatz der Konsumentenelektronik erfordert darüber hinaus ein starkes Vertrauen sowohl in die Authentifizierung als auch in die Autorisierung der Benutzer.Dieses Vertrauen wird durch die Kryptographie innerhalb der Blockchain-Technologie erreicht.

Der Cluster 3 ist dominiert von der Vertrauenseigenschaft Distributed Ledger, die wiederum zu den Vertrauensdomänen Authentifizierung sowie Systemisches Vertrauen führt. Hervorzuheben ist die Differenzierung zu den vorangegangenen Clustern hinsichtlich des Vertrauens in Code und systemisches Vertrauen. Die auf diesen Eigenschaften basierenden Geschäftsmodellen sind so einzurichten, dass den Benutzern sowohl ein hohes Vertrauen zu den programmierten Anwendungen als auch zu der Plattform beziehungsweise dem System vermittelt wird. Die in diesem Kontext relevanten IoT-Anwendungen sind beispielsweise IoT-Apps im Bereich Home Automation.

### 4.2 Diskussion der Ergebnisse

In diesem Beitrag wurde der Wissensstand zum Vertrauen im Kontext von IoT im Zusammenspiel mit der Blockchain-Technologie dargelegt. Eine der wesentlichen Eigenschaften der Blockchain-Technologie ist die Fähigkeit, vertrauenslose Interaktionen zwischen Menschen und Technologien zu ermöglichen [12]. Basis dieser vertrauenslosen Interaktionen ist ein Konsensalgorithmus wie beispielsweise Proof-of-work, der für die Integrität der Daten in einer Blockchain sorgt [1]. Diese Vertrauenseigenschaften der Blockchain-Technologie ergeben zusammen mit den Vertrauensdomänen drei unterschiedliche Cluster (siehe Tabelle 6), die wir nachfolgend den Wertschöpfungsstufen einer IoT-Anwendung nach Fleisch et al. (2015) zuordnen. Mit dieser Zuordnung wird deutlich, auf welchen Ebenen der Wertschöpfungsstufe die Komposition aus Vertrauenseigenschaften der Blockchain und den Vertrauensdomänen eine Konfiguration der Elemente eines Geschäftsmodells darstellen. Der Cluster 1 beispielsweise ist der Ebene 4 Analytik zugeordnet, in der Daten von Sensoren gesammelt, gespeichert, plausibilisiert und klassifiziert werden [11]. Geschäftsmodelle in diesem Kontext schaffen Mehrwert für den Kunden durch die Verarbeitung von Daten und Gewinnung von Erkenntnissen aus diesen Daten. Die Blockchain-Technologie kann an dieser Stelle mit Hilfe der Smart Contracts und den Konsensmechanismen für ein hohes Vertrauen in die Daten sorgen und damit ein systemisches Vertrauen beim Kunden erzeugen.

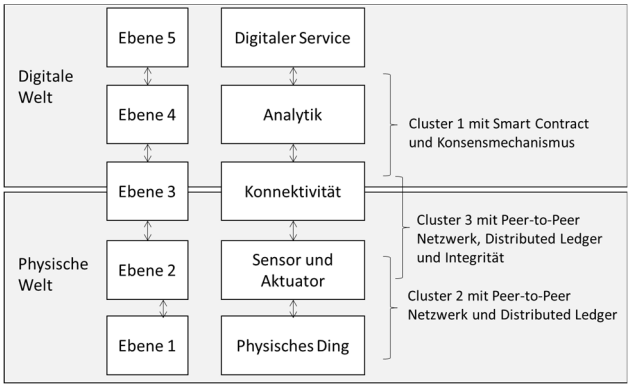


Bild 2: Wertschöpfungsstufen einer IoT-Anwendung [11]

