Tim Zobjack

B. Sc. (2020), ist Absolvent der Berufsakademie Sachsen, Staatliche Studienakademie Dresden. Mittlerweile arbeitet er und entwickelt seine Karriere bei Integration Experts (Hann & Kropp Consulting GmbH & Co.KG) in Dresden.

Interessengebiete:

- IoT und angewandte Datensicherheit
- Softwaretechnik und -integration
- BWL und internationale WiWi.

KONTAKT: Tim.Zobjack@integration-experts.de

Prof. Dr. habil. Andriy Luntovskyy

ist Professor an der Berufsakademie Sachsen, Staatliche Studienakademie Dresden seit 2008. Im Zeitraum 2001 bis 2008 arbeitete Andriy Luntovskyy als wiss. Mitarbeiter und PostDoc am Lehrstuhl Rechnernetze an der Technischen Universität Dresden. Seine „Alma Mater“ ist die Technische Universität Kiew „Igor Sikorsky KPI“ (Abschluss 1989).

Interessen-/Lehrgebiete:

- Rechnernetze und mobile Kommunikation
- Verteilte Systeme und angewandte Datensicherheit
- Softwaretechnik und Betriebssysteme
- Grundlagen der Programmierung in C/C++ und Java
- Grundlagen der Informatik

KONTAKT: andriy.luntovskyy@ba-sachsen.de

Blockchained IoT: Verbindlichkeit in der dezentralisierten Welt smarter Dinge

Tim Zobjack | Andriy Luntovskyy

Blockchained IoT trägt zur Verbindlichkeit in der dezentralisierten Welt smarter Dinge bei. Sichere und in der Blockchain genutzte IoT-Geräte können nur unter Hinzunahme und Kombination bekannter Krypto-Technologien erreicht werden. Etwas weiter gedacht kann die schrittweise Bereitstellung von Blockchain dabei helfen angestrebte Schutzziele zu erreichen.

Blockchained IoT contributes to compulsoriness in the decentralized world of smart things. Secure IoT devices used in the blockchain can only be achieved by adding and combining well-known crypto technologies. More broadly speaking, the gradual deployment of block chain can help achieve the intended protective goals.

Motivation

Das „Internet der Dinge“ oder „Internet of Things“ (IoT) unterliegt seit seiner ersten Erwähnung durch Ashton im Jahr 1999 einer stetigen Entwicklung und ist heute nahezu überall im täglichen Leben wiederzufinden. Dabei reicht die Bandweite von internetfähigen Haushaltsgeräten, die sich zentral steuern und überwachen lassen, über medizinische Geräte, die den persönlichen Zustand überwachen, bis hin zur Überwachung ganzer Maschinenparks und Produktionsstraßen in der Industrie. Das alles wurde erst durch die rasante Technologieentwicklung der letzten Jahrzehnte möglich, vor allem im Bereich der Mikroelektronik und der Kommunikationstechnik. Die stetige Miniaturisierung bei gleichzeitiger Leistungssteigerung eröffnet immer wieder neue Einsatzmöglichkeiten für IoT [1-9].

Neben der Einzelnutzung können IoT-Geräte auch in Netzwerken betrieben werden. Durch deren Verknüpfung über dedizierte Plattformen ergibt sich die Möglichkeit der Sammlung und Auswertung teils großer Datenmengen. Diese können als Grundlage für Prognosen, maschinelles Lernen sowie den Einsatz von künstlicher Intelligenz dienen und unterstützten im Allgemeinen einen kontinuierlichen Verbesserungsprozess.

Dementsprechend versuchen viele Unternehmen, diese Technologien in die bestehenden Geschäftsprozesse einzubinden. Problematisch wird es allerdings bei der unternehmensübergreifenden Nutzung solcher Geräte, zum Beispiel im Zuge von Lieferketten. Bereitstellung von und Verantwortlichkeit für Daten kann schnell unübersichtlich werden. Allgemein ist die Einhaltung und Garantie von wichtigen Schutzzielen, allen voran Vertraulichkeit, Verfügbarkeit und Integrität der Daten in solchen Kooperationen ein Problem.

