Eine vertrauenswürdige Zusammenarbeit mit Hilfe der Blockchain-Technologie

39

Norbert Pohlmann

Zusammenfassung

Die „Blockchain“ ist eine spannende und faszinierende IT-Technologie, die das Potenzial hat, Politik, Verwaltung und Wirtschaftszweige gewaltig auf den Kopf zu stellen. Die Blockchain-Technologie ist eine Querschnittstechnologie mit hohem disruptiven Potenzial für viele Wirtschaftsbereiche. Die Blockchain-basierten Systeme könnten in vielen Bereichen zentrale Instanzen ablösen, wie Banken, Notare oder Treuhänder. Das ist möglich, weil die Validierungsalgorithmen der Blockchain-Technologie ganz ohne solche Intermediäre die Vertrauenswürdigkeit der aufgezeichneten Transaktionsdaten garantieren. In der Zukunft werden zunehmend sogenannte Smart Contracts im Rahmen der Blockchain-Technologie umgesetzt, die eine vorprogrammierte, selbstausführende Vertragsabwicklung möglich machen. Die Blockchain-Technologie wird unsere IT-Systeme im Laufe der Digitalisierung effektiver und sicherer machen. Damit neue Geschäftsideen mit der Blockchain-Technologie positiv gestaltet werden können, soll dieser Artikel helfen, die komplizierte Technologie besser zu verstehen und mit Hilfe von Anwendungsfällen die Nutzungsmöglichkeiten aufzuzeigen.

39.1 Einleitung

Die verschiedenen Disziplinen können die Blockchain-Technologie aus sehr unterschiedlichen Blickwinkeln betrachten. Für einen Informatiker ist die Blockchain grundsätzliche eine einfache Datenstruktur, die Daten als Transaktionen in einzelnen „Blöcken“ verkettet

N. Pohlmann (✉)
Instituts für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen
Aachen, Deutschland
E-Mail: pohlmann@internet-sicherheit.de

M. Bartsch, S. Frey (Hrsg.), *Cybersecurity Best Practices*,
https://doi.org/10.1007/978-3-658-21655-9_39

und in einem verteilten Netz redundant verwaltet. Die Alternative wäre z. B. eine konventionelle Datenbank, die kontinuierlich repliziert wird. Für die IT-Sicherheitsexperten hat die Blockchain den Vorteil, dass die Daten als Transaktionen in den einzelnen „Blöcken" manipulationssicher gespeichert werden können, das heißt, die Teilnehmer an der Blockchain sind in der Lage, die Echtheit, den Ursprung und die Unversehrtheit der gespeicherten Daten zu überprüfen. Die Alternative wäre hier z. B. ein PKI-System als zentraler Vertrauensdienstanbieter. Für den Anwendungsdesigner bedeutet die Nutzung der Blockchain-Technologie eine vertrauenswürdige Zusammenarbeit zwischen verschiedenen Organisationen, ohne die Einbindung einer zentralen Instanz. Die Alternative könnte hier z. B. ein kostenintensiver Treuhänder sein.

Grundsätzlich sind Blockchains fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind. Damit lassen sich mit Hilfe der Blockchain-Technologie Eigentumsverhältnisse direkter und effizienter als bislang sichern und regeln, da eine lückenlose und unveränderliche Datenaufzeichnung hierfür die Grundlage schafft.

Die Blockchain-Technologie stellt mit unterschiedlichen Sicherheitsmethoden ein „programmiertes Vertrauen" zur Verfügung.

Nach einer Studie, die der eco-Verband in Auftrag gegeben hat, glaubt der Mittelstand an die Blockchain-Technologie. Die Blockchain setzt sich für bestimmte Anwendungsfälle und Branchen in der Breite durch – das denken 44 Prozent der Mittelständler. Neun Prozent der befragten Unternehmen planen bereits konkret den Einsatz einer Blockchain im eigenen Unternehmen. 17 Prozent der Befragten denken immerhin über den Einsatz in ihrem Unternehmen nach. Drei Prozent der Mittelständler nutzen die Blockchain bereits. Nur 26 Prozent glauben nicht an diese Technologie, 30 Prozent sind unschlüssig oder machen keine Angaben [1].

Die IT-Marktführer in den USA bauen ihre IT-Systeme und Dienstleistungen in der Regel auf zentrale Dienste auf. Dazu passt das Konzept der Blockchain-Technologie nicht wirklich! Da wir in Deutschland und in der EU sehr viel mehr KMUs haben, ist die Blockchain eine ideale IT-Technologie, die eine vertrauenswürdige verteilte Zusammenarbeit ermöglicht. Aus diesem Grund werden wir mit Hilfe der Blockchain-Technologie in vielen Bereichen den Digitalisierungsprozess beschleunigen, aber auch sicherer und vertrauenswürdiger umsetzen können.

Damit neue Geschäftsideen mit der Blockchain-Technologie positiv gestaltet werden können, soll dieser Artikel helfen, die komplizierte Technologie besser zu verstehen und mit Hilfe von Anwendungsfällen die Nutzungsmöglichkeiten aufzuzeigen.

„Geschichte" der Blockchain Als „Satoshi Nakamoto" an der Bitcoin-Kryptowährung arbeitete, benötigte er eine dezentrale, öffentliche und vor Manipulationen geschützte Datenstruktur, auf welcher die einzelnen Transaktionen gespeichert werden konnten und dabei noch öffentlich einsehbar waren. Sozusagen ein öffentliches Transaktionsbuch (Distributed Ledger). Da dies mit traditionellen relativen Datenbanken nicht möglich war, entwickelte er die Blockchain [2].

39.2 Elemente, Prinzipien und Struktur der Blockchain-Technologie

In diesem Kapitel werden die Elemente, Prinzipien und Struktur der Blockchain-Technologie als Grundlagen beschrieben.

Element: Daten Die Blockchain ist eine einfache Datenstruktur, wie eine Datenbank (Siehe Abb. 39.1). Daten werden in der Blockchain in einzelnen, chronologisch miteinander verketteten Blöcken als Transaktionen verwaltet. Die Daten werden in Transaktionen vor Manipulationen gesichert in der Blockchain gespeichert, siehe auch Abschnitt Transkationen. Die Blockchain ist bei jeder Node (Teilnehmer) und damit verteilt und redundant vorhanden, d. h. es besteht eine sehr hohe Verfügbarkeit der Daten und alle Nodes müssten gleichzeitig manipuliert werden. Eine Blockchain kann sehr groß werden, wie z. B. die Bitcoin-Blockchain etwa 115 GByte groß ist, Stand: Mai 2017.

Element: Block Ein Block in einer Blockchain ist ein strukturierter Datensatz, der beliebige Transaktionen mit Daten enthalten kann und vor Manipulationen gesichert ist (Siehe Abb. 39.2). Was die Blockchain interessant macht, ist der sogenannte *Blockheader*. In diesem wird z. B. der jeweilige Hashwert des Blockheaders vom Vorgänger-Block gespeichert. Dieser Hashwert, *HashPrev*, wird dabei über den gesamten letzten Blockheader – inklusive des Hashwertes des Vorgänger-Blockes – generiert, wodurch die Verkettung der Blöcke manipulationssicher umgesetzt werden kann.

