Vertrauenswürdige Zusammenarbeit ohne zentrale Instanz

Blockchain-Technologie revolutioniert das digitale Business

Blockchain wird gerne als „Technologie hinter Bitcoins", der digitalen Kryptowährung des Internets, beschrieben. Für sich betrachtet ist die Blockchain-Technologie jedoch weitaus mehr: eine sehr vielversprechende Idee und ein IT-Mechanismus, mit dem Unternehmen, Behörden und weitere Organisationen ohne zentrale Steuerung vertrauenswürdig zusammenarbeiten können. Auf der Grundlage der Blockchain-Technologie lassen sich neue Anwendungen entwickeln und komplett neue Ökosysteme begründen, zum Beispiel in den Bereichen Finanzwesen, Notare, Treuhänder, Einhaltung von Verträgen, Grundbücher, Energiesektor, Identity-Lösungen und Internet der Dinge. Im vorliegenden Artikel geht es um die Technologie und ihre Sicherheitsmechanismen als solche sowie um Anwendungsformen der Blockchain wie Smart Contracts und die Blockchain-Technologie als Dienstleistung. Des Weiteren sehen wir uns die wichtigsten Anwendungsfelder an, auf welchen Blockchain heute bevorzugt zum Einsatz kommt.

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 in den 90er Jahren formulierten Grundlagen der Blockchain-Technologie weiter in ihre aktuelle Form.[1]

Elemente, Prinzipien und Struktur der Blockchain-Technologie

Die Blockchain ist eine einfache Datenstruktur, die nicht, wie es in konventionellen Datenbanken üblich ist, Daten in Tabellen, sondern in einzelnen, miteinander verketteten „Blöcken" verwaltet. Ein Block in einer Blockchain ist dabei ein strukturierter Datensatz, der beliebige Transaktionen mit Daten enthalten kann und vor Manipulationen gesichert ist.

Element: Block

Was die Blockchain besonders interessant macht, ist der sogenannte **„Blockheader"**. In diesem wird zum Beispiel der jeweilige

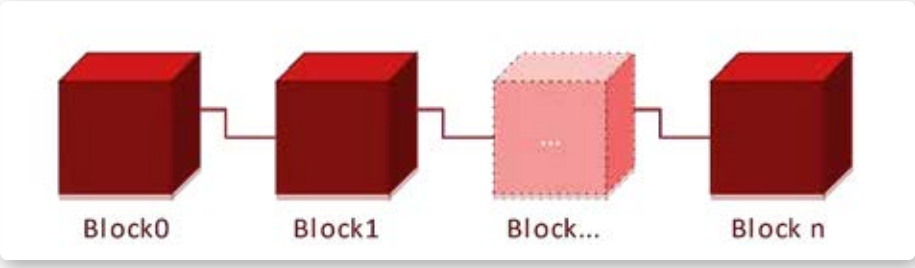

Bild 1: Datenstruktur einer Blockchain

Hashwert des Blockheaders vom Vorgänger-Block gespeichert. Dieser Hashwert wird dabei über den gesamten letzten Blockheader – inklusive des Hashwerts 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 Informationen als Transaktionen, die in der Blockchain gespeichert werden. Blöcke können auf ihre Integrität geprüft werden, indem der Hashwert eines Blockes mit dem gespeicherten Hashwert 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 eines Konsensfindungsve - fahrens bestimmt werden, welche Node einen Block hinzufügen darf, damit es nicht möglich ist, die Blockchain zu manipulieren.