Der Cluster 2 ist den physischen Ebenen 1 und 2 zugeordnet. Die Geschäftsmodelle mit dem Fokus auf diesen Ebenen streben die Digitalisierung von physischen Gegenständen an. Die Blockchain kann hierbei aufgrund ihres Peer-to-Peer Netzwerkes und der Distributed Ledger Technologie verbunden mit der Kryptographie für ein Vertrauen in die sichere Authentifizierung sowie Autorisierung dieser physischen Geräte sorgen. Die physische Ebene sowie die Verbindung zur digitalen Ebene ist die Zuordnung von Cluster 3, die mit Hilfe des Peer-to-Peer Netzwerkes und der Distributed Ledger Technologie die Grundlage für darauf basierende Geschäftsmodelle bietet. Diese Geschäftsmodelle benötigen neben einem hohen Vertrauen in die Authentifizierung ebenfalls ein Vertrauen sowohl in die programmierten Anwendungen als auch in das System. Eine sichere IT-Infrastruktur verbunden mit einer sicheren Konnektivität zu den Kunden schafft Vertrauen [17].

Die Ergebnisse aus unserer Cluster Analyse (siehe Tabelle 8) als auch die Einordnung der Cluster in die Wertschöpfungsstufen (siehe Bild 2) zeigen die Muster der Vertrauensgenerierung für IoT-basierte Geschäftsmodelle. Dieses Ergebnis beantwortet die Forschungsfrage FF3.

### 4.3 Mögliche Forschungsthemen

Die zuvor dargestellten Ergebnisse werfen ethische, rechtliche und soziale Fragestellungen (ELSI – Ethical, legal and social issues) auf und führen zu folgenden möglichen Forschungsthemen (siehe Tabelle 9).

Tabelle 9: Forschungsthemen nach ELSI-Dimensionen

| *ELSI Dimension* | *Relevante Forschungsthemen* |
|---|---|
| Ethische Implikationen | Die Autonomie der Entscheidung wird über das durch die Blockchain generierte Vertrauen im Kontext von IoT auf die Anwendung verlagert. Die Mensch-IoT-Blockchain-Interaktion führt aufgrund ihrer Komplexität zu einer enormen Anpassungsleistung für den Menschen. Zukünftige Forschungen sollten sich diesen Veränderungen und den Auswirkungen für den Menschen widmen (z.B. Autonomieverlust, Algorithmen-Ethik). |
| Rechtliche Implikationen | In 2018 sind mit Art. 16 DSGVO das Recht auf Berichtigung und mit Art. 17 DSGVO das Recht auf Löschung personenbezogener Daten in Kraft getreten. Hinsichtlich der personenbezogenen Daten auf einer Blockchain wird unterschieden |

| *ELSI Dimension* | *Relevante Forschungsthemen* |
|---|---|
| | in personenbezogene Daten gespeichert auf der Blockchain sowie öffentlichen Schlüsseln der Teilnehmer einer Blockchain. Wie können in einer öffentlichen und globalen Blockchain für IoT-Applikationen die Art. 16 und 17 der DSGVO eingehalten werden? Wie ist die Blockchain zu konzipieren, um einem Betroffenen das Recht auf Berichtigung und das Recht auf Löschung seiner Daten zu gewähren? |
| Soziale Implikationen | Die Generierung von Vertrauen im Kontext von IoT durch die Blockchain und deren Komplexität führt zu einer Verantwortungsdiffusion, in dem für den Menschen nicht mehr klar erkennbar ist, von wem und an welcher Stelle das notwendige Vertrauen stattgefunden hat. Die Zuordnung der Vertrauensgenerierung zu einer verantwortlichen Stelle ist nicht mehr gegeben. Die sich hieraus ergebenden Auswirkungen im Verhalten der Menschen mit IoT sollten analysiert werden sowie Handlungsfelder zur Problemlösung ermittelt werden. |