Jeder Block in der Blockchain kann im Prinzip gelesen und überprüft werden. In den Blöcken finden sich die verschiedenen Daten als Transaktionen vor, die in der Blockchain gespeichert werden. Blöcke können auf ihre Integrität geprüft werden, indem der aktuelle Hashwert eines Blockes des gespeicherten Hashwertes im Folgeblock (HashPrev) übereinstimmen muss. Dies ist für jede Node ohne weiteres möglich, da jede Node im Normalfall alle Informationen innerhalb eines Blockes lesen kann. Soll ein neuer Block hinzugefügt werden, so kann dieser nicht einfach an die Blockchain angehängt werden. Für jeden neuen Block muss die Richtigkeit des Blockes geprüft werden und mit Hilfe

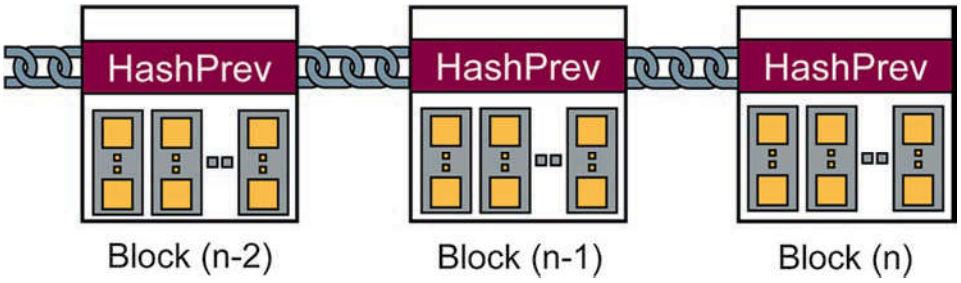


Abb. 39.1 Datenstruktur einer Blockchain

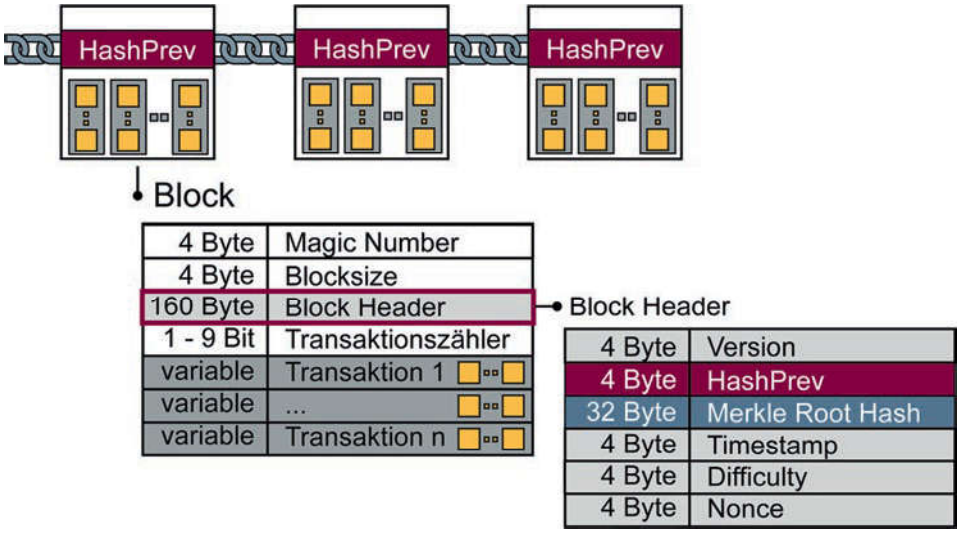
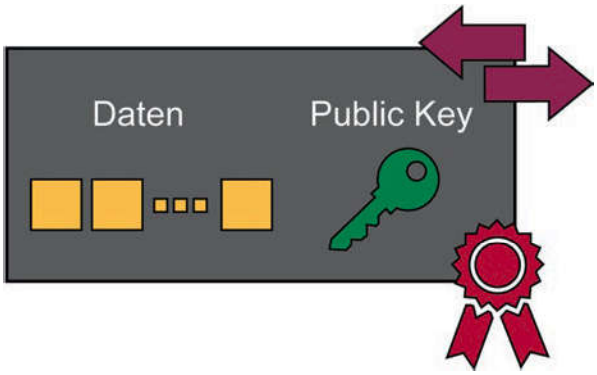


Abb. 39.2 Inhalt eines Blocks

Abb. 39.3 Aufbau einer Transaktion



eines Konsensfindungsverfahrens bestimmt werden, welche Node einen Block hinzufügen darf, damit es nicht möglich ist, die Blockchain zu manipulieren.

Element: Transaktionen Alle Daten innerhalb der Blöcke, werden als „Transaktionen" bezeichnet. Transaktionen enthalten Daten, die in der Zeitfolge protokolliert (chronologisch), nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind (Siehe Abb. 39.3.). Die Daten können Kontostände, Werte, Attribute, Quelltexte, Merkmale, usw. oder allgemein „digital Assets" sein. Eine Transaktion enthält auch immer den Public-Key (Adresse) der Node, der die Transaktion erstellt und signiert hat.

Jede Transaktion, die hinzugefügt werden soll, muss zunächst von der erstellenden Node mit dem Private-Key aus der eigenen Wallet signiert und an alle Nodes über das P2P-Blockchain-Netzwerk gesendet werden. Jede Node im P2P-Blockchain-Netzwerk

kann die Identität der Node, welche die Transaktion erstellt und abgesendet hat, und den Inhalt der Transaktion verifizieren.

Element: Node Jeder, der an der „Blockchain“ teilnimmt, wird als „Node“ beziehungsweise „Teilhaber“ bezeichnet. Jede Node erhält eine aktuelle Kopie der Blockchain, die fortlaufend aktualisiert wird. Jede Node, die zu einer „Blockchain“ gehört, falls diese nicht eingeschränkt ist, hat im Prinzip die gleichen Rechte, die Blockchain zu speichern und neue Blöcke hinzuzufügen (validieren). Jede Node hat eine eigene Wallet und kann Transaktionen mit Daten erstellen, signieren und im Peer-to-Peer-Blockchain-Netzwerk verteilen (Siehe Abb. 39.4).

Element: Wallet Jede Node verfügt über eine „Wallet“. Eine Wallet ist dabei eine Datenstruktur, in der die eigenen Private- und Public-Keys der Node sicher gespeichert sind. Aus dem Public-Key wird mit Hilfe einer Funktion die eindeutige Kennung (Adresse) einer Node berechnet. Mit dem Private-Key signiert eine Node eine Transaktion, die sie erstellt hat (Siehe Abb. 39.5). Mit Hilfe des Public-Keys ist es möglich zu verifizieren, dass die Transaktionen von einer bestimmten Node erstellt wurden.

Abb. 39.4 Inhalt einer Node

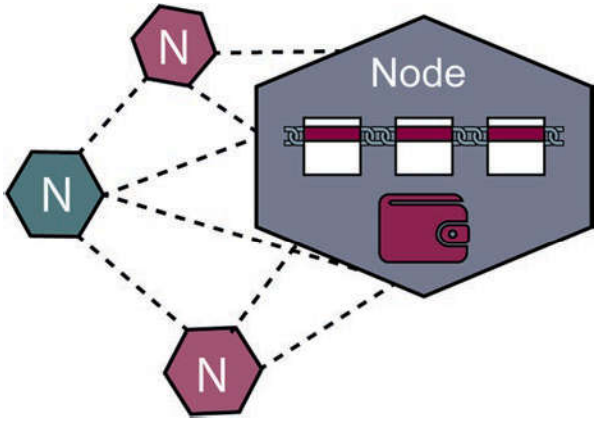
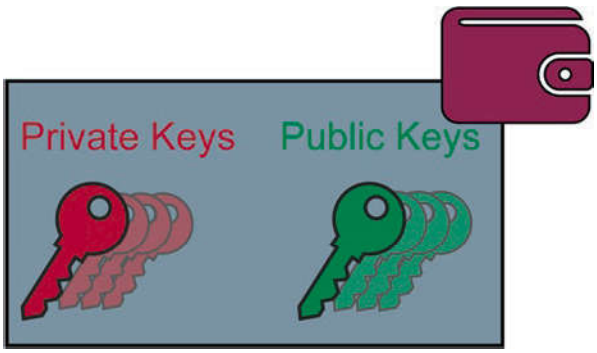


Abb 39.5 Inhalte einer Wallet



Angriffe auf eine Blockchain passieren sehr häufig auf die Wallet der Node, da mit den Private-Keys manipuliert werden kann. Wallets können in verschiedenen Formen existieren bzw. gespeichert werden. Dazu zählt zum Beispiel eine einfache Datei auf der Node. Es ist aber auch möglich, eine Wallet auf einem Sicherheitsmodul, wie z. B. USB-Stick, für Personen oder High-Level-Sicherheitsmodule für Server zu realisieren. Eine weitere Möglichkeit ist es, die Wallet auf einem Papierzettel in Form eines QR-Codes zu halten.

Prinzip: Keine „zentrale Instanz“ Eine Blockchain besitzt keine „zentrale Instanz“, sondern ist auf all ihren Nodes (Teilhabern) in einem Peer-to-Peer-Netzwerk verteilt (Siehe Abb. 39.6). Jeder kommuniziert z. B. über das Internet direkt miteinander. Damit gibt es keinen „Single Point of Failure“ mehr und Logs bzw. Backups müssen nicht besonders berücksichtigt werden, da die Datenstruktur sich selbst regeneriert.

Jeder Block wird mit dem vorherigen Block über den Hashwert (HashPrev) des Blockheaders „verkettet“. Wird versucht innerhalb eines Blockes Daten in Transaktionen zu ändern, so würden die gesamten Hashwerte ab diesem Block „falsch“ werden.

Struktur: Unterschiedliche Arten von Nodes In der Praxis gibt es unterschiedliche Ausprägungen von Nodes (siehe Abb. 39.7). Nodes, die die gesamte Blockchain speichern, werden als „Full Nodes“ bezeichnet.

Für ein portables Gerät, wie zum Beispiel ein Smartphone oder IoT-Geräte, wie Autos, ist es allerdings nicht umsetzbar, eine eventuell mehrere Gigabyte große Blockchain zu speichern. Solche Nodes werden auch als „Lite Node“ bezeichnet. Sie speichern nur die aktuellsten bzw. für sich „relevantesten“ Blöcke wie z. B. Blöcke, an welchen die Node selber teilhatte. Die Wallet ist sicher im Geräte gespeichert. Zudem gibt es auch noch sogenannte „Service Nodes“, welche keine direkten Teilhaber sind. Endgeräte wie Smartphones nutzen einen Dienst, der virtuelle Nodes anbietet. Die Aktivierung der Dienste müssen bei den Service Nodes sicher umgesetzt werden, um Missbrauch zu vermeiden.

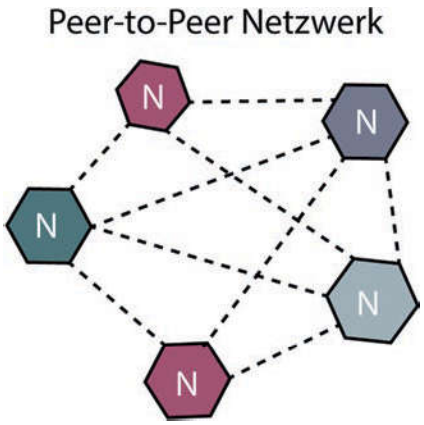


Abb. 39.6 Verteilung der Nodes untereinander

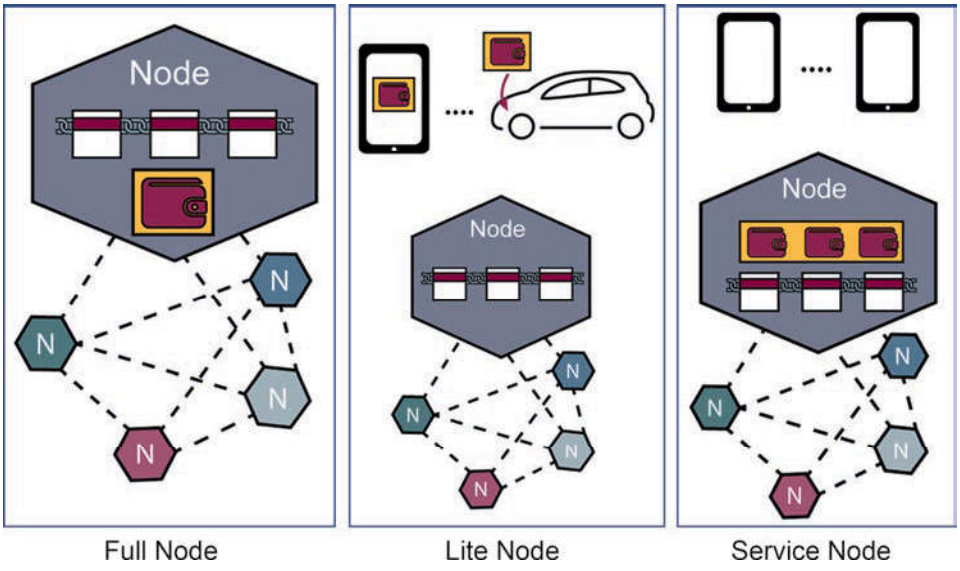


Abb. 39.7 Verschiedene Arten von Nodes/Wallets

Struktur: Konsensfindungsverfahren Alle Transaktionen werden von den entsprechenden Nodes signiert, die für die Daten in der Transaktion verantwortlich sind und an alle anderen Nodes über das Peer-to-Peer-Netzwerk verteilt. Ein Konsensfindungsverfahren bestimmt, welche Node einen neuen Block validieren und an die Blockchain „hängen" darf [3]. Diese Node überprüft, ob die Transaktionen von Semantik und Syntax her richtig sind und ob die digitalen Signaturen des Initiators der Transaktionen mit der Adresse übereinstimmen. Dann wird ein neuer Block mit HashPrev und Merkle Root Hash generiert und an alle Nodes verteilt. Jede Node hat dadurch jederzeit eine Kopie der aktuell gültigen Blockchain.