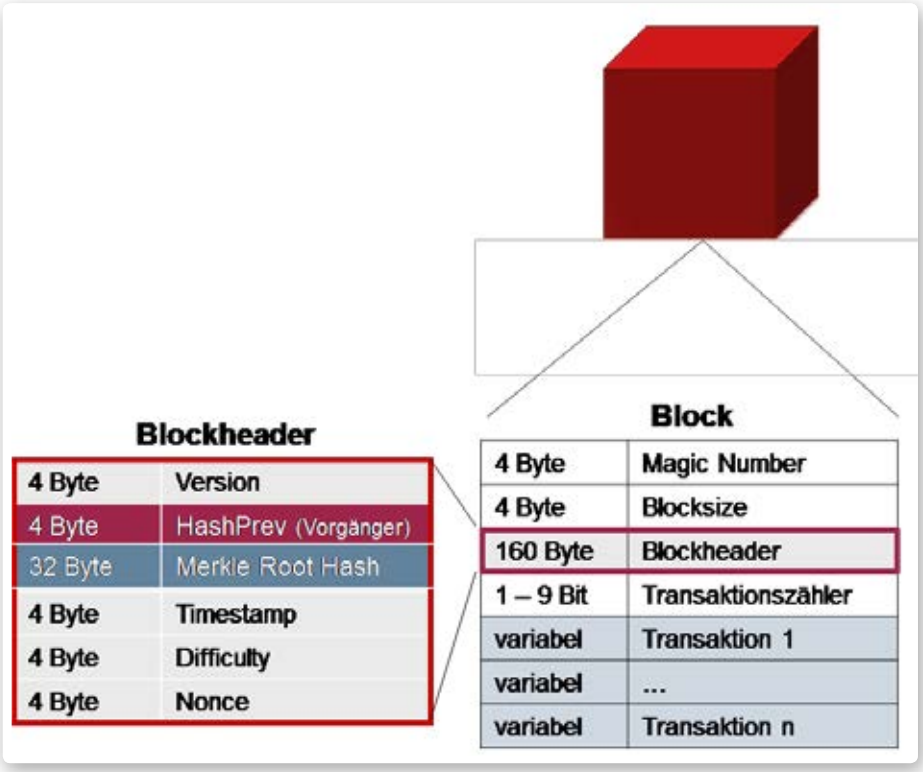

Bild 2: Inhalt eines Blockes

Element: Transaktionen

Alle Informationen innerhalb der Blöcke werden als „Transaktionen" bezeichnet. Eine Transaktion kann Informationen über verschiedene Kontostände, Werte, die verschoben werden sollen, etc., aber auch Quelltext erhalten. Eine Transaktion enthält auch immer den Public-Key (Adresse) der Nodes, welche die Transaktion erstellt und signiert haben.

Jede Transaktion, die hinzugefügt werden soll, muss zunächst von der erstellenden Node mit dem Private-Key aus der Wallet signiert und an alle Nodes über das P2P-Blockchain-Netzwerk gesendet werden (P2P = Peer-to-Peer). Jede Node im P2P-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, die zu einer Blockchain gehört, falls diese nicht eingeschränkt ist, hat im Prinzip die gleichen Rechte, die Blockchain zu speichern und neue Blöcke hinzuzufügen.

Element: Wallet

Jede Node verfügt über eine „Wallet". Eine Wallet ist dabei eine Datenstruktur, in der die eigenen Private- und Public-Keys der Node 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. Mit Hilfe des Public-Keys ist es möglich, zu verifizi - ren, dass die Transaktionen von einer bestimmten Node erstellt wurden.

Angriffe auf eine Blockchain passieren sehr häufig auf die Wallet der Node, da mit den Schlüsseln manipuliert werden kann. Wallets können in verschiedenen Formen existieren beziehungsweise gespeichert werden. Dazu

zählt zum Beispiel eine einfache Datei auf der Node. Es ist aber auch möglich, eine Wallet auf einem Sicherheitsmodul wie zum Beispiel einem USB-Stick zu realisieren. Eine weitere Möglichkeit ist, 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. Jeder kommuniziert zum Beispiel über das Internet direkt miteinander. Damit gibt es keinen „Single Point of Failure" mehr und Logs beziehungsweise Backups müssen nicht besonders berücksichtigt werden, da die Datenstruktur sich selbst regeneriert.

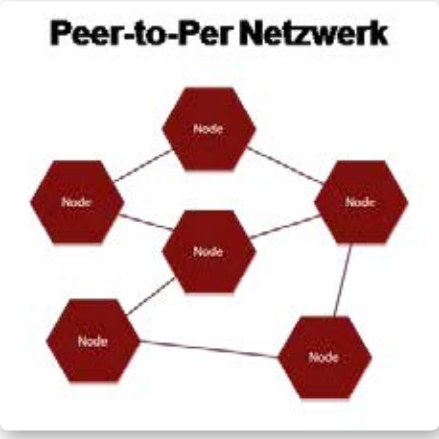

Bild 3: Verteilung der Nodes untereinander

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.