## 5. Limitationen und Ausblick

Die Generierung von (System-) Vertrauen im Kontext von IoT mit Hilfe der Blockchain-Technologie bleibt den Beweis einer verlässlichen Bewertung mangels einer verlässlichen Messung schuldig. Die Kernfrage, wie sich Vertrauen in der digitalen Welt verlässlich messen lässt, konnte mit diesem Beitrag nicht beantwortet werden. Sie stand allerdings auch nicht im Fokus unserer Analysen. Dennoch schafft die Blockchain-Technologie anhand ihrer systemimmanenten Vertrauenseigenschaften eine Grundlage zur Bildung von Vertrauen im Kontext von IoT. Die bisherigen Lösungen setzen auf zentrale Vertrauensinstanzen, die jedoch aufgrund der Vielzahl und Heterogenität der Geräte keinen verlässlichen und überzeugenden Schutz gegenüber Cyberkriminalität bieten können [15]. Die Distributed Ledger Technologie der Blockchain in einem Peer-to-Peer-Netzwerk hat das Potential zur Schaffung von Vertrauen im Kontext von IoT. Jedoch gilt zu bedenken, dass die komplexe Blockchain-Technologie in der Breite der Gesellschaft in Deutschland bisher eine unverstandene Technologie ist [39]. An dieser Stelle sind weitere Forschungen dahingehend notwendig, ob ein Vertrauen in eine technologische Lösung unabhängig vom Wissensstand über die Technologie generiert werden kann.

Neben den in Bild 1 dargestellten systemimmanenten Eigenschaften der Blockchain zur Generierung von Vertrauen im Kontext von IoT sind weitere Eigenschaften der Blockchain geeignet, das Vertrauen in dezentrale Anwendungsgebiete wie Logistik, Gesundheit oder Medizin zu erzielen. Die Blockchain findet in einer vernetzten Welt ihre Anwendungsmöglichkeiten, jedoch gibt es nicht die „eine“ Blockchain, sondern eine Vielzahl von Blockchain Varianten mit unterschiedlichen Anwendungsgebieten. An dieser Stelle sind weitere Forschungen hinsichtlich der unterschiedlichen Vertrauenseigenschaften sinnvoll.

## 6. Literatur


[1] Azaria, Asaph, Ekblaw, Ariel, Vieira, Thiago, Lippman, Andrew (2016), MedRec: Using Blockchain for Medical Data Access and Permission Management, in: 2016 2nd International Conference on Open and Big Data, DOI 10.1109/OBD.2016.11.

[2] Beck, Roman, Müller-Bloch, Christoph (2017), Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers, in: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2017).

[3] Benshoof, Brendan, Rosen Andrew, Bourgeois, Anu G., Harrison, Robert W. (2016), Distributed Decentralized Domain Name Service, in: 2016 IEEE International Parallel and Distributed Processing Symposium Workshops, DOI 10.1109/IPDPSW.2016.109 DOI 10.1109/IPDPSW.2016.109.

[4] Bitkom (2019), Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. 2019, abrufbar unter: https://www.bitkom.org/Bitkom/Publikationen/Blockchain-Deutschland-Einsatz-Potenziale-Herausforderungen, Stand: 19. Juli 2019.

[5] Bohn, Ursula (2007), Welchen Einfluss haben Reorganisationsmaßnahmen auf Vertrauensprozesse? Eine Fallstudie, Inaugural-Dissertation 2007, Ludwig-Maximilians-Universität München.

[6] Bordel, Borja, Alcarria, Ramon, Martin, Diego, Sanchez-Picot, Alvaro (2019), Trust Provision in the Internet of Things Using Transversal Blockchain Networks, in: Intelligent Automation and Soft Computing, Jahrgang 25, Ausgabe 1, S. 155-170.

[7] Bracamonte, Vanessa, Okada, Hitoshi (2017), The issue of user trust in decentralized applications running on blockchain platforms, in: 2017 IEEE International Symposium on Technology and Society (ISTAS), Sydney, NSW.

[8] Eckstein, Peter P. (2016), Angewandte Statistik mit SPSS. Praktische Einführung für Wirtschaftswissenschaftler, 8. Auflage, Springer-Gabler, Wiesbaden.

[9] Engelschall, Ralf S. (2019), Blockchain. Suchen wir nur das Problem zur Lösung?, in: Informatik Spektrum, Jahrgang 42, Ausgabe 3, S. 205–210.

[10] Fleich, Elgar, Weinberger, Markus, Wortmann, Felix (2014), Geschäftsmodelle im Internet der Dinge, in: HMD Praxis der Wirtschaftsinformatik, Jahrgang 51, Ausgabe 6, S. 812-826.

[11] Fleisch, Elgar, Weinberger, Markus, Wortmann, Felix (2015), Geschäftsmodelle im Internet der Dinge, in: Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung, Jahrgang 67, S. 444-464.

[12] Foroglou, Georgios, Tsilidou, Anna Lali (2015), Further applications of the blockchain, Conference Paper, in: Proceedings of the 12th Student Conference on Managerial Science and

Technology, Athens, Greece.
[13] Frauchiger, Daniel (2017), Anwendungen von Design Science Research in der Praxis, In: Portmann, Edy (Eds.) Wirtschaftsinformatik in Theorie und Praxis, Festschrift zu Ehren von Prof. Dr. Andreas Meier, Springer Fachmedien, Wiesbaden 2017.
[14] Glaser, Florian (2017), Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis, in: Proceedings of the 50th Hawaii International Conference on System Sciences 2017.
[15] Goncalves, Nicholas (2018), Can decentralised networks influence the level of digital trust in eCommerce sites? DOI: 10.13140/RG.2.2.21778.71364.
[16] Green, Charles H. (2019), Trust and the Sharing Economy: A New Business Model, abrufbar unter: https://trustedadvisor.com/trust-and-the-sharing-economy-a-new-business-model, Stand: 18. November 2019.
[17] Grünert, Lars, Sejdic, Goran (2017), Industrie 4.0-getriebene Geschäftsmodellinnovationen im Maschinenbau am Beispiel von TRUMPF, In: Seiter, Mischa, Grünert, Lars, Berlin, Sebastian (Hrsg.), Betriebswirtschaftliche Aspekte von Industrie 4.0, ZfbF-Sonderheft 71.17, Springer-Gabler.
[18] Guo, Shaoyong., Hu, Xing, Zhou, Ziqiang, Wang, Xinyan et al. (2019), Trust access authentication in vehicular network based on blockchain, in: China Communications, Jahrgang 16, Ausgabe 6, Juni 2019.
[19] Hair, Joseph F., Black, William C., Babin, Barry J., Anderson, Roph E. (2014), Multivariate Data Analysis, 7. Auflage, Pearson Education Limited.
[20] Hammi, Mohamed Tahar, Hammi, Badis, Bellot, Patrick, Serhrouchni, Ahmed (2018), Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, in: Computers & Security, Jahrgang 78, S. 126-142.
[21] Hawlitscheka, Florian, Notheisena, Benedikt, Teubnerb, Timm (2018), The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy, in: Electronic Commerce Research and Applications, Jahrgang 29, S. 50-63.
[22] Heidt, Michael, Berger, Arne, Bischof, Andreas (2019), Blockchain and Trust: A Practice-Based Inquiry, In: Nah, Fiona Fui-Hoon, Siau, Keng (Hrsg.), HCI in Business, Government and Organizations. eCommerce and Consumer Behavior, HCII 2019, Lecture Notes in Computer Science, Springer.
[23] Hörler, Salomon (2015), Vertrauen im Zeitalter der digitalen Moderne. Ein Mechanismus der Reduktion digitaler Komplexität, abrufbar unter: http://www.effibeisst.com/portfolio_page/vertrauen-im-zeitalter-der-digitalen-moderne/, Stand: 14. November 2019. 14.11.2019)
[24] Huber, Daniel, Kaiser, Thomas (2015), Wie das Internet der Dinge neue Geschäftsmodelle ermöglicht, in: HMD Praxis der Wirtschaftsinformatik, Oktober 2015, Heft 52, Ausgabe 5, S. 681-689.
[25] Idelberger, Florian, Governatori, Guido, Riveret, Regis, Sartor, Giovanni (2016), Evaluation of Logic-Based Smart Contracts for Blockchain Systems, in: Conference Paper, July 2016, DOI: 10.1007/978-3-319-42019-611.
[26] Iqbal, Razi, Butt, Talal Ashraf, Afzaal, Muhammad, Salah, Khaled (2019), Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions, in: International Journal of Distributed Sensor Networks, Jahrgang 15, Ausgabe 1, DOI: 10.1177/1550147719825820.
[27] Kettenring, Joan R. (2006), The Practice of Cluster Analysis, Journal of Classification, Jahrgang 23, S. 3–30.
[28] Kratz, Hans-Jürgen (2017), Erfolgreich führen von A-Z. Für gute Vorgesetzte und zufriedene Mitarbeiter, Metropolitan, Regensburg 2017.
[29] Lewin, Marcus, Dogan, Alaettin, Schwarz, Jonas, Fay, Alexander (2019), Distributed-Ledger-Technologien und Industrie 4.0. Eine Untersuchung der Relevanz für Industrie 4.0, in: Informatik Spektrum, Band 42, Heft 3, Juni 2019. Seite 166-173.
[30] Linnhoff-Popien, Claudia (2018), 1. Internet of Things (IoT), in: Digitale Welt, Jahrgang 3, https://doi.org/10.1007/s42354-018-0102-6.
[31] Liu, Qi, Zou, Xiao (2019), Research on trust mechanism of cooperation innovation with big data processing based on blockchain, in: Journal on Wireless Communications and Networking, https://doi.org/10.1186/s13638-019-1340-5.
[32] Luber, S., Schmitz, P. (2019), Was ist Authentifizierung? abrufbar unter: https://www.security-insider.de/was-ist-authentifizierung-a-617991/, Stand: 18. Juli 2019.
[33] Malik, Sidra, Dedeoglu, Volkan, Kanhere, Salil S., Jurdak, Raja (2019), TrustChain: Trust Management in Blockchain and IoT supported Supply Chains, in: IEEE Blockchain 2019, arXiv:1906.01831 [cs.CR].
[34] Mkpa, Akpanakak, Chin, Jeannette, Winckles, Adrian (2019), Holistic Blockchain Approach to Foster Trust, Privacy and Security in IoT based Ambient Assisted Living Environment, abrufbar unter: https://www.researchgate.net/publication/333132719_Holistic_Blockchain_Approach_to_Foster_Trust_Privacy_and_Security_in_IoT_based_Ambient_Assisted_Living_Environment, Stand: 19. Juli 2019.
[35] Möllering, Guido (2019), Grundlagen des Vertrauens: Wissenschaftliche Fundierung eines Alltagsproblems, abrufbar unter: https://www.mpg.de/451610/forschungsSchwerpunkt, Stand: 16. Juli 2019.
[36] Moinet, Axel, Darties, Benoît, Baril, Jean-Luc (2017), Blockchain based trust & authentication for decentralized sensor networks, in: IEEE Security & Privacy, Special Issue on Blockchain, arXiv:1706.01730 [cs.CR].

[37] Naerland, Kristoffer, Müller-Bloch, Christoph, Beck, Roman, Palmund, Søren (2017), Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments, in: Proceedings ICIS 2017.

[38] Pietro, Robert Di, Salleras, Xavier, Signorini, Matteo, Waisbard, Erez (2018), A blockchain-based distributed Trust System for the Internet of Things, SACMAT'18, Juni 13-15, 2018, Indianapolis.

[39] Pwc (2016), Privatkundengeschäft der Zukunft. Juli 2016, abrufbar unter: https://www.pwc.de/de/finanzdienstleistungen/digital/pwc-befragung-privatkundengeschaeft der-zukunft.pdf, Stand: 19. Juli 2019.

[40] Ranz, Fabian, Guldin, Marc (2018), Geschäftsmodelle für die Industrie 4.0, Erfolgsfaktoren, Hindernisse und Anwendungsbeispiele, abrufbar unter: https://www.esb-business-school.de/fileadmin/user_upload/Fakultaet_ESB/Forschung/Wertschoepfungs-_und_Logistiksysteme/ESB_Business_School_GENI40_Studie_Geschaeftsmodelle_fuer_die_Industrie_40.pdf, Stand: 19. November 2019.

[41] Rodig, Jan (2017), Erfolgreiche IoT-Geschäftsmodelle, Chancen im Internet der Dinge und der Industrie 4.0 nutzen, abrufbar unter: http://fs-media.nmm.de/ftp/ITI/ITP/files/vortraege/2017/jan-rodig-tresmo.pdf, Stand: 18. November 2019.

[42] saïd Business school (2019), rebuilding trust in Business, A collaborative research project between DLA Piper, the Oxford University Centre for Corporate reputation, saïd Business school, University of Oxford; and Populus, abrufbar unter: https://www.sbs.ox.ac.uk/sites/default/files/2019-04/Rebuildingtrustinbusiness.pdf, Stand: 18. November 2019.

[43] Schubert, Manuel (2014), Vertrauensmessung in der digitalen Welt. Übersicht und Ausblick, DIVSI Diskussionsbeiträge 06, 2014, ISSN 2196-6729.

[44] Schütz, Andreas E., Fertig, Tobias, Weber, Kristin et al. (2018), Vertrauen ist gut, Blockchain ist besser – Einsatzmöglichkeiten von Blockchain für Vertrauensprobleme im Crowdsourcing, in: HMD Praxis der Wirtschaftsinformatik, Jahrgang 55, Ausgabe 6, S. 1155-1166.

[45] Schwabe, Gerhard (2017), Blockchain-Enhanced Trust in International Trade, In: Beck, Roman, Becker, Christian, Lindman, Juho, Rossi, Matti (Hrsg.), Opportunities and Risks of Blockchain Technologies, Report from Dagstuhl Seminar 17132. 2017, 10.4230/DagRep.7.3.99.

[46] Schwarzkopf, Julia, Adam, Katarina, Wittenberg, Stefan (2018), Vertrauen in nachhaltigkeitsorientierte Audits und in Transparenz von Lieferketten – Schafft die BlockchainTechnologie einen Mehrwert? In: Khare, Anshuman, Kessler, Dagmar, Wirsam, Jan (Hrsg.), Marktorientiertes Produkt- und Produktionsmanagement in digitalen Umwelten, Festgabe für Klaus Bellmann zum 75. Geburtstag, SpringerGabler, S. 171-180.

[47] She, Wei, Liu, Qi, Tian, Zhao, Chen, Jian-Sen, Wang, Bo, Liu, Wei (2019), Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks, in: IEEE ACCESS, Jahrgang 7, S. 38947-38956-

[48] Singh, Madhusudan, Kim, Shiho (2018), Trust Bit: Reward-based intelligent vehicle comminationation using blockchain paper, in: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT).

[49] Suchanek, Andreas (2019), Vertrauen, abrufbar unter: https://wirtschaftslexikon.gabler.de/definition/vertrauen-50461, Stand: 16. Juli 2019.

[50] Söllner, Matthias, Benbasat, Izak, Gefen, David, Leimeister, Jan Marco, Pavlou, Paul A. (2016), Trust, An MIS Quarterly Research Curation, MISQ Research Curation, abrufbar unter: https://misqresearchcurations.files.wordpress.com/2016/10/trust-research-curation_oct-31-20161.pdf, Stand: 21. November 2019.

[51] Son Jai-Yeol, Tu Lingling, Benbasat Izak (2006), A descriptive content analysis of trust-building measures in B2B electronic marketplaces, in: Communications of the Association for Information Systems, Jahrgang 18, https://doi.org/10.17705/1CAIS.01806.

[52] Treiblmaier, Horst, Önder, Irem (2018), 1. The Impact of Blockchain on the Tourism Industry: A Theory-Based Research Framework, In: Treiblmaier, Horst, Beck, Roman (Hrsg.), Business Transformation through Blockchain, Volume II, palgrave macmillan.

[53] Walterbusch, Marc, Teuteberg, Frank, Gräuler, Matthias (2014), How Trust is Defined: A Qualitative and Quantitative Analysis of Scientific Literature, AMCIS 2014.

[54] Yang, Yao-Tsung, Chou, Li-Der, Tseng, Chia-Wei, Tseng, Fan-Hsun, Liu, Chien-Chang (2019), Blockchain-Based Traffic Event Validation and Trust Verification for VANETs, in: IEEE Access, Jahrgang 7, DOI: 10.1109/ACCESS.2019.2903202.