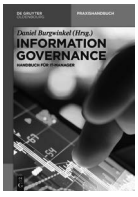
Daniel Burgwinkel (Hrsg.)
Blockchain Technology

Weitere empfehlenswerte Titel



Information Governance
D. Burgwinkel, 2017
ISBN 978-3-11-044369-1, e-ISBN 978-3-11-044526-8,
e-ISBN (EPUB) 978-3-11-043623-5, Set-ISBN 978-3-11-044527-5

Informatik und Gesellschaft
A. Kienle, G. Kunau, 2014
ISBN 978-3-486-73597-0, e-ISBN 978-3-486-78145-8,
e-ISBN (EPUB) 978-3-486-99058-4

Vernetzte Organisation
A. Richter (Hrsg.), 2014
ISBN 978-3-486-74728-7, e-ISBN 978-3-486-74731-7,
e-ISBN (EPUB) 978-3-486-98956-4, Set-ISBN 978-3-486-98957-1

Kooperation von Rechenzentren
D. von Suchodoletz et al. (Hrsg.), 2016
ISBN 978-3-11-045888-6, e-ISBN 978-3-11-045975-3,
e-ISBN (EPUB) 978-3-11-045895-4, Set-ISBN 978-3-11-045976-0

Blockchain Technology

Einführung für Business- und IT Manager

Herausgegeben von Daniel Burgwinkel

DE GRUYTER
OLDENBOURG

Herausgeber
Dr. Daniel Burgwinkel
Blockchain Advisory
Neuhausstr. 30
4057 Basel
Schweiz
daniel.burgwinkel@blockchain.jetzt
www.blockchain.jetzt

ISBN 978-3-11-048731-2
e-ISBN (PDF) 978-3-11-048895-1
e-ISBN (EPUB) 978-3-11-048751-0
Set-ISBN 978-3-11-048896-8

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress.

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

Einbandabbildung: ublubachka/iStock/thinkstock
Druck und Bindung: CPI books GmbH, Leck
♾ Gedruckt auf säurefreiem Papier
Printed in Germany

www.degruyter.com

Inhalt

Vorwort

In der Wirtschaftspresse und in der Startup-Community wird intensiv über zukünftige Anwendungsfelder der Blockchain-Technologie diskutiert. Das vorliegende Buch führt Business- und IT Manager in die neue Technologie Blockchain ein und dient als Grundlage für ein dreitägiges Seminar, welches in Kooperation mit der Fachhochschule Nordwestschweiz durchgeführt wird. Folgende Ziele werden hier verfolgt:

- **Blockchaintechnologie und deren Funktionsweise verstehen:** In den Beiträgen von Daniel Burgwinkel und Tarmo Ploom wird die Funktionsweise sowohl aus Business- und IT Sicht erläutert.
- **Aktuelle Blockchain-Plattformen verstehen und beurteilen:** Im Kapitel von Romeo Kienzler wird die Plattform Hyperledger vorgestellt.
- **Einsatzgebiete von Blockchaintechnologie kennen und verstehen:** Michael Merz erläutert die Potenziale im Energiesektor und Martin Ploom beschreibt Einsatzgebiete in der Finanzindustrie.
- **Potential und Auswirkungen von Blockchains auf das eigene Unternehmensumfeld erkennen und übertragen:** Anhand von Checklisten unterstützt Daniel Burgwinkel die Konzeption von Blockchainanwendungen. Bruno Wildhaber beschreibt in seinem Beitrag die Rolle des Vertrauens im Kontext Blockchain. Vladimir Tosovic nimmt den aktuellen Fall des Hackerangriffes auf das Crowdfundingprojektes „DAO“ zum Anlass um Potenziale und Grenzen von Smart Contracts zu beschreiben.

Der Markt und die Blockchain-Technologie entwickeln sich dynamisch. Daher werden wir auf der Website www.blockchain.jetzt und auf der Verlagswebsite www.degruyter.com Zusatzmaterial und ergänzende Beiträge publizieren. Somit versteht sich das vorliegende Buch als Startpunkt für neue Diskurse und soll den Einstieg in das Thema für den deutschsprachigen Leser erleichtert.