Eine mögliche Lösung bietet die Nutzung der Blockchain-Technologie [10-17]. Durch ihren Einsatz entfällt die Notwendigkeit für eine zentrale Datenverwaltung und -verarbeitung. Alle Teilnehmer haben zu jeder Zeit vollen Zugriff auf die Daten. Eine Manipulation bestehender Datensätze ist so gut wie ausgeschlossen. Somit können die besagten Schutzziele eingehalten werden. Ein genauerer Einblick in die Technologien folgt in den nächsten Abschnitten.

Die Technologie hinter IoT

Im Allgemeinen kann ein physikalisches System mit IT-Komponenten innerhalb eines verteilten Netzwerks als IoT bezeichnet werden. Das umfasst eingebettete Sensoren, RFID/NFC, Roboter, Computer, Smartphones, Tablets und andere intelligente Geräte, die Algorithmen zur Verarbeitung oder Analyse von Interaktion zwischen physikalischen Objekten bereitstellen [6-9]. Diese Systeme oder „smarte Dinge“ sind in bestimmten Einsatzszenarien datenschutz- und datensicherheitskritisch und müssen abgesichert werden [1,2, 6-8,11,26]. IoT-Geräte können selbstständig Daten erzeugen, teilweise verarbeiten und weiterleiten. Sie unterstützen damit die konventionelle verteilte IT und drahtlose Sensornetzwerke. Typische Komponenten eines IoT-Geräts können der folgenden Abbildung 1 entnommen werden.

Die Geräte sind im Grunde sehr einfach aufgebaut und besitzen nur wenige Bestandteile. Sensoren nehmen Umgebungszustände auf,

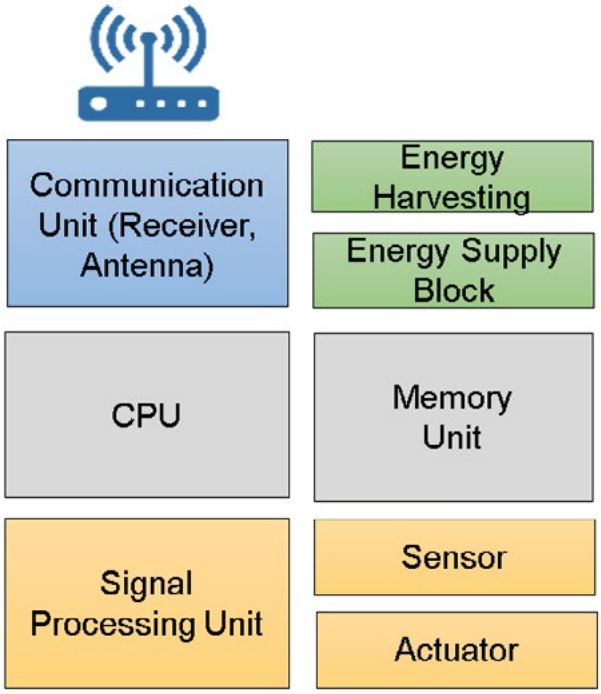

Abb. 1: Architektur und typische Komponenten eines IoT-Geräts

zum Beispiel Temperatur, Lichtintensität, Staubbelastung, Schwingungen usw. Aktoren setzen gegebene Befehle um, öffnen oder schließen beispielsweise ein Ventil. Die Recheneinheit ist für die Umwandlung und teilweise Verarbeitung von Sensordaten verantwortlich, unterstützt wird sie dabei von der Signalverarbeitung, die eingehende Sensorwerte entrauscht oder verstärkt. Eine Speichereinheit ist optional vorhanden und erlaubt das Zwischenspeichern von Daten. Die Energieversorgung ist ein weiterer wichtiger Bestandteil. Je nach Einsatzort und -art des IoT-Gerätes kann ein Batterie- oder Akkubetrieb notwendig sein oder die Energieversorgung erfolgt über Solar- und Windenergie oder Wasserkraft. Das Kommunikationsmodul sorgt für die Anbindung des Gerätes an ein Netzwerk.

