IT kompakt

Hans-Georg Fill
Andreas Meier

Blockchain kompakt

Grundlagen, Anwendungsoptionen und kritische Bewertung

Springer Vieweg

IT kompakt

Die Bücher der Reihe „IT kompakt“ zu wichtigen Konzepten und Technologien der IT:

- ermöglichen einen raschen Einstieg,
- bieten einen fundierten Überblick,
- eignen sich für Selbststudium und Lehre,
- sind praxisorientiert, aktuell und immer ihren Preis wert.

Weitere Bände in der Reihe http://www.springer.com/series/8297

Hans-Georg Fill · Andreas Meier

Blockchain kompakt

Grundlagen, Anwendungsoptionen und kritische Bewertung

Unter Mitwirkung von Matthias Egli, Mark Fenwick, Daniel Gerber, Felix Härer, Tim Niemer, Edy Portmann, Sarah Röthlisberger, Anton Sentic, Bernd Teufel und Stefan Wrbka

Springer Vieweg

Hans-Georg Fill
Forschungsgruppe Digitalisierung und Informationssysteme
Departement für Informatik
Universität Fribourg
Fribourg, Schweiz

Andreas Meier
Departement für Informatik
Universität Fribourg
Fribourg, Schweiz

ISSN 2195-3651 ISSN 2195-366X (electronic)
IT kompakt
ISBN 978-3-658-27460-3 ISBN 978-3-658-27461-0 (eBook)
https://doi.org/10.1007/978-3-658-27461-0

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Mit der fortschreitenden Entwicklung der digitalen Wirtschaft und Gesellschaft gewinnt die Sicherheit von Transaktionen im World Wide Web an Bedeutung: Wie können Austauschbeziehungen ohne zentrale Instanz unter den Teilnehmenden risikofrei realisiert werden? Wie lassen sich internationale Verträge zwischen diversen Handelspartnern weltweit absichern? Wie kann ein globales Identitätsmanagement für alle Erdenbewohner vertrauenswürdig realisiert werden? Wie lassen sich Vermögenswerte und Eigentumsrechte weltweit verbindlich speichern und absichern? Eine erfolgsversprechende Antwort zu diesen Fragen lautet: Mit der Blockchain-Technologie.

Die Blockchain ist eine Art elektronisches Register, welches ein dezentrales Transaktionsmanagement über Peer-to-Peer Netzwerke und Konsensalgorithmen realisiert. Jeder gültige Datenblock der Blockchain verweist auf seine vor ihm validierten Blöcke, wodurch eine Kette von verifizierten, unabänderlichen Blöcken entsteht. Da jeweils eine vollständige Kopie der Blockchain auf den Geräten der Teilnehmer vorhanden ist, sind die hinterlegten Informationen für alle Teilnehmer transparent. Zur Validierung der Blöcke wird zufällig ein Teilnehmer der Blockchain ausgewählt und anschließend ein Konsens durch die Mehrheit gefunden.

Zu den bekanntesten Anwendungsfällen für Blockchains zählen Kryptowährungen wie Bitcoin oder Ether. Die Blockchain übernimmt dabei die Rolle einer Bank, indem sie sämtliche Transaktionen validiert und speichert. Bei dieser Anwendung ist

die Funktion der Blöcke auf die Erfassung und Überprüfung von Geldtransaktionen limitiert.

Die Blockchain ermöglicht darüber hinaus die Automation verteilter Anwendungsfunktionen, ohne auf eine zentrale Instanz angewiesen zu sein. Dementsprechend groß ist das Interesse von Unternehmen aus unterschiedlichen Branchen.

Das vorliegende Fachbuch erläutert die Grundlagen zu den Datenstrukturen von Blockchains, insbesondere zu Hash-Funktionen und -Bäumen, zur digitalen Signatur, zu den Funktionen von Blockchains sowie zu Konsensalgorithmen. Darüber hinaus werden wichtige Anwendungsoptionen aufgezeigt, rechtliche Fragen aufgeworfen und eine kritische Bewertung zur Blockchain-Technologie gegeben.

Für die Vielfalt der Anwendungsoptionen zur Blockchain und zur Klärung rechtlicher Fragen haben uns Experten unterstützt und einzelne Beiträge verfasst. Wir sind folgenden Fachkollegen zu besonderem Dank verpflichtet:

- Felix Härer vom Departement für Informatik der Universität Fribourg (diuf.unifr.ch) hat den Abschn. 4.1 über Kryptowährungen verfasst und den Abschn. 4.2 über Identity Management überarbeitet und ergänzt.
- Der Abschn. 4.4 über Smart Grid stammt von den Kollegen Bernd Teufel, Anton Sentic und Tim Niemer vom international institute of management in technology (iimt.ch) der Universität Fribourg.
- Edy Portmann vom Institut Human Centered Interaction Science & Technology (human-ist.unifr.ch) der Universität Fribourg sowie seine Mitforschenden Matthias Egli, Daniel Gerber und Sarah Röthlisberger von der Schweizerischen Post bzw. der Postfinance, Bern (post.ch) haben den Abschn. 4.6 über Smart Cities beigesteuert.
- Mark Fenwick von der Fakultät für Recht der Universität Kyushu in Fukuoka, Japan (hyoka.ofc.kyushu-u.ac.jp) und Stefan Wrbka von der Fachhochschule Wien der Wirtschaftskammer Wien (fh-wien.ac.at) haben die rechtlichen Fragen bezüglich der Blockchain-Technologie in Kap. 5 dargelegt.