Ich bedanke mich bei meinem Autoren Michael Merz, Romeo Kienzler, Martin Ploom, Tarmo Ploom, Vladimir Tosovic und Bruno Wildhaber für Ihre Beiträge. Gerne steht das Autorenteam bei Fragen und Anregungen zur Verfügung.

Basel, im September 2016

Dr. Daniel Burgwinkel

Daniel Burgwinkel

Blockchaintechnologie und deren Funktionsweise verstehen

1 Einleitung

Dieses Kapitel führt in die grundlegenden Begriffe der Blockchain-Technologie ein und zeigt auf für welche Einsatzgebiete Blockchain-Plattformen genutzt werden können.

Das Thema Blockchain wird zurzeit intensiv sowohl von Business- als auch IT Managern diskutiert. Businessmanager sehen neue disruptive Geschäftsmodelle und die Technologie fasziniert IT-Fachleute, die über die digitale Währung Bitcoin erste Erfahrungen sammeln durften. Stand 2016 analysieren globale Banken und Fintech-Startups neue Anwendungsfelder wie elektronische Handelssysteme oder digitale Zahlungssysteme auf Basis dieser Technologie. Sowohl Fachpresse, wie der Economist [1] und das Handelsblatt [2], als auch Trendforscher, wie das World Economic Forum [3], sehen in der Blockchain-Technologie einen zukunftsweisenden Trend.

Auch die globalen IT-Unternehmen IBM [4] und Microsoft [5] haben die Bedeutung der Blockchain Technologie erkannt und neue Blockchain-Services auf ihren Cloud-Plattformen eingeführt.

Mit dem Begriff Blockchain wird ein technisches Konzept bezeichnet, welches Daten nicht in einer zentralen Datenbank, sondern verteilt auf den Systemen der Nutzer mithilfe von kryptographischer Verfahren speichert. Das Wort „Blockchain“ wurde gewählt, da die Daten in einzelnen Blöcken gespeichert werden, welche dann verteilt auf den Systemen der Netzwerkteilnehmer abgelegt werden und die Reihenfolge der Blöcke anhand einer Kette dokumentiert wird. Im Verlauf dieses Kapitels werden wir das Prinzip näher erläutern.

Obwohl dies nur ein technisches Konzept ist, sind Experten der Meinung, dass dieser Ansatz die Geschäftsmodelle in verschiedensten Branchen revolutionieren wird. Will man diese Technologie für ein Einsatzgebiet nutzen so stellen sich folgende Fragen:

- Welche Anwendungen und Use Cases lassen sich auf Basis Blockchain realisieren?
- Welche Daten lassen sich sinnvoll in Blockchains abspeichern?
- Welche Transaktionen können sinnvoll durch Blockchains unterstützt werden?
- Welche technischen Restriktionen gibt es?

Die neue Technologie Blockchain, die zum Beispiel für Bitcoin verwendet wird, hat das Potential die Geschäftsmodelle in allen Branchen zu verändern. Blockchains ermöglichen Banken neue Modelle für den Handel- und Zahlungsverkehr während Industrieunternehmen den Einsatz im Bereich Internet-of-Things (IoT) erforschen. Blockchains werden bereits heute produktiv im eHealth und eGoverment in anderen Ländern eingesetzt. Experten gehen davon aus, dass die Blockchaintechnologie in allen Branchen neue Geschäftsmodelle ermöglicht, welche im Wettbewerb zu etablierten Unternehmen stehen.

2 Grundlegende Begriffe im Kontext Blockchain

Beginnt man sich in das Thema Blockchain einzulesen, so stößt man auf eine Vielzahl von Pressemeldungen und Fachartikeln. Die Meinungen schwanken zwischen Euphorie und der Ankündigung des Untergangs und sind typischerweise nach dem folgenden Schema aufgebaut:

- „Startup X will mit Blockchain die Branche Y revolutionieren…“
- „Expertengruppe X hat Studie zum Einfluss von Blockchains auf den Wirtschaftszweig Y erarbeitet…“
- „Softwarehersteller X bietet eine Blockchain Plattform als Clouddienst an…“
- „Die Kryptopwährung X steigt von 1 Dollar auf 15 Dollar innerhalb von sechs Monaten…“
- „Börse für Kryptowährung X wurde durch einen Hacker angegriffen und Kurs der Währung fällt…“