Dieses Prinzip des Distributed Consensus macht die Konsistenzprüfung der Transaktionen vollkommen unabhängig von einer einzelnen vertrauenswürdigen Instanz. Für die Herstellung des Konsenses zwischen den Nodes, wer für den Abschluss neuer Transaktionen und das Hinzufügen eines bestimmten Blocks an die Blockchain verantwortlich ist, gibt es verschiedene Verfahren.

Proof of Work-Konsensfindungsverfahren Proof of Work ist die aktuell gebräuchlichste Methode zur Konsensfindung und wird z. B. aktuell von der Bitcoin-Blockchain genutzt.

Hier konkurrieren die einzelnen Nodes als sogenannte „Miner" untereinander, indem sie jeweils ein mathematisches Problem – dessen Schwierigkeit sich dynamisch ändern lässt – lösen müssen. Jeder Miner einer Node muss einen Hashwert für einen Block finden, der einem bestimmten vorgegebenen Muster entspricht. Dieses Muster wird vom Netzwerk eigenständig festgelegt, wobei die Schwierigkeit sich mit der Anzahl der vorgegebenen Stellen des Musters erhöht. Zum Beispiel soll ein Hashwert 5 führende Nullen als Muster besitzen.

Die einzige Möglichkeit für die Nodes, einen anderen Hashwert zu erzeugen, ist es, den NONCE-Wert eines Blockes, ein bestimmter Wert, welcher jede Zahl enthalten kann, zu verändern. Somit wird die Konsensfindung eines Blockes zu einem Glückspiel für die Miner in einer Node, da diese nun einen NONCE-Wert finden müssen, der den zu suchenden Hashwert ergibt. Der Miner, der dieses Problem als erstes gelöst hat, darf den Block an die Blockchain anhängen. Die Komplexität des Problems wird in der Praxis so gewählt, dass die Aufgabe im Schnitt 10 Min. dauern soll. Das bedeutet, dass die Transaktionen nur alle 10 Min. in einen Block der Blockchain hinzugefügt werden und gültig sind Abb. 39.8.

Die Berechnung des mathematischen Problems beim Proof of Work-Konsensfindungsverfahren kostet sehr viel Energie. Bei Bitcoin werden pro Tag Stromkosten von 2,8 Mio. US-Dollar verbraucht, 1,3 Giga-Watt, das sind ca. 10 US-Dollar pro Transaktion. Solange eine Node nicht die Mehrheit an Miner-Kapazitäten besitzt (mehr als 50 %), ist das Mining-Prinzip robust und nicht zu kompromittieren. Ein weiteres Problem ist, dass der Zeitraum der Validierung sehr hoch ist.

Proof of Stake-Konsensfindungsverfahren Bei dieser Methode der Konsensfindung wird z. B. die Node gewählt, die die meisten Anteile an Blöcken einer Blockchain hinzugefügt hat. Dieses Verfahren merzt einige Sicherheitslücken aus, die bei Proof of Work-Problemen vorhanden sind. Es ist zum Beispiel für einen Angreifer nicht mehr möglich, eine beliebige Anzahl an „Pseudo Miners“, welche falsche Blöcke als richtig validieren, dem Netzwerk ungesehen hinzuzufügen. Zudem hätte z. B. die Node mit den meisten Coins das größte Interesse an einer stabilen und sicheren Blockchain. Zudem müsste ein Angreifer erst einmal so viele Coins besitzen, dass er Blöcke erstellen darf. Mit einer Attacke würde er sich also im Grunde selbst angreifen. Da der Konsensmechanismus sehr auf „Vertrauen“ basiert, wird dieses Verfahren eher bei privaten Blockchains genutzt.

Alternative Konsensfindungsverfahren Neben den beiden Grundmethoden gibt es noch weitere, sich aktuell in der Probephase befindliche Methoden zur Konsensfindung. Ein Verfahren ist das sogenannte „Byzantine Fault Tolerance“ Verfahren, das eigentlich zur

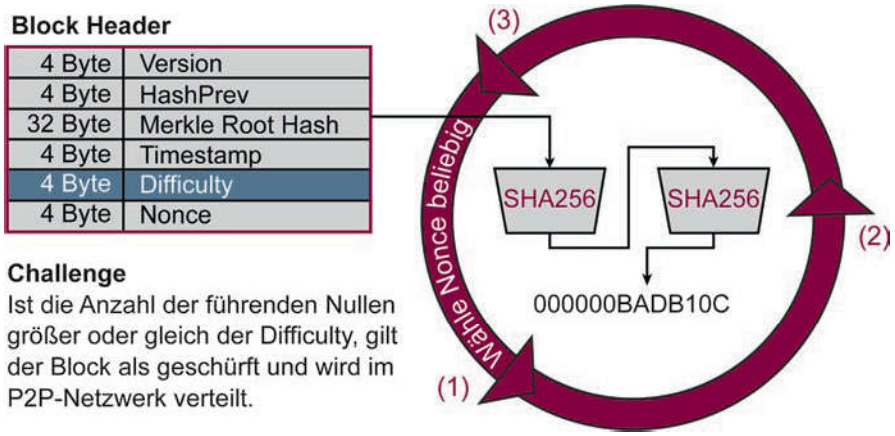


Abb. 39.8 Mining (Proof of Work)

Ermittlung von defekten Sensoren genutzt wird. Damit soll ermittelt werden, welche Node in einer Blockchain versucht, kompromittierte Blöcke an die Blockchain anzuhängen.

Struktur: Berechtigungsarchitektur Eine Blockchain kann sowohl für jeden zugänglich, als auch nur für bestimmte Nodes (Teilnehmer) einsehbar und nutzbar sein. Es wird zwischen den Zugriffsberechtigungen der Nutzung einer Blockchain und der Validierungsberechtigung, Blöcke hinzuzufügen, unterschieden (Abb. 39.9). Bei den Zugriffbeschränkungen wird festgesetzt, wer überhaupt auf eine Blockchain zugreifen darf. Bei einer Public Blockchain darf jede Node uneingeschränkt die Blockchain nutzen. Bei einer Private Blockchain dürfen nur klar definierte Nodes zugreifen. Die Validierungsberechtigungen sagen dagegen aus, welche Nodes Blöcke einer Blockchain hinzufügen dürfen. Auf „Permissioned"-Blockchains dürfen nur bestimmte Nodes, wohingegen auf „Permissionless"-Blockchains alle Nodes Blöcke einfügen dürfen.

Public permissionless Diese Struktur ist die zurzeit am besten erprobte Blockchain-Struktur. Eine solche Blockchain kann jeder einsehen und auch jede Node im Prinzip Blöcke hinzufügen. Dabei ist die Identität der Node, welche die Blockchain einsieht und/oder Blöcke dieser Blockchain hinzugefügt hat, nicht mehr nachzuweisen. Dieses Modell wird unter anderem für die Blockchain der Kryptowährung Bitcoin verwendet. Hier kann jeder von der Blockchain lesen und jede Node als Miner Blöcke der Blockchain hinzufügen, wenn sie die Challenge gewinnt.

Private permissionless Diese Art der Blockchain verpflichtet die Nodes sich zunächst zu registrieren, um Zugriff auf die eigentliche Blockchain zu erlangen. Danach kann jedoch jeder registrierte Node Blöcke zu der Blockchain hinzufügen. Diese Art der Blockchain ist die am wenigsten genutzte Art.

Private permissioned Die restriktivste Blockchain Variante ist eine private permissioned Blockchain, die nicht öffentlich lesbar und auch nicht für alle Nodes beschreibbar ist. Die einzelnen Blöcke dürfen nur die Nodes einer Transaktion und eventuell eigens dazu berechtigte Nodes einsehen. Ansonsten ist es unmöglich für außenstehende Nodes, die Blöcke der Blockchain einzusehen.

		Validierung	
		Permissionless	Permissioned
Zugriff	Public	„Jeder darf lesen und validieren."	„Jeder darf lesen, nur Berechtigte validieren."
	Private	„Nur Berechtigte dürfen lesen, jeder darf validieren."	„Nur Berechtigte dürfen lesen und validieren."

Abb. 39.9 Berechtigungsarchitektur

Dieses mehr lokalisierte Modell eignet sich vor allem für Unternehmen, die die Vorteile der Blockchain nutzen wollen, jedoch keine öffentliche Einsicht in ihre Trankaktionen bzw. Daten geben möchten.

Zum Beispiel möchte eine Bank nicht unbedingt, dass die gesamten Transaktionsdaten ihrer Kunden für jeden (auch für Nicht-Kunden der Bank) öffentlich einsehbar sind. Zudem besitzt eine Bank immer noch eine „zentrale Instanz" und überlässt das Verifizieren und Hinzufügen von Blöcken lieber den eigenen Nodes, denen sie mehr vertrauen kann, als anderen Nodes, welche zu den Kunden gehören.

Public permissioned Bei einer solchen Blockchain sind die Blöcke zwar für jeden einsehbar, allerdings haben nur durch die Organisation ausgewählte Nodes das Recht, Blöcke der Blockchain hinzuzufügen.

Dabei wird die „Wahl zur vertrauenswürdigen Node" zwar nicht dauerhaft festgelegt, allerdings muss diese deutlich klar sein, warum wurde gerade diese „Node" zur „vertrauenswürdigen Node" gewählt. Da in der Regel den Nodes vertraut wird, werden zur Konsensfindung Verfahren, wie zum Beispiel das „Byzatine Fault Tolerance" Verfahren genutzt.

Wird eine Node als kompromittiert angemahnt, so gibt es eine Gruppe an Entscheidern, die die Node überprüfen und darüber entscheiden, ob der Block, den diese Node einfügen möchte, kompromittiert ist oder nicht. Diese „Entscheider" werden „Konsortium" („Consortium") genannt, weswegen eine solche Blockchain auch als „Consortium Chain" bezeichnet wird.

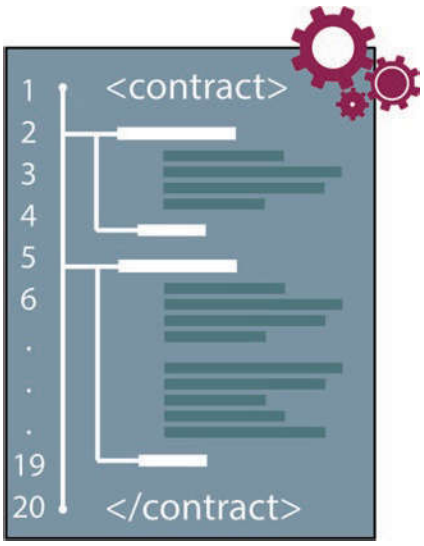
39.3 Anwendungsformen und Anwendungen der Blockchain

Mit Hilfe der Blockchain-Technologien können verschiedene Anwendungsformen und Anwendungen realisiert werden. Im Folgenden werden einige exemplarisch dargestellt.

Anwendungsform „Smart Contracts" In den Blöcken einer Blockchain lassen sich nicht nur Werte, sondern beliebige Elemente in den Transaktionen speichern. So ist es möglich, Quelltext, also ausführbaren Programmcode, abzulegen, der bei einem bestimmten definierten Ereignis ausgeführt wird. Der in einem Block abgelegte Quelltext ist dabei Blockchain-charakteristisch unveränderlich. Diese Idee wird auch als Smart Contracts bezeichnet (Siehe Abb. 39.10.).

Smart Contracts sind Verträge zur „automatisierten" Umsetzung von Vertragsbedingungen über Programmcode. Damit sollen in der Zukunft z. B. Juristen überflüssig werden. Ein Jurist hat bisher die Aufgabe, bei jedem Vertrag die Bedingungen, die dieser Vertrag stellt, nachzuprüfen. Soll beispielsweise für den Kauf eines Autos ein Betrag von einem auf das andere Konto fließen, so muss dies ein Jurist nachvollziehen, bevor der Schlüssel übergeben werden kann. Durch einen Smart Contract soll es nun möglich sein, die Vertragsbedingungen in „Wenn-Dann-Funktionen" einzuteilen. Wenn zum Beispiel eine Node einen

Abb. 39.10 Smart Contracts



bestimmten Betrag auf das Konto einer anderen Node überweist, würde dies der entsprechende Smart Contract merken und beispielsweise den elektronischen Autoschlüssel des Verkäufers für den entsprechenden Käufer freischalten oder – falls es sich bei dem Kauf um ein älteres Auto handelt – den Verkäufer per E-Mail darüber informieren, dass sein Auto verkauft wurde. So kann der Verkäufer dem Käufer den Schlüssel des Autos übergeben.

Smart Contracts stellen eine Kontroll- oder Geschäftsregel innerhalb eines technischen Protokolls dar und helfen, die Zusammenarbeit zwischen verschiedenen Organisationen vertrauenswürdig und vor allem automatisiert umzusetzen.

Anwendungen, die eine Blockchain-Technologie nutzen Da es in vielerlei Hinsicht Bemühungen gibt, Firmen und Entwickler für die Blockchain zu begeistern, stellt sich die Frage, was mit der Blockchain-Technologie alles gemacht werden kann.

Kryptowährung Angefangen hatte alles mit der Realisierung der Bitcoin-Kryptowährung, die Banken als dritte Instanz, also als Vermittler zwischen zwei Parteien, überflüssig macht.

Idee und Verfahren von Bitcoin:

Bitcoin ist eine Internetwährung, die verteilt, dezentral und unabhängig von einer Zentralbank ein globales Zahlungsnetzwerk zur Verfügung stellt. Die Funktionsweise des Bitcoin-Systems stellt sicher, dass es in ein paar Jahrzehnten maximal 21.000.000 Bitcoins weltweit geben wird. Die Node, die beim Mining gewonnen hat, bekommt 12,5 Bitcoins als Belohnung (Stand 2017). Jede Person hat eine Wallet und der Public-Key entspricht der Kontonummer. Mit dem Private-Key werden Transaktionen signiert, um Guthaben auf diesem Bitcoin-Konto an eine andere Adresse zu überweisen (public permissionless Blockchain).

Bitcoin hat in Deutschland zurzeit keine gesetzliche Grundlage für die Verwendung eines Zahlungssystems. Der schwankende Kurs ist ein weiterer Grund, warum sich Bitcoin nicht als globales Zahlungssystem im Alltag durchgesetzt hat. Bitcoin ist aber dennoch eine sehr relevante Währung, vergleichbar mit z. B. Gold. Am 07.12.17 um 21:45 Uhr waren ca. 16,65 Mio. Bitcoins vergeben und ein Bitcoin hatte einen Wert von **12.559,45 €**. Damit sind alle Bitcoin zusammen, d. h. die Bitcoin-Blockchain, über 209 Mrd. € wert.

Weitere Zahlungssysteme Die Banken gingen nach dem ersten Schock selbst in die Offensive und stellten Forscherteams zusammen, mit dem Ziel, die Blockchain-Technik für sich selber nutzbar zu machen.

Die Schweizer Bank UBS möchte beispielsweise ihre eigene digitale Währung entwickeln, den sogenannten „Utility Settlement Coin", kurz USC. Zum Einsatz kommen soll die Währung beim Handel an der Börse mit dem Ziel, Clearinggesellschaften zu ersetzen, die sich bisher um die Geld- und Wertpapiertransfers gekümmert haben. So lassen sich Tage beim Transfer einsparen, da sich Geld und Wertpapiere sofort durch einen neu hinzugefügten Block austauschen lassen. Smart Contracts regeln dabei die automatische Überweisung der USC des Käufers an den Verkäufer. Nach Angaben der UBS ist der Utility Settlement Coin keine parallele Währung wie der Bitcoin, sondern basiert auf realen Werten. 2018 soll das Projekt in die Tat umsetzt werden. Einige Banken haben ihre Beteiligung an dem Projekt zugesichert, unter anderem die Deutsche Bank. Die Bundesbank arbeitet zusammen mit der Deutschen Börse an einem ähnlichen Prototyp, der noch mehrere Jahre Entwicklungszeit benötigt. Eine private permissioned Blockchain wird für Wertpapiere und den Transfer von USC eingesetzt. Full Nodes befinden sich bei den Banken, die mit den Wertpapieren handeln. Für Kunden würden Light Nodes infrage kommen, die nur die für den Kunden wichtigen Blöcke mit den entsprechenden Wertpapieren abspeichern.

Der RSCoin wurde von Forschern für die britische Zentralbank entworfen und ist eine Kryptowährung, die zentral verwaltet werden soll. Die Blockchain ist immer noch dezentral, jedoch weist die Zentralbank das Recht auf Einträge in diese mit Hilfe von kryptographischen Schlüsseln anderen Parteien, wie zum Beispiel Geschäftsbanken, zu. Begrenzte Geldmengen, sieben Transaktionen pro Sekunde und das Proof-of-Work-Problem, wie es bei Bitcoin zum Einsatz kommt, fallen weg. Zweitausend Transaktionen pro Sekunde sollen verarbeitet werden. Was bleibt, ist die Pseudoanonymität des Nutzers. Werden keine zusätzlichen Maßnahmen für den Schutz der Privatsphäre getroffen, entsteht ein transparenter Nutzer, dessen Transaktionen immer und überall nachverfolgt werden können. Zudem ist, wie bei der Schweizer Bank UBS, eine private permissioned Blockchain vorstellbar, damit nicht in bestehende Transaktionen eingesehen werden kann. Andere Parteien, die die Blockchain verändern wollen, können Light Nodes oder Service Nodes einrichten.

Im Bereich rund um die Bezahlung von Dienstleistungen, Inhalten und Rohstoffen werden ebenfalls Überlegungen und Lösungen präsentiert.

Das Startup-Unternehmen Pey möchte Firmen auf einfachem Wege ermöglichen, ihren Mitarbeitern Teile des Gehalts in Bitcoin auszuzahlen. Pey arbeitet mit dem Dienst „PayrollAPI“ von Bitpay, der den Umtausch von Euro in Bitcoin und die Auszahlung an die Arbeitnehmer übernimmt. Das Geschäftsmodell sieht vor, die Nutzung zunächst kostenlos anzubieten und später eine Gebühr von einem Euro pro Mitarbeiter pro Monat einzuführen. Die Mitarbeiter müssen sich zunächst auf der Pey-Plattform anmelden und den Wert, den sie von ihrem Gehalt umwandeln wollen, eintragen.

Ein Ärgernis für Inhalte-Anbieter sind Ad-Blocker. Viele finanzieren sich durch die auf ihrer Seite gezeigte Werbung. Für Ad-Block-Nutzer, aber auch um allgemein mit den bereitgestellten Informationen Geld zu verdienen, gibt es Paywalls. Gegen Bezahlung wird ein Inhalt für den Leser freigegeben. Das deutsche Bitcoin-Startup „Satoshipay“ möchte die Zahlung für Paywalls leichter machen. An den Browser wird ein Online-Wallet angedockt, worüber die Inhalte mit einem Klick bezahlt werden. Den Dienst von Satoshipay zahlt der Inhalte-Anbieter mit 10 % seines Verdienstes. Gefördert wird das Startup von Axel Springer und Visa. Das Wallet soll zukünftig auch mit der Visa-Karte aufgeladen werden können. Zudem sind Bezahlungen in die andere Richtung geplant, sprich der Anbieter zahlt seinen Nutzern für die Teilnahme an Umfragen oder Tests Geld.

Große Energiekonzerne wie RWE wollen gleich mehrere Probleme mit der Blockchain-Technologie lösen. Bei der Elektro-Mobilität gibt es zum einen kein einheitliches Bezahlsystem für das Aufladen von E-Autos und zum anderen ist die Reichweite dieser im Vergleich zu Autos mit Verbrennungsmotoren geringer.

Ladesäulen werden von verschiedenen Energiekonzernen angeboten. Jedes Unternehmen hat eine andere Art der Bezahlung. Bei längeren Fahrten, bei denen öfter an einer Ladestation haltgemacht werden muss, ist es also schwierig, eine Säule passend zum eigenen Bezahlsystem zu finden. RWE hat sich an dieser Stelle mit dem Startup „Slock.it“ zusammengesetzt und an einer Blockchain-basierten Lösung mittels Smart Contracts gearbeitet. Ladesäulen sollen nur noch mit dem Auto kommunizieren und die Bezahlung automatisch abwickeln. Diese Entwicklung würde RWE auch bei einem anderen Projekt helfen. Micropayments sind Bezahlungen z. B. im Cent-Bereich und sind in großen Massen sehr aufwändig und teuer. Durch Smart Contracts wäre dies wiederum einfach und schnell. Es kann genutzt werden, um Ladungen an Ampeln für E-Autos zu ermöglichen, wie RWE es für die Zukunft plant. Dadurch würde auch die Reichweite von E-Autos verbessert, da die Aufladung automatisch und problemlos während der Rotphase an einer Ampel geschieht und so weite Strecken zurückgelegt werden können.