IoT-Geräte werden meist, je nach Einsatzort und -zweck, autonom betrieben, ohne die Notwendigkeit externer Steuerung. Sie arbeiten für gewöhnlich aperiodisch, das heißt es werden konstant Daten aufgenommen, aber nur dann versendet, wenn eine Änderung vorliegt. Das ist notwendig, damit im Betrieb möglichst wenig Bandbreite und Energie verwendet wird. Wie bereits erwähnt können IoT-Geräte auf Batterien angewiesen sein, die nur begrenzte Kapazität haben. Weiterhin ist es denkbar, dass nicht zu jeder Zeit eine Datenverbindung besteht oder die Bandbreite allgemein nur sehr beschränkt ist. Trotz ihrer autonomen Funktionsweise besitzen IoT-Geräte meist nur sehr begrenzte Möglichkeiten zur Datenverarbeitung. Diese findet für gewöhnlich auf innerhalb des Netzwerks vorhandenen Plattformen statt.

Aufgrund der großen Bandbreite an Einsatzszenarien gibt es eine ebenso große Anzahl an Verbindungsmöglichkeiten und Kommu-

nikationsprotokollen. Die nachfolgende Abbildung 2 gibt dazu eine kurze Übersicht.

Für die Verwaltung und Datenverarbeitung von IoT-Geräten gibt es

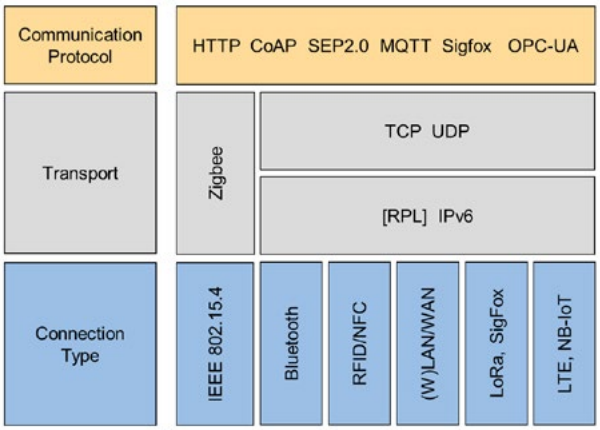

Abb. 2: Verbindungsarten und Kommunikationsprotokolle von IoT-Geräten

mittlerweile eine große Anzahl an Plattformen namenhafter Softwarehersteller. Zu nennen sind hier unter anderen:

- IBM Watson IoT Platform
- Microsoft Azure IoT Hub
- Google Cloud IoT
- Amazon AWS IoT
- SAP Internet of Things, SAP Leonardo IoT, SAP Edge Service.

Die Technologie der Blockchain

Bekannt wurde der Name durch das Whitepaper für Bitcoin aus dem Jahre 2008 durch den unbekannten Autor Satoshi Nakamoto. Die zugrundeliegende Technik wurde allerdings schon wesentlich früher beschrieben. Konkret basiert die Blockchain auf der Distributed Ledger Technologie. Der Grundgedanke dahinter ist, ein Kontenbuch nicht mehr zentral, sondern verteilt über mehrere Teilnehmer zu betreiben. Die Vorteile sind eine erhöhte Sicherheit gegen Manipulation durch die Verteilung und Redundanz des Datenbestands und die leichtere Zugänglichkeit für die einzelnen Teilnehmer [18-26].

Bei der Blockchain handelt es sich ebenfalls um ein dezentrales Netzwerk, in dem jeder Teilnehmer einen eigenen Knoten bildet. Diese besitzen jeweils den kompletten Datenbestand der Blockchain. Diese Redundanz macht den Inhalt des Netzwerks weniger anfällig gegen externe Einflüsse oder den Ausfall von einzelnen Knoten. Innerhalb der Blockchain finden Transaktionen direkt unter den einzelnen Teilnehmern statt, ähnlich einem Peer-to-Peer Netzwerk. Der Inhalt dieser Nachrichten kann dabei je nach Art der Blockchain [12] unterschiedlichen Charakter haben, vom einfachen Informationsaustausch, über das Versenden monetärer Güter zum Beispiel in Form einer Kryptowährung, bis hin zu ganzen Dokumenten.

Die Transaktionen werden grundsätzlich in Blöcken zusammengefasst. Die detaillierte Struktur eines solchen Blocks ist in nachfolgender Abbildung 3 aufgezeigt.

Das zentrale Element einer Blockchain ist der Block. Er enthält die Transaktionen, die zwischen den Teilnehmern des Peer-to-Peer-Netzwerks getätigt werden. Auf Grundlage der Distributed Ledger Technologie werden die Transaktionen dabei in chronologischer Reihenfolge gespeichert. Ist die maximale Anzahl an Transaktionen für einen Block erreicht, wird dieser geschlossen und der Nächste gestartet. Die Blockgröße variiert dabei zwischen den einzelnen Blockchain-Technologien. Neben den Transaktionen enthält ein Block einen sogenannten Header-Bereich, in dem weitere blockspezifische Attribute gespeichert sind. Dazu gehören unter anderen die Blocknummer, ein Zeitstempel, der Hashwert des Vorgängerblocks und je nach Technologie noch ein Muster und eine Nonce[1]. Ist der Block vollständig, wird für ihn ein einzigartiger Schlüsselwert (Hash) aus den Transaktionen und den Header-Attributen erstellt. Dieser Hash dient der Validierung und wird im nachfolgenden Block als Header-Attribut wiederverwendet. Damit findet eine Verkettung statt, die Hashwerte der einzelnen Blöcke sind voneinander abhängig.

Die Schlüsselwerte eines Blockes, also der Hash des Vorgängerblocks, der Hash der Transaktionen und der daraus erzeugte Block-

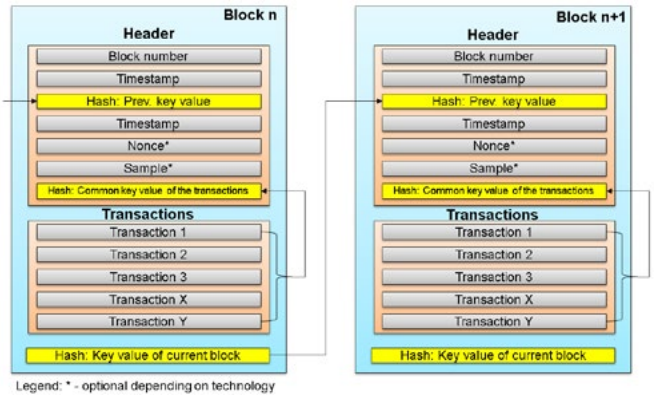

Abb. 3: Detaillierte Darstellung der Bestandteile eines Blocks innerhalb der Blockchain

Hash werden gemeinhin nach SHA-256 und NIST als Hashwerte bezeichnet. Der zugrundeliegende Algorithmus erzeugt aus einem Input beliebiger Größe und Form einen Output, den Hashwert, der eine feste Länge und Form besitzt. Die Erzeugung ist dabei unidirektional, das heißt aus dem Hashwert können keine Rückschlüsse auf den Inhalt des Inputs gezogen werden

Hash- und Signaturalgorithmen, zum Beispiel SHA-256 und RSA, werden neben der Blockverkettung häufig auch für die Authentifizierung und integrierte Verifikation innerhalb von Transaktionen genutzt, wie in Abbildung 4 dargestellt.

1 *Das Muster gibt in diesem Fall das Aussehen des Hashwerts vor, zum Beispiel die Anzahl führender Nullen. Die Nonce ist eine einzigartige Nummer die solange durchprobiert wird, bis ein entsprechender Hash gefunden wird.*

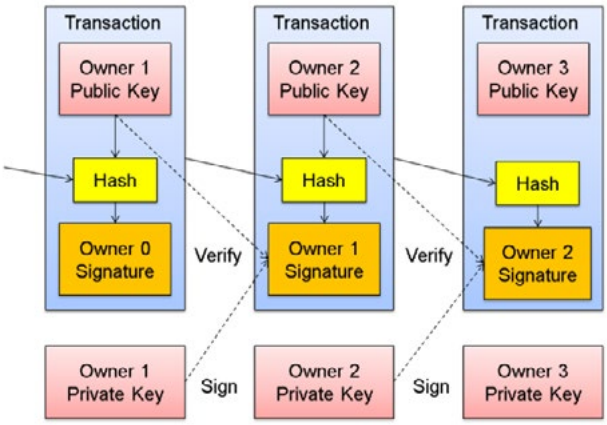

Abb. 4: Nutzung von Hash- und Verschlüsselungsalgorithmen für Transaktionen

Für die Erstellung von Blöcken gibt es mehrere sogenannte Konsensalgorithmen, die wichtigsten werden in nachfolgender Tabelle 1 aufgeführt.

Name	Beschreibung	Nachteile	Beispiele
Proof-of-Work	Teilnehmer (Miner) stellen ihre Rechenleistung gegen Entlohnung zur Verfügung, um die Hashwerte neuer Blöcke zu errechnen. Die Schwierigkeit der Errechnung wird so angepasst, dass Blöcke in regelmäßigen Zeitabständen erstellt werden.	Sehr rechen- und energieaufwändig	Bitcoin
Proof-of-Authority	Nur bestimmte Knoten innerhalb des Netzwerks können Blöcke erstellen. Reihenbasierte Auswahl.	Anfälliger gegen Manipulation	Hyperledger Fabric, Ripple
Proof-of-Stake	Teilnehmer besitzen Kryptowährung eines Netzwerks. Je höher der Anteil, desto wahrscheinlicher ist die Wahl zum Erstellen eines Blocks gegen Entlohnung.	Kapitalanhäufung kann andere Teilnehmer abschrecken	Stratis, Reddcoin

Tab. 1: Konsensalgorithmen für die Blockerstellung in der Blockchain

Blockchains können allgemein in zwei verschiedene Typen unterteilt werden. Die offenen Blockchains sind prinzipiell für jeden zugänglich, wobei hier noch unterschieden wird in:

- ein komplett offener Zugang, zum Beispiel Bitcoin.
- ein beschränkter Zugang, bei dem sich der Teilnehmer zunächst anmelden muss, zum Beispiel Sovrin.

Auf der anderen Seite gibt es die geschlossenen Blockchains. Diese sind meist Konsortium geführt und haben wesentlich weniger Teilnehmer als die offenen Vertreter. Der Zugang in das Netzwerk erfolgt hier nur nach ausdrücklicher Einladung. Besonders häufig findet man diese Art der Blockchain in der unternehmensübergreifenden Zusammenarbeit. Es gibt auch komplett private Netzwerke, die vor allem innerhalb eines Konzerns eingesetzt werden, allerdings entspricht diese Nutzungsart nicht dem Grundgedanken der Blockchain [17].
Zusammenfassend ergibt sich eine Reihe von Vorteilen aber auch Nachteilen gegenüber herkömmlichen Datenbanken, dargestellt in nachfolgender Tabelle 2.

Vorteile	Nachteile
Durch die redundante Speicherung des Blockchain-Inhaltes und den unbeschränkten Zugriff durch die einzelnen Teilnehmer ergibt sich eine maximale Transparenz.	Die bekannte ACID-Semantik von Datenbanken kann nicht eingehalten werden. Atomarität ist durch stark beschränkte Rollback-Funktion kaum möglich. Konsistenz ist durch die simultane Blockerstellung nicht immer gegeben.
Durch die Verkettung der Blöcke über Hashwerte und die Verteilung im Netzwerk sind die Daten der Blockchain besonders fälschungssicher	Die Erstellung von Blöcken ist besonders in den offenen Blockchains mit einem sehr hohen Rechen- und Energieaufwand verbunden.
Durch direkte Transaktionen und die gegebene Transparenz sind bisher notwenige Intermediäre überflüssig	Durch das permanente Speichern von Daten in der Blockchain ist nachträgliches Löschen nicht möglich. Das könnte zu Problemen in Verbindung mit der DSGVO führen.
Transaktionen in der Blockchain können beliebige Inhalte besitzen und es können Programme und Verträge innerhalb des Netzwerks hinterlegt werden	Der sinnvolle Einsatz einer Blockchain unterliegt gewissen Einschränkungen. Das betrifft die Teilnehmeranzahl, die Art der auszutauschenden Daten, dem Vertrauen untereinander und verfügbare Drittparteien.

Tabelle 2: Vor- und Nachteile der Blockchain gegenüber Datenbanken

Blockchained IoT

In der unternehmensübergreifenden Zusammenarbeit kann die gemeinsame Nutzung von IoT-Daten schnell zum Problem werden. Eine Kooperation zwischen Unternehmen bedeutet nicht immer, dass auch ein gegenseitiges Vertrauen vorhanden ist. Gerade bei langen Lieferketten mit vielen Akteuren sind damit wiederholte Warenüberprüfungen notwendig, um geforderte Qualität sicherzustellen. Gegen Umwelteinflüsse empfindliche Ware muss konstant von Sensoren überwacht werden, deren Dokumentation und Protokollierung findet aber selten über die Unternehmensgrenzen hinweg statt oder wird an eine außenstehende Drittpartei abgegeben.

Durch den Einsatz einer Blockchain entlang einer Lieferkette bietet sich die Möglichkeit, den Warenzustand entlang der gesamten Wertschöpfungskette lückenlos zu verfolgen. Damit können die bereits am Anfang angesprochenen Schutzziele erreicht werden:

1. Integrität: Aufgenommene Sensorwerte von IoT-Geräten werden in Echtzeit in der Blockchain gespeichert und sind dort permanent und fälschungssicher abgelegt.
2. Verfügbarkeit: Jedes Unternehmen in der Wertschöpfungskette betreibt einen eigenen Knoten im Blockchain-Netzwerk und hat damit jederzeit Zugriff auf die aktuelle und komplette Blockchain. Damit können Probleme entlang der Lieferkette sofort erkannt werden.
3. Vertraulichkeit: Unternehmensübergreifende Blockchains sind für gewöhnlich geschlossene Systeme, zu denen nur eingeladene Parteien Zugriff haben. Weiterhin bietet sich die Möglichkeit, zusätzlich eine Verschlüsselung für die Transaktionen zu verwenden, zum Beispiel das Public-Key-Verfahren. Auch können in der Blockchain Programme zur Regelung der Sichtbarkeit hinterlegt werden, so dass jedes Unternehmen innerhalb der Lieferkette nur die Informationen sieht, die notwendig sind.
4. Authentizität und Zurechenbarkeit: Ein weiterer wichtiger Aspekt ist, dass zu jedem Zeitpunkt eindeutig ermittelbar ist, welcher Teilnehmer für die geschriebenen Daten verantwortlich ist. Auch hier bietet die Blockchain mit dem Einsatz des Public-Key-Verfahrens eine Lösung an.

Es zeigt sich also, dass die Blockchain in diesen Szenarien eine tatsächliche Alternative zu etablierten Technologien darstellt. Die unternehmensübergreifende Zusammenarbeit erfüllt auch alle Anforderungen an den Einsatz einer Blockchain [1, 17]:

- Mehrere Teilnehmer vorhanden
- Zustände müssen gespeichert werden
- Eine Drittpartei ist nicht ständig verfügbar
- Alle Teilnehmer sind bekannt, aber ihnen wird nicht vertraut.

Gegen den Einsatz einer Blockchain-Lösung spricht aktuell noch die geringe Bekanntheit der Technologie. Für den übergreifenden Einsatz gibt es bisher noch kaum Plattformen [12-25], die eine ganzheitliche und einfache Lösung zur Anbindung von Unternehmen bieten. Somit dürfte es aktuell noch schwierig sein, Kooperationspartner von der Technologie zu überzeugen. Auch ist die initiale Einrichtung zur Anbindung mehrerer Teilnehmer noch recht aufwändig.

Schlussfolgerung und Evaluation zur Kopplung von IoT und

Blockchain

1. Ausgehend von Statistiken und Prognosen führender Beratungsfirmen, zum Beispiel Gartner, ist festzustellen, dass die Themen IoT und Blockchain in den letzten Jahren intensiver Forschung unterlagen. Viele IT-Firmen haben dazu eigene Pilotprojekte gestartet, um neue Möglichkeiten für das digitale Zeitalter zu testen.
2. Diese Arbeit befasst sich mit den Architekturen, Protokollen und Plattformen für IoT-Geräte und mit den wichtigen Themen Datensicherheit und Datenschutz.
3. Die Verknüpfung von IoT und Blockchain bietet die angestrebte Verbindlichkeit in der dezentralisierten Welt der smarten Dinge, im Vergleich zu weiteren existierenden Herangehensweisen, zum Beispiel Krypto-Protokolle, Firewalls, IDS/IPS und CIDN [6-8].
4. Eine Blockchain ist ein digitaler Speicher, der in einem Peer-to-Peer-Netzwerk betrieben wird. In ihr werden Transaktionen aus dem Netzwerk in gesicherten und verketteten Blöcken gespeichert.
5. Sichere und in der Blockchain genutzte IoT-Geräte können nur unter Hinzunahme und Kombination bekannter Krypto-Technologien erreicht werden. Etwas weiter gedacht kann die schrittweise Bereitstellung von Blockchain dabei helfen, klare Pflichten, Verantwortung und Haftung bei IoT-Lösungen festzulegen.
6. Eins der bekannten Probleme der Blockchain-Technologie ist der vernünftige Umgang mit Rechenleistung und Ressourcen. Es muss ein Konsens zwischen energiesparsamer IoT und dem energietechnisch vertretbaren Einsatz einer Blockchain gefunden werden.
7. Der Fokus liegt auf der Integration über die effizienten Softwareplattformen. Es bleibt jedoch zu erwarten, dass diese Integrationsplattformen [15-26] für IoT und Blockchain künftig mit zusätzlichen Funktionen ausgestattet werden, die das Handling verbessern und deren Akzeptanz erhöhen.

Literaturverzeichnis

[1] Tim Zobjack. Untersuchung der Integration von IoT und Blockchain mit Hilfe der SAP Cloud Platform Integration Suite und Abschätzung der Eignung als zusätzliche Kompetenzfelder für ein mittelständisches Beratungsunternehmen, 2020, BA Dresden, Bachelor-Thesis, 87 Seiten mit Anlagen.

[2] Jamil Y. Khan, Mehmet R. Yuce (Eds.). Internet of Things (IoT): Systems and Applications, 2019, New York, Jenny Stanford Publishing, ISBN 9780429399084, 366 p.

[3] Lueth, Knud Lasse. The 25 best IoT Platforms 2019 - Based on Customer Review (Online 2020): https://iot-analytics.com/the-25-best-iot-platforms-2019/.

[4] Mahmood Zaigham (Ed.): Fog Computing: Concepts, Frameworks and Technologies, Springer 2017, London, ISBN 978-3-319-94890-4.