Als Leser dieser Meldungen sollte man sich zuerst Klarheit schaffen, was der eigentliche Gegenstand ist:

- Handelt es sich um den Einfluss des Blockchainkonzeptes auf eine bestimmte Branche?
- Ist es ein konkreter Anwendungsfall (Use Case) der mit Blockchains gelöst wurde?
- Ist es eine Meldung über Blockchain Software, welche zur Programmierung genutzt werden kann?
- Ist es eine Meldung über eine Blockchain Plattform auf welcher Applikationen betrieben werden können?
- Ist es eine Blockchain im Kontext einer Kryptowährung?
- Oder ein Clouddienst, welcher Blockchain Software zur Verfügung stellt?

In der Presse und im Internet findet sich eine Vielzahl Artikeln die Funktionsweise von Blockchains erläutern. Für das grundlegende Verständnis ist es wichtig, folgende Begriffe zu unterscheiden:

- **Blockchain als technisches Konzept** in der Informatik, welches Methoden einsetzt die mehr als dreißig Jahre bekannt sind.
- **Blockchain Software**, die den Programmcode bereitstellt, um die kryptographischen Verfahren durchzuführen. In 2016 sind mehr als zwanzig verschiedene kommerzielle als auch Open-Source Softwareprodukte verfügbar.
- **Blockchain-Applikationen** zur Realisierung eines bestimmten Anwendungsfalles (Use Case). Typischerweise werden diese Applikationen mit Hilfe einer Blockchainsoftware bzw. auf einer Blockchain Plattform betrieben.
- **Blockchain-Plattformen**, welche eine ausgewählte Software nutzen und im Internet als Dienst betrieben werden, z.B. als offenes Peer-to-Peer Netzwerk oder als kommerzieller Dienst.
- **Blockchain-as-a-Service**, der in einer Cloud die erforderliche Software und Dienste zur Verfügung stellt. In diesen Angeboten kann eine ausgewählte Blockchain-Software auf virtuellen Rechnern in der Cloud betrieben werden.

Diese Zusammenhänge sind in der folgenden Abbildung dargestellt.

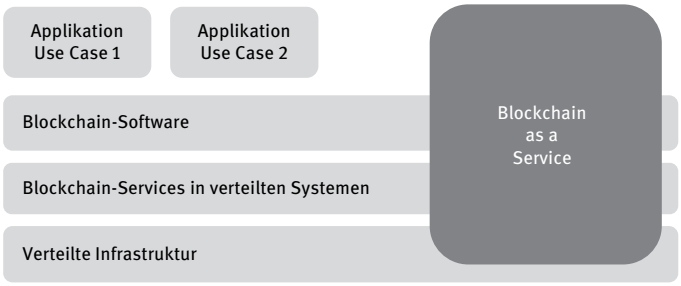


Abb. 1: Zusammenhang Blockchain Software, Plattform, Service

2.1 Das technische Grundkonzept von Blockchains

Für das vorliegende Buch führen wir folgende Definitionen ein:

Mit dem Begriff **Blockchain** wird ein technisches Konzept bezeichnet, welches einzelne Datensätze (z.B. Transaktionen) zu Blöcken zusammenfasst und mit Hilfe kryptografischer Verfahren die Datenintegrität gewährleistet.

Die **Blöcke sind miteinander sequentiell verkettet**, so dass die zeitliche Reihenfolge als auch die Datenintegrität des gesamten Datenbestandes sichergestellt ist. Eine Manipulation eines Datensatzes

würde nachweisbar sein. Bei einer Blockchain werden neue Daten zu einem neuen Block zusammengefasst und dieser wird an die bestehende Blockchain angehängt.

Eine Blockchain kann entweder als einzelne Instanz betrieben werden oder wird als verteiltes System aufgebaut. Im **verteilten Ansatz** werden die Daten nicht in einer zentralen Datenbank gespeichert, sondern verteilt auf den Systemen der Netzwerkteilnehmer abgelegt und mithilfe von kryptographischer Verfahren die Integrität gewährleistet.

Um das Prinzip der Blockchain zu erläutern, wollen wir ein vereinfachtes Beispiel der Erzeugung einer Blockchain beschreiben. In den nachfolgenden Abschnitten werden wir dann auch komplexere Fälle beschreiben.