Da es unsinnig ist, eine komplette Blockchain in einem Auto zu speichern, sind betreffende E-Autos Light Nodes.

Manipulationssicherheit von Zuständen Eine weitere Idee ist, das Manipulieren von Tachometern bei Autos zu erkennen und damit einen Betrug zu verhindern. Das Verfahren könnte dabei wie folgt funktionieren: Wird ein Auto gestartet, so wird eine Transaktion mit dem Kilometerstand gesendet. Dies ermöglicht, eine Manipulation des Tachometers zu erkennen. Aber auch Versicherungen können so einfach die gefahrenen Kilometer berechnen und den Vertrag entsprechend anpassen.

Elektronische Auktion In der Ukraine wurde im Februar 2016 die erste elektronische Auktion mit einer Blockchain durchgeführt. Dies geschah testweise und soll die Welt der Auktionen einfacher und vor allem sicherer machen. Ein Block der Kette fungiert hierbei als eine private Handelsplattform, die eine Schnittstelle für Interessenten und Auktionäre bereitstellt. Hier kann nun für das Objekt der Wahl geboten werden. Es können auch feste Anfangsgebote gesetzt werden. Durch das Zahlen einer Teilnahmegebühr ist ein Teilnehmer mit seinem Bankkonto oder einem Konto für Kryptowährungen mit einer API des Systems verbunden und kann bei einem Kauf sofort das ersteigerte Objekt bezahlen.

Der Code, um nach diesem Prinzip elektronische Auktionen zu starten, ist frei erhältlich. Denkbar ist für Auktionshäuser, dass eine private permissonless Blockchain erstellt wird, damit jeder, der registriert ist, unkompliziert mitbieten kann.

Supply Chain Hier ist z. B. die Idee, eine automatische 3D-Druck-Produktions-, Bezahl- und Lieferkette umzusetzen. Nach der Bestellung wird die Konstruktion des gewünschten Teils an die Blockchain gesendet (one time use only). Die Produktion druckt dann automatisch das gewünschte Teil (pay per use). Nach dem 3D-Druck läuft die Zahlung automatisch. Das gedruckte und bezahlte Teil ruft den Versanddienst automatisch (Siehe Abb. 39.11).

Identity Management Große Vorteile können auch für das Identity-Management gefunden werden. Jeder Mensch trägt seinen Personalausweis oder andere Ausweisdokumente mit sich. Die persönlichen Informationen liegen schriftlich wie digital vor. Im Grunde genommen haben wir keine Kontrolle darüber, wer was sehen darf. Kauft ein Jugendlicher einen Film oder ein Spiel, der erst ab sechzehn oder achtzehn freigegeben ist, muss er seinen Personalausweis vorzeigen, um zu bestätigen, dass er das betreffende Alter erreicht hat. Einzusehen sind aber auch andere Daten, wie der vollständige Name und die Adresse. Das Unternehmen ShoHei bietet ein Konzept zu einer Blockchain-basierten Lösung an. Alle persönlichen Daten werden in einem Block gespeichert. ShoHei nutzt dazu den

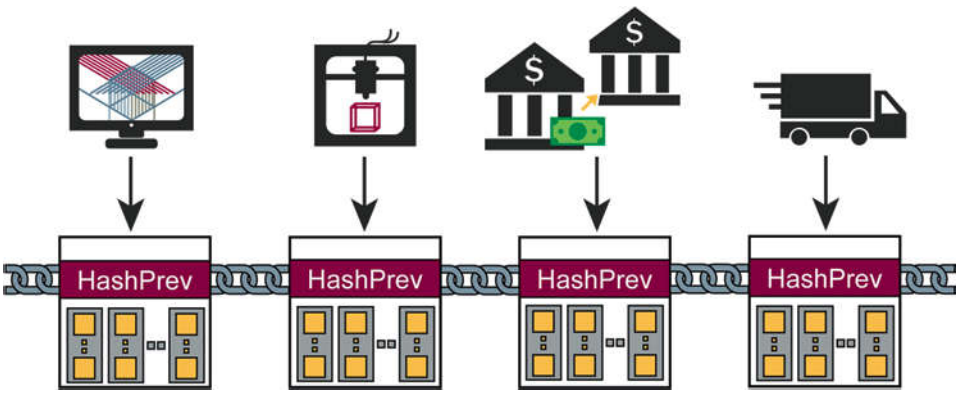
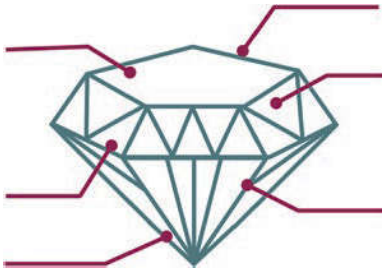


Abb. 39.11 Supply Chain

Abb. 39.12 Diamantenhandel



BlockCypher Blockchain Service. Es soll unter anderem möglich sein, sich mit dem Handy auszuweisen. Der Identifikationsnachweis geschieht dabei biometrisch. Nach der Identifikation kann festgelegt werden, welche Daten gezeigt werden sollen. Da die Blockchain nicht manipuliert werden kann, ist diese Technologie zum Identifizieren von Personen in vielen Lebensbereichen hilfreich, nicht zuletzt für die EU und die Anforderung nach mehr Sicherheit beim Überprüfen von auffälligen Flüchtlingen.

Da vertrauliche Daten verwaltet werden, sollten Full Nodes nur in den entsprechenden Ämtern stehen und die genutzten Smartphones als Light Nodes dienen, die nur die eigenen Blockdaten speichern.

Diamantenhandel Im Diamantenhandel werden alle Edelsteine zertifiziert. Unter anderem wird vermerkt, wem diese gehören und was für eine Qualität vorliegt. Es ist kaum zu glauben, aber so ist eine Zettelwirtschaft entstanden, die Kriminellen in die Hände spielt und es Behörden nicht leicht macht, Fälschungen oder Betrüger schnellstmöglich in Kontrollen zu entlarven. Selbst Datenbanken wurden gehackt und Tausende von Informationen verändert. Bei der Diamantenhandel-Blockchain werden alle Diamanten aufgenommen mit Informationen über den Besitzer, die Qualität und mehr als vierzig Merkmalen, die diesen Diamanten auszeichnen (Siehe. Abb. 39.12).

Wird der Diamant X von Person A an Person B verkauft, wird an die Blockchain einfach ein neuer Block gehängt mit den Informationen von Diamant X, nur dass als Besitzer Person B eingetragen ist. Mehr als 800.000 Diamanten wurden bereits eingetragen. Minengesellschaften, Händler und Versicherer unterstützen diese Art der Verwaltung.