Das Werk richtet sich an Führungsverantwortliche, Projektleiter und Interessierte, die sich einen Überblick über das Potenzial der Blockchain-Technologie verschaffen möchten. Es soll helfen, Verbesserungen im eigenen Unternehmen, in der Verwaltung oder im öffentlichen Leben zu erkennen und Lösungsansätze anzugehen.

Fribourg
im September 2019

Hans-Georg Fill
Andreas Meier

Inhaltsverzeichnis

Motivation Betrugsprävention

1

Zusammenfassung

Blockchains sind verteilte elektronische Register, die mithilfe kryptografischer Verfahren und Konsensalgorithmen vor Manipulationen geschützt sind und als vertrauenswürdige Quelle von Informationen dienen. Damit können sie insbesondere zur Betrugsprävention eingesetzt werden, unter Verzicht auf zentrale Überwachungsinstanzen. Bekanntheit erlangten sie durch den Erfolg der Kryptowährung Bitcoin, deren Eigenschaften bis heute die Entwicklung von Blockchain-Ansätzen beeinflussen.

Das sogenannte Problem der Byzantinischen Generäle bezieht sich auf die Eroberung der Stadt Konstantinopel im Jahre 1453. Einer Legende nach hatten die Angreifer unter dem osmanischen Sultan Mehmed II. ein Kommunikationsproblem, als sie versuchten, die Stadt von mehreren Seiten gleichzeitig anzugreifen. Der Austausch der Angriffszeit mit Botengängern erschien als schwierig, da einige osmanische Befehlshaber gegen andere intrigierten, um diese beim Sultan Mehmed II. in Misskredit zu bringen. Wegen der stark gesicherten Stadt war es hingegen wichtig, gleichzeitig einen Angriff zu starten. Die Verteidigung der Stadt oblag Kaiser Konstantin XI., der als letzter Kaiser des

H.-G. Fill und A. Meier, *Blockchain kompakt,* IT kompakt,
https://doi.org/10.1007/978-3-658-27461-0_1

Byzantinischen Reiches aller Wahrscheinlichkeit nach während des letzten Sturms durch das osmanische Belagerungsheer fiel.

Das obige Problem tritt in der Informatik ebenfalls auf und ist unter dem Begriff Byzantinischer Fehler bekannt. In einem verteilten Netz von Sensoren für Autobahnen, Flughäfen, Kraftwerken oder Produktionsanlagen werden Nachrichten untereinander ausgetauscht. Falls ein oder mehrere Sensoren fehlerhaft messen und falsche Daten liefern, liegen für wichtige Entscheidungen fehlerhafte Informationen vor. Im Extremfall kann das Netz durch fehlerhafte Messungen resp. Übertragungen zum Erliegen kommen, falls einzelne Knoten diese falschen Informationen weiterverwenden.

Im Jahre 1982 haben Lamport, Shostak und Pease den Forschungsbericht ‚The Byzantine Generals Problem' veröffentlicht (siehe Lamport et al. 1982) und aufgezeigt, dass obiges Kommunikationsproblem gelöst werden kann, falls ein Konsensalgorithmus unter den Generälen angewendet wird.

Die Blockchain ist ein verteiltes elektronisches Register, dessen Sicherheit gegen Manipulationen mithilfe kryptografischer Verfahren und dank Konsensalgorithmen gewährleistet wird. Dabei wird auf eine zentrale Überwachungsinstanz verzichtet.

Kryptowährungen[1] wie Bitcoin, Ether u. a. basieren auf der Blockchain-Technologie (Hosp 2018; Berentsen und Schär 2017) und sind täglich in den Medien präsent. Viele sprechen von einem Hype, obwohl es immer wieder kritische Stimmen dazu gibt. Beispielsweise warnt der bekannte Investor Warren Buffet die Anleger vor virtuellen Währungen. Er vergleicht den Hype mit der Tulpenmanie in Holland von 1637, die als eine der

[1]Kryptowährung oder Kryptogeld sind digitale Zahlungsmittel, die mit Hilfe asymmetrischer Verschlüsselungsverfahren abgesichert werden und keiner zentralen Kontrolle (Bank, Aufsicht) unterliegen. Neben der bekanntesten Währung Bitcoin mit der zur Zeit größten Kapitalisierung gibt es über 4000 weitere digitale Währungen (Wikipedia 2018), welche auf der Blockchain-Technologie oder anderen technischen Ansätzen beruhen.

ersten Spekulationsblasen in die Wirtschaftsgeschichte einging. Kürzlich bezeichnete Warren Buffet die digitalen Währungen in seinem Interview vom 7. Mai 2018 beim TV-Sender CNBC gar als ‚rat poison squared' (Rattengift hoch zwei).