[5] Mattern, Friedemann/Flörkemeier, Christian (Online 2010): Vom Internet der Computer zum Internet der Dinge: http://www.vs.inf.ethz.ch/publ/papers/Internet-der-Dinge.pdf

[6] Andriy Luntovskyy, Dietbert Gütter. Moderne Rechnernetze – Lehrbuch; Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken, Vorwort: Alexander Schill, Springer Vieweg, 2020, ISBN 978-3658-25616-6.

[7] Andriy Luntovskyy, Dietbert Gütter. Moderne Rechnernetze – Übungsbuch; Aufgaben und Musterlösungen zu Protokollen, Standards und Apps in kombinierten Netzwerken (Übungen und Musterlösungen zum Lehrbuch), Springer Vieweg, 2020, ISBN 978-3658-25618-0.

[8] Andriy Luntovskyy, Josef Spillner. Architectural Transformations in Network Services and Distributed Systems: Service Vision. Case Studies, Springer Nature Verlag, April 2017, 348 p. (ISBN: 9-783-6581-484-09).

[9] S.Newman. Building Micro-Services, O'Reilly Media, USA, 2015, ISBN: 978-1-491-95035-7, 473 p.

[10] MIT Blockchain Course (Online 2020): http://executive-education.mit.edu/MIT-Blockchain/Online-Course/.

[11] A.Luntovskyy, D.Guetter. Cryptographic Technology Blockchain and its Applications, in „Advances in Information and Communication Technologies", Springer (ISBN: 978-3-030-16769-1), LNCS „Processing and Control in Information and Communication Systems (Int. Conf. UkrMiCo-2019)" (eds.:M.Ilchenko, L.Globa et al.), 2019, pp. 14-33 (https://link.springer.com/book/10.1007/978-3-030-16770-7).

[12] Survey on Crypto-platforms (Online 2002) https://hackernoon.com/top-blockchain-platforms-to-watch-out-in-2019-aa80e336a426/.

[13] Blockchain as a Service: Teamwork ohne Daten-Grenzen (Online 2020): https://www.t-systems.com/blockchain/.

[14] A.Antonopoulos, G.Wood. Mastering Ethereum: Building Smart Contracts and Dapps, 2019, O'Reilly Media, 345p., ISBN:978-1491971-949.

[15] Codius: Open-source Hosting Platform for Smart Programs (Online 2020): https://codius.org/.

[16] Hyperledger Sawtooth (Online 2020): https://www.hyperledger.org/projects/sawtooth/.

[17] Karl Wuest, Arthur Gervais. Do you need a Blockchain? ETH Zurich & Imperial College London (Online 2020): https://eprint.iacr.org/2017/375.pdf.

[18] MS Bletchley (Online 2020): https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md/.

[19] Leske, Christophe, Göbel, Andreas, Joswig, Steffen (2020): Blockchain mit SAP, 1. Aufl.

[20] SAP Cloud Integration (Online 2020): https://www.sap.com/.

[21] SAP Cloud Platform unterstützt Blockchain-Frameworks, Kap. 2 (in German, Online 2020): https://www.edvbuchversand.de/productinfo.php?replace=false&cnt=productinfo&mode=2&type=2&id=rw-6914&index=2&nr=0&window=edvbv&art=Leseprobe&preload=false

[22] SAP Leonardo for IoT (Online 2020): https://blogs.sap.com/2019/05/06/sap-leonardo-iot-for-smbs/.

[23] Siemens Blockchain (Online 2020): https://www.plm.automation.siemens.com/.

[24] Siemens Blockchained IoT (Online 2020): https:// new.siemens.com/.

[25] Smart Contracts (Online 2020): http://www.icertis.com/.

[26] A. Luntovskyy, L. Globa. Performance, Reliability and Scalability for IoT, IEEE Conf. IDT-2019, Zilina, Slovakia, 2019, 6p. (IEEE Xplore: https://ieeexplore.ieee.org/document/8813679, DOI: 10.1109/DT.2019.8813679).