39.4 Blockchain-as-a-Service

Da die Blockchain-Technologie nicht nur in der IT-Branche große Fortschritte bringen soll, sondern in möglichst vielen Arbeitsbereichen, die jedoch das nötige Wissen für den Umgang mit einer solchen IT-Technik nicht mitbringen, wird die Blockchain-Technologie auch „Blockchain-as-a-Service“ angeboten.

Hierbei handelt es sich um vorgefertigte Blockchain-Lösungen, die bei Unternehmen eingepflegt werden. Zwei große Anbieter sind IBM und Microsoft.

Microsoft widmet sich unter dem Projektnamen „Bletchley“ der Verkettung und bietet in seinem Clouddienst „Azure“ den Aufbau einer eigenen Blockchain und deren Verwaltung an. Nodes können einfach festgelegt und entweder mit einem Passwort oder einem SSH Key gesichert werden. Zusätzlich können bestimmte Pakete eingebunden werden, wie zum Beispiel das „Ethereum Studio“ für 0,001$ je Stunde zuzüglich der Kosten für die Azure Infrastruktur. Hiermit können Smart Contracts erstellt und getestet werden. Die Einbindung ins Netzwerk geschieht nach Abschluss aller Tests einfach mit einem Klick. Microsoft möchte mit seinem Angebot besonders Entwicklern entgegenkommen. Für Visual Studio gibt es Erweiterungen, die es erlauben, Smart Contracts zu erstellen, wodurch später der Umstieg auf Ethereum vereinfacht werden soll.

IBM bietet seine Blockchain-Lösung ebenfalls im eigenen Clouddienst „Bluemix“ an. Mit mehr Sicherheit und einer schnelleren Verwaltung richtet sich das Angebot gezielt an Unternehmen. Die Blockchain-Technologie kann zunächst mittels vier bereitgestellter Nodes und einer Zertifizierungsstelle in einer virtuellen Umgebung getestet werden. Zudem werden Beispiel-Code und Beispiel-Apps zur Verfügung gestellt. Entscheidet sich ein Unternehmen, den Dienst in Anspruch zu nehmen, wird eine einzelne isolierte Umgebung aufgebaut, deren Miete 10.000 Dollar im Monat kostet. Smart Contracs stehen hier ebenso im Fokus wie bei Microsoft. Informationen von IoT-fähigen Geräten sollen integriert werden, um als Auslöser der Verträge zu dienen. Als zusätzliche Hilfe sollen in Großstädten wie New York, London und Tokyo Anlaufstellen entstehen, in denen Unternehmen und Entwickler Hilfestellungen zu verschiedenen Problemstellungen bekommen.

IBM ist Teil des von der Linux Foundation ins Leben gerufenen „Hyperleger“ Projekts. Das Projekt kümmert sich um die Festlegung von Standards im Umgang mit der Blockchain-Technologie.

39.5 Sicherheit und Vertrauenswürdigkeit von Blockchains

Damit eine Blockchain sicher und vertrauenswürdig langfristig genutzt werden kann, müssen z. B. die folgenden Aspekte berücksichtigt werden.

Das verwendete *Public-Key-Verfahren* und *Hashfunktionen* müssen dem *Stand der Technik* genügen und die passenden Schlüssellängen müssen verwendet werden. Außerdem müssen langfristig Post-Quantum Kryptoverfahren berücksichtigt und genutzt werden. Die Lebensdauer einer Blockchain muss von Anfang an berücksichtigt werden. In der BSI – Technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ steht z. B. beschrieben, welche kryptographische Verfahren und Schlüssellängen genutzt werden sollten, damit sie für die nächsten 10 Jahre als sicher gelten: Für Hashfunktionen SHA-2/SHA-3 mit einer Mindestschlüssellänge von 256 Bit. Für Public-Key-Verfahren bei RSA mit einer Schlüssellänge von mindestens 3000 Bit und für elliptische Kurven mit einer Mindestschlüssellänge von 256 Bit.

Die Sicherheit der Blockchain-Technologie hängt auch von der *Geheimhaltung der privaten Schlüssel* der Public-Key-Verfahren in der Wallet ab. Der private Schlüssel muss geheim

bleiben. Wer immer den privaten Schlüssel einer Wallet besitzt, ist in der Lage, über die gesamten Transaktionen der Wallet zu verfügen. Ein Verlust des privaten Schlüssels bedeutet gleichermaßen, dass sämtliche in der Adresse gespeicherten Transaktionen für immer „verloren" sind. Gefahren bei nicht ausreichendem Schutz des privaten Schlüssels sind z. B.: Der private Rechner des Nutzers wird gehackt (Malware), IoT, z. B. Auto (Light Node) wird gehackt, die Website der Online Wallet (Service Node) wird gehackt, ein nicht ausreichend gesichertes Smartphone wird gestohlen (Light Node). Der Schutz des privaten Schlüssels in der Wallet sollte mit Hilfe von Hardware-Security-Module realisiert werden (SmartCards, Sec-Token, High-Level-Sicherheitsmodule) und unberechtigte Nutzung muss aktiv verhindert werden!

Außerdem müssen bei den Konsensfindungsverfahren die *Randbedingungen überprüft* werden, damit keine Manipulation bei den unterschiedlichen Konsensfindungsverfahren durchgeführt werden kann.

Ein weiterer wichtiger Punkt ist die *vertrauenswürdige Anzeige der Transaktionen*. Hierzu werden einfache und vertrauenswürdige *Blockchain-Viewer* benötigt. Aber auch die Blockchain-Anwendung muss manipulationssicher sein, damit keine erfolgreichen Angriffe umgesetzt werden können.

Wenn die Blockchain an sich eine hohe Sicherheit bietet, werden die Angreifer über die eigentliche Anwendung, die die Blockchain nutzt, angreifen. Daher muss auch die Blockchain-Anwendung manipulationssicher sein, damit keine erfolgreichen Angriffe umgesetzt werden können.

39.6 Zusammenfassung

Die Blockchain-Technologie schafft eine Basis für eine verteilte und vertrauenswürdige Zusammenarbeit und stellt damit ein hohes Potenzial für neue Geschäftsmodelle und Ökosysteme dar. Die Elemente, Prinzipien und Struktur der Blockchain zeigen den technischen Hintergrund und die interessanten Möglichkeiten auf. Für Deutschland und die EU mit sehr vielen KMUs ist Blockchain eine ideale Technologie für eine vertrauenswürdige verteilte Zusammenarbeit. Vertrauensdienste spielen eine immer wichtigere Rolle in der Zukunft! Die beschriebenen Anwendungen der Blockchain zeigen deutlich, dass die Blockchain-Technologie in der Zukunft ein hohes Potenzial für interessante Anwendungen hat.

Literatur

1. https://www.eco.de/2017/pressemeldungen/eco-und-yougov-mittelstand-glaubt-an-die-blockchain.html – letzter Aufruf 07.12.2017
2. C. Kammler, N. Pohlmann: „Kryptografie wird Währung – Bitcoin: Geldverkehr ohne Banken". IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 6/2013
3. R. Palkovits, N. Pohlmann, I. Schwedt: „Blockchain-Technologie revolutioniert das digitale Business: Vertrauenswürdige Zusammenarbeit ohne zentrale Instanz", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 2/2017