Am 1. November 2008 veröffentlichte Satoshi Nakamoto (Pseudonym) eine E-Mail unter dem Titel ‚Bitcoin P2P e-cash paper' mit den Worten: ‚I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party' (Nakamoto 2008a). Als wichtigste Eigenschaften hob er u. a. hervor:

- ‚Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof-of-work.'

Den Vorschlag konkretisierte Satoshi Nakamoto in seinem Beitrag über ‚Bitcoin – A Peer-to-Peer Electronic Cash System' (Nakamoto 2008b).

Die kürzeste Formulierung zur Charakterisierung der Blockchain lässt sich als Gleichung schreiben (siehe Meier und Stormer 2018): Blockchain = Distributed Ledger + Consensus. Diese verkürzte Form geht auf Niklaus Wirth zurück, der in seinen Vorlesungen an der ETH in Zürich zu sagen pflegte: Programs = Data Structures + Algorithms (Wirth 1976). In abgewandelter Form definiert sich die Blockchain (Software) als Distributed Ledger (Datenstruktur für dezentrale Buchführung) plus Consensus (Konsensalgorithmus zur Betrugsprävention).

Das vorliegende Buch führt in die Blockchain-Technologie ein und beschreibt ihre wesentlichen Bestandteile. Darauf aufbauend werden Anwendungsbereiche für Blockchains beschrieben, die sich bereits in Umsetzung befinden oder aktuell erforscht werden. Ein eigenes Kapitel, das von den Autoren Mark Fenwick und Stefan Wrbka beigesteuert wurde, widmet sich den rechtlichen Aspekten von Blockchains. Abschließend wird die Technologie einer kritischen Einschätzung unterzogen.

Literatur

Berentsen, A., Schär, F.: Bitcoin, Blockchain und Kryptoassets. Books on Demand, Norderstedt (2017)

Hosp, J.: Kryptowährungen einfach erklärt – Bitcoin, Ethereum, Blockchain, Dezentralisierung, Mining, ICOs & Co. München, Finanzbuch Verlag (2018)

Lamport, L., Shostak, R., Pease, M.: The Byzantine General Problem. ACM Trans. Program. Lang. Syst. **4**(3), 382–401 (1982)

Meier, A., Stormer, H.: Blockchain = Distributed Ledger + Consensus. In: Kaufmann, M., Meier, A. (Hrsg.) Blockchain (HMD Zeitschrift der Wirtschaftsinformatik **55**(6)), S. 1139–1154. Springer, Heidelberg (2018)

Nakamoto S.: Bitcoin P2P e-cash paper. https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html (2008a). Zugegriffen: 7. Mai 2018

Nakamoto S.: Bitcoin – A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf (2008b). Zugegriffen: 7. Mai 2018

Wikipedia: Kryptowährung. https://de.wikipedia.org/wiki/Kryptowährung (2018). Zugegriffen: 7. Mai 2018

Wirth, N.: Algorithms + Data Structures = Programs. Prentice Hall, New Jersey (1976)

Grundlagen zur Blockchain-Technologie

2

Zusammenfassung

In diesem Kapitel werden die Grundlagen zur Blockchain-Technologie vorgestellt. Diese sind essenziell, um die Funktionsweise von Blockchains zu verstehen und ihr Potenzial für Anwendungen einschätzen zu können. Insbesondere wird auf Hash-Funktionen, Merkle-Bäume und Merkle-Proofs sowie digitale Signaturen eingegangen und es werden deren Mechanismen anhand von einfachen Beispielen erläutert.

Die für die Realisierung von Blockchains zugrundeliegenden Technologien sind im Einzelnen in der Informatik bereits seit geraumer Zeit bekannt. Das innovative an Blockchains ist jedoch die Kombination dieser Technologien zur Realisierung von neuen Geschäftsmodellen und -praktiken. Blockchains sind somit dem Kernbereich der gestaltungsorientierten Wirtschaftsinformatik zuzuordnen, die sich mit der Konzeption und technischen Realisierung von Informationssystemen für die Wirtschaft und Gesellschaft befasst. Zum Verständnis von Blockchains sind sowohl Kenntnisse der technischen Grundlagen zu den Technologien im Einzelnen als auch deren Zusammenführung im Kontext von wirtschaftlichen Anwendungsfällen erforderlich. Im Folgenden werden daher Grundlagen zu Hash-Funktionen, Hash-Bäumen und digitalen Signaturen erläutert.

H.-G. Fill und A. Meier, *Blockchain kompakt,* IT kompakt,
https://doi.org/10.1007/978-3-658-27461-0_2