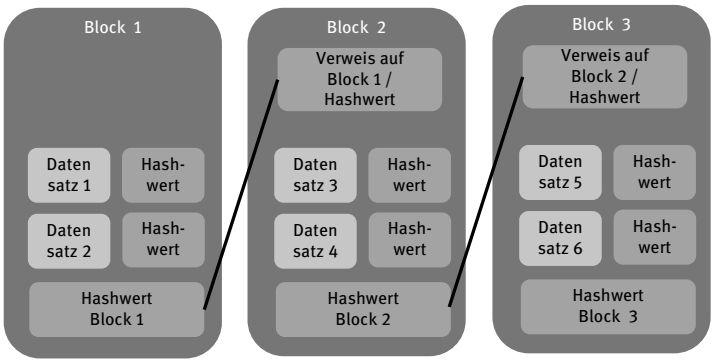


Abb. 2: Vereinfachtes Beispiel des Blockchain Prinzips

In Beispiel 1 wollen wir eine Blockchain erzeugen, die uns dabei unterstützt nachzuweisen, dass der Datensatz D1
- exakt zum Zeitpunkt T1 erzeugt wurde
- nicht nachträglich verändert wurde und
- und die Reihenfolge der Datensätze D1, D2, D3 etc. nicht manipuliert wurde.

In der folgenden Tabelle sind die Schritte aufgeführt:

Tab. 1: Beispiel 1 – Vereinfachtes Beispiel der Erzeugung einer Blockchain

Nr.	Aktion	Eingesetzte Methoden
1	Die einzelnen Datensätze werden von einer Applikation erzeugt, z.B. pro Sekunde werden zwei Datensätze erzeugt.	

Nr.	Aktion	Eingesetzte Methoden
2	Die Datensätze werden in einem Block zusammengefasst und Hashwerte (Prüfsummen) werden erzeugt.	Hashwert erzeugen
3	Die Daten und die Hashwerte werden zusammen mit der Nummer des Vorgängerblocks in Block Nr. 1 gespeichert.	Bildung eines Blocks
4	Im nächsten Block Nr. 2 wird auf Blockes 1 verwiesen und die neuen Datensätze hinzugefügt.	Verkettung der Blöcke
5	Die Blockchain, welche zurzeit aus Block 1 und Block 2 besteht, wird auf mehrere Rechner kopiert. Es existieren somit mehrere Kopien der Blockchain.	Kopieren der Blockchain auf mehrere Rechner

In diesem einfachen Beispiel wurde eine lange Datei (Blockchain) erzeugt, welche auf zwei Rechnersystemen gespeichert wurde. Im Beispiel 2 wollen wir das Grundprinzip um folgende Funktionen erweitern:

- Je nach Konzept können in der Blockchain die geschäftsrelevanten Informationen selber gespeichert werden (wie z.B. Transaktionsdaten) oder die Daten der Blockchain enthalten eine Referenz auf externe Daten, weil z.B. die Daten ein hohes Speichervolumen besitzen oder die Daten sehr vertraulich sind.
- Um zu vermeiden, dass die kryptografischen Berechnungen manipuliert werden setzt man auf eine Verteilung der Rechenkapazität. Je nach Consensus-Verfahren berechnen mehrere Rechner die Operationen, um sich dann auf ein Ergebnis zu einigen.
- Um einen Verlust der gesamten Daten in der Blockchain vorzubeugen wird die Blockchain kopiert und im Netzwerk auf die Systeme verteilt.

Tab. 2: Beispiel 2 – Vereinfachtes Beispiel der Erzeugung einer Blockchain

Nr.	Aktion	Eingesetzte Methoden
1	Die einzelnen Datensätze werden von einer Applikation erzeugt, z.B. pro Sekunde werden 10 Datensätze erzeugt.	
2a	Die Datensätze werden auf die verteilten Rechner übermittelt und jedes Rechnersystem (Knoten) führt die kryptographischen Funktionen aus. Der Knoten welcher den „Wettbewerb“ gewinnt führt die Blockbildung aus.	– Verteilung der kryptographischen Berechnung auf verschiedene Rechner – Abstimmung durch einen Konsens-Algorithmus
2b	Falls die Blockchain mit einer Kryptowährung betrieben wird, wir dem Rechnerknoten (Miner) ein Betrag gutgeschrieben.	– Bezahlung der Miner mit einer Kryptowährung
2c	Die Datensätze werden in einem Block zusammengefasst und ein Hashwert erzeugt.	– Hashwert erzeugen

Nr.	Aktion	Eingesetzte Methoden
3	Die Daten, Hashwerte werden zusammen mit der Nummer des Vorgängerblocks in Block 1 gespeichert.	– Bildung eines Blocks
4	Im nächsten Block Nr. 2 wird der Hashwert des Blockes 1 gespeichert und wiederum der Hashwert der neuen 10 Datensätze errechnet.	– Verkettung der Blöcke
5	Die Blockchain, welche aus Block 1 und Block 2 besteht, wird auf verschiedene Rechner kopiert.	– Kopieren der Blockchain auf Rechner Nr. 2

Ein vielzitiertes Beispiel der Anwendung von Blockchains ist die Bitcoin-Blockchain, welche die Transaktionen im Peer-to-Peer Netzwerk Bitcoin speichert. Bei der Speicherung von Transaktionen werden zusätzliche Verfahren eingesetzt, wie z.B. die Verwendung von Adressen für die Teilnehmer. In dem vorliegenden Kapitel wollen wir nicht detaillierter auf die Transaktionen eingehen, sondern verweisen auf die zahlreichen Publikationen im Kontext Bitcoin, wie z.B. die Bitcoin Entwicklerdokumentation [6].

Um die verschiedenen Arten von Blockchains zu unterscheiden ist es jedoch wichtig zu verstehen, dass die Bitcoin-Blockchain als öffentliches Register, auch Kontobuch genannt (englischer Ausdruck „Ledger“) aufgebaut ist, in welches alle Teilnehmer Einblick haben. Die im Bitcoin-Netzwerk durchgeführten Zahlungen sind als Transaktionen mit Zeitstempeln dokumentiert. Mehre Einträge der Transaktionen werden zu einem Block zusammengefasst. Durch diese Dokumentation in der Blockchain (und weitere Mechanismen) wird vermieden, dass die Geldeinheiten doppelt ausgegeben werden. Ein Missbrauch z.B. durch Fälschung der Transaktionshistorie ist nachweisbar. Zudem wird die Ausfallsicherheit erhöht, da jeder Teilnehmer des Netzwerkes, welcher einen Knotenpunkt betreibt, eine Kopie der Blockchain speichert.

In diesem Einführungskapitel haben wir vier wichtige Gestaltungsvarianten von Blockchains angesprochen, welche in der unteren Tabelle aufgeführt sind. Weitere Merkmale und Unterschiede werden in den folgenden Kapiteln erläutert.

Tab. 3: Grundlegende Unterscheidungsmerkmale von Blockchains

Kriterium	Ausprägungen
Art der Verteilung der Rechnerknoten	– Blockchain auf einem Einzelrechner bzw. in einem geschlossen organisationsinternen Netzwerk (private Blockchain). – Blockchain auf verteilten Rechnern in einem öffentlichen Netzwerk (public Blockchain). – Blockchain auf verteilten Rechnern bei denen nur ausgewählte Rechnerknoten zugelassen sind (Consortium Blockchain, z.B. innerhalb einer Branche).

Kriterium	Ausprägungen
Daten in der Blockchain	– Die Nutzdaten (z.B. Transaktionen) werden in der Blockchain gespeichert. – Die Nutzdaten sind außerhalb der Blockchain gespeichert. Eine Referenz auf die Daten und die Hashwerte wird in der Blockchain gespeichert.
Einsatz einer Kryptowährung	– Keine Kryptowährung (z.B. Guardtime) – Einsatz einer Kryptowährung als Lohn für die Betreiber der Rechnerknoten (z.B. Bitcoin, Ethereum). – Einsatz einer Kryptowährung um Zahlungen zwischen Teilnehmern zu ermöglichen (z.B. Bitcoin, Ethereum).
Weitere Eigenschaften	Werden in nachfolgenden Kapiteln erläutert.

Bei diesen aufgeführten Unterscheidungsmerkmalen von Blockchains sind folgende Aspekte von Interesse:

– Das Blockchain-Konzept kann sowohl in einem **Einzelsystem**, z.B. in einem unternehmensinternen Archiv, eingesetzt werden oder in einem **verteilten Ansatz**, z.B. in einem Peer-to-Peer Netzwerk. Insbesondere im Finanzbereich werden diese neuen verteilten Ansätze intensiv diskutiert und der Begriff „Distributed Ledger“ also eine Art „verteiltes Kontobuch“ wird hierbei verwendet, um aufzuzeigen, dass die Datenhaltung in einem verteilten System erfolgt.
– Es gibt Blockchains, welche eine Kryptowährung verwenden und Blockchains die ohne diesen Ansatz konzipiert sind. Ein Kryptowährung wird zum einen eingesetzt, um die Betreiber der Rechenknoten für ihre Arbeitsleistung zu bezahlen und kann außerdem als Währung für Transaktionen und Zahlungen genutzt werden.

2.2 Blockchain Software

In den letzten Jahren sind verschiedene Blockchain Software Codes als freie oder kommerzielle Softwareprodukte auf den Markt gekommen. In einem einfachen Einsatzszenario lässt sich die Blockchain-Software auch als Einzelsystem betreiben, wie z.B. für ein Dokumentenarchivsystem, welches die Datenintegrität mit dem Blockchainprinzip gewährleistet.

Die wesentliche Innovation der neuen Implementierungen ist der Aspekt der Verteilung der Rechenkapazität und der Datenspeicherung in einem verteilten Netzwerk. Für die Koordination des verteilten Rechnens müssen Services im Netzwerk zur Verfügung gestellt werden:

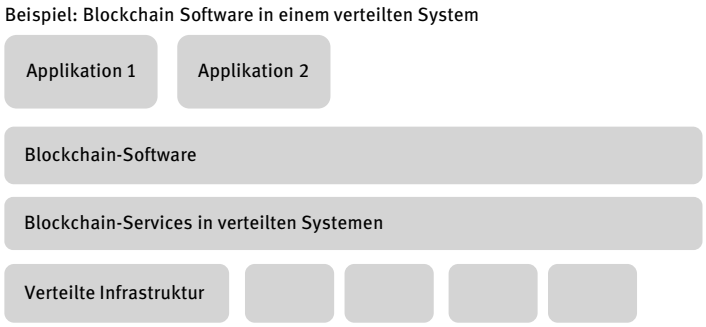


Abb. 3: Blockchain auf verteilten Systemen

Zum einen gibt es Blockchain Software die sich auf ein Einsatzfeld bzw. Use Case fokussiert. Seit 2013 sind vermehrt Softwareprodukte auf den Markt gekommen, welche sich als universeller Software verstehen und auf Anwendungsfälle anpassen lassen:

Tab. 4: Kategorien von Blockchain Software

Kategorie	Einsatzgebiete	Beispiele
Blockchain Software mit Fokus auf einen Use Case	– Digitale Zahlungen – Internet-Domains	– Bitcoin – Namecoin
Blockchain Software mit Fokus auf ein Einsatzgebiet	– Datenintegrität – Cybersecurity	– Guardtime
Blockchain Software als universelle Entwicklungsumgebung	– Gestaltung von Anwendungen möglich	– Ethereum – Hyperledger – Tendermint

2.3 Blockchain Plattformen

Ausgewählte Blockchain-Software steht nicht nur als Programmcode zur Verfügung, sondern wird als operative Plattform in Peer-to-Peer Netzwerken betrieben. Als Blockchain-Plattform wollen wir einen operativen Dienst bezeichnen, an den sich einzelne Nutzern oder Organisationen anschließen können. Ausgewählte Plattformen ermöglichen es Blockchain Applikation zu entwickeln und zu betreiben.

Als **Blockchain Plattform** wird eine Software- und Dienste-Infrastruktur bezeichnet, welche für unterschiedliche Einsatzfelder genutzt werden kann. Die operative Blockchainplattform kann öffentlich zugänglich sein (public) oder nur für einen geschlossenen Benutzerkreis (private/consortium). Im Modell „Consortium" Blockchain werden die kryptographischen Verfahren von definierten Teilnehmern ausgeführt während bei einer Public Blockchain jeder Teilnehmer seine Rechenleistung zur Verfügung stellen kann.

Stand 2016 sind insbesondere folgende Plattformen bekannt:

- **Die Bitcoin-Blockchain:** Das Zahlungssystem wurde 2008 in Betrieb genommen. Auf Basis der Bitcoin-Blockchain wurden zahlreiche Erweiterungen, sogenannte „Sidechains" entwickelt, welche sich aber noch nicht am Markt durchgesetzt haben.
- **Guardtime:** Die Blockchain ist seit 2007 am Markt und fokussiert sich auf den Nachweis der Integrität von Daten und Cybersecurity.
- **Ethereum:** Die Plattform wird seit 2013 entwickelt und versteht sich als universelle Plattform auf der die Nutzer eigene Anwendungen erstellen können.
- **Hyperleder:** Das Projekt wurde 2015 gestartet mit dem Ziel die Blockchaintechnologie für Unternehmen zu entwickeln. Stand 2016 stehen erste Versionen des Softwarecodes bereit.

Neben diesen branchenübergreifenden Plattformen gibt es zahlreiche Brancheninitiativen (insbesondere im Finanzbereich wie Digital Asset Holding und das R3 Konsortium) sowie neue Entwicklungsprojekte.

2.4 Blockchain Applikationen für bestimmte Use Cases

Eine Vielzahl von Blockchainapplikationen und Entwicklungsprojekten wird in der Presse genannt von denen sich viele in der Startup-Phase befinden:

- Grundbuchdienste in Entwicklungsländern (Fatcom)
- Anwendungen im Kontext Internet of Things (slock.it)

Eine **Blockchain Applikation** kann entweder auf einer Blockchainplattform entwickelt und betrieben werden oder das Blockchainkonzept wird innerhalb einer Applikation eingesetzt. Eine Applikation hat immer ein konkretes Anwendungsszenario.

2.5 Blockchain-as-a-Service

Seit 2016 haben Microsoft und IBM ihre Cloudplattformen um sogenannte *Blockchain-as-a-Service* Dienste erweitert. Hierbei wird sowohl die Hardwareinfrastruktur bzw. Rechenleistung als auch ausgewählte Blockchain-Software und Applikationen dem Kunden zur Verfügung gestellt.

2.6 Die Historie und Meilensteine im Bereich Blockchain

Die Konzepte auf denen Blockchains basieren beruhen auf mehr als dreißig Jahren Forschung:

- Im Jahr 1979 erfindet Ralph Merkle das Prinzip von Hashbäumen, welche auch als „Merkle-Tree“ bezeichnet werden [7].
- Im Jahr 1991 haben Haber/Stornetta in einem wissenschaftlichen Artikel publiziert, wie man Dokumente mit ein Zeitstempel versieht und diese Zeitstempel verkettet, dies wird auch als „linked timestamping“ bezeichnet [8].
- In 1997 publizierte Nick Szabo seine Vision von „Smart Contracts“, um aufzuzeigen wie sich der E-Commerce weiterentwickeln kann und wie Vertragsprozesse im Internet unterstützt werden könnten [9].
- Die in Estland entwickelte Blockchain „Guardtime“ wird 2007 als kommerzielles System in Betrieb genommen.
- In 2008 publizierte ein Autor unter dem Pseudonym Satoshi Nakamoto den Artikel „Bitcoin: A Peer-to-Peer Electronic Cash System”, welcher die Funktionsweise des Bitcoin Systems beschreibt [10].
- 2013 wird das Projekt „Ethereum“ gegründet mit dem Ziel eine weltweite, offene Plattform für Blockchain-Applikationen zu gründen.
- 2015 wird das Hyperleger Projekt gegründet.
- 2015 erweitern Microsoft und IBM das Angebot ihrer Clouddienste um Blockchain-Anwendungen.

Insbesondere die Finanzindustrie hat ein reges Interesse an Blockchains. Im Jahr 2014 wurden die ersten Blockchain Pilotprojekte in London gestartet. In 2015 wurde das Konsortium R3 wird in New York gegründet, welches im September 2015 mit drei Banken zusammenarbeitete. Im Jahr 2016 sind mehr als fünfzig Banken an dieser Initiative beteiligt.