Unterschiedliche Arten von Nodes

In der Praxis gibt es unterschiedliche Ausprägungen von Nodes. Nodes, welche die gesamte Blockchain speichern, werden als „Full Nodes" bezeichnet. Für ein portables Gerät wie zum Beispiel ein Smartphone ist es allerdings nicht umsetzbar, eine eventuell mehrere Gigabyte große Blockchain zu speichern. Solche Nodes werden auch als „Light Node" bezeichnet, welche nur die aktuellsten beziehungsweise für sich „relevantesten" Blöcke wie zum Beispiel Blöcke, an welchen die Node selber teilhatte, speichert. Zudem gibt es auch noch sogenannte „Service Nodes", welche keine direkten Teilhaber sind.

Konsensfindungsverfahren

Eine Transaktion besteht immer aus einem bestimmten Inhalt, der von einer Node signiert wurde und den alle anderen verifizieren können sollen. Der Inhalt ist bei einer Kryptowährung zum Beispiel ein Betrag wie bei Bitcoin oder ein Vertrag bei SmartContracts. Transaktionen müssen, bevor sie einer Blockchain hinzufügt werden, zunächst von einer Node validiert werden. Validieren bedeutet: Überprüfung, ob die Transaktion von Semantik und Syntax her richtig ist.

Das Konsensfindungsverfahren hat die Aufgabe, eine Node auszuwählen, die einen Block in die Blockchain hinzufügen soll. Dabei gibt es unterschiedliche Methoden der Konsensfindung zwischen den Nodes, wer für den Abschluss neuer Transaktionen und das Hinzufügen eines bestimmten Blocks an die Blockchain verantwortlich ist.

Proof of Work – Konsensfindungsverfahren

Proof of Work ist die aktuell gebräuchlichste Methode zur Konsensfindung und wird zum Beispiel 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 Minuten dauern soll. Das bedeutet, dass die Transaktionen nur alle 10 Minuten in einen Block der Blockchain hinzugefügt werden und gültig sind.

Proof of Stake – Konsensfindungsverfahren

Bei dieser Methode der Konsensfindung wird zum Beispiel die Node gewählt, welche die meisten Anteile an Blöcken einer Blockchain hinzugefügt hat. Dieses Verfahren merzt einige Sicherheitslücken aus, die bei Proof of Work 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 zum Beispiel 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 Ermittlung von defekten Sensoren genutzt wird. Damit soll ermittelt werden, welche Node in einer Blockchain versucht, kompromittierte Blöcke an die Blockchain anzuhängen.

Varianten von Blockchain

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. Bei den Zugriffsbeschränkungen wird festgesetzt, wer überhaupt auf eine Blockchain zugreifen darf. Bei einer Public Blockchain darf jede Node (Teilhaber) uneingeschränkt die Blockchain nutzen. Bei einer Private Blockchain dürfen nur klar definierte Nodes darauf zugreifen.

Die Validierungsberechtigungen sagen dagegen aus, welche Nodes Blöcke zu einer Blockchain hinzufügen dürfen. Auf „Permissioned"-Blockchains dürfen nur bestimmte Nodes Blöcke einfügen, wohingegen das auf „Permissionless"-Blockchains alle Nodes dürfen.

Public permissionless

Diese Struktur ist die zurzeit am besten erprobte Blockchain-Struktur. Eine solche Blockchain kann jeder einsehen und auch jede Node kann im Prinzip Blöcke hinzufügen. Dabei ist die Identität der Node, welche die Blockchain einsieht und/oder Blöcke hinzufügt, im Anschluss 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 (Aufgabe bei der Proof of Work – Konsensfindung) gewinnt

Private permissionless

Diese Art der Blockchain verpflichtet die Nodes (Teilnehmer), sich zunächst zu registrieren, um Zugriff auf die eigentliche Blockchain zu erlangen. Danach kann jedoch jeder registrierte Teilnehmer Blöcke zu der Blockchain hinzufügen. Diese Art der Blockchain wird derzeit in der Praxis am wenigsten genutzt.

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 Teilnehmer (Nodes) einer Transaktion und eventuell eigens dazu berechtigte Nodes einsehen. Ansonsten ist es unmöglich für außenstehende Nodes, die Blöcke der Blockchain einzusehen.

Dieses stärker lokalisierte Modell eignet sich vor allem für Unternehmen, welche die Vorteile der Blockchain nutzen wollen, jedoch keine öffentliche Einsicht in ihre Transaktionen beziehungsweise 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 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. Die „Wahl zur vertrauenswürdigen Node" ist dabei immer temporär und muss klar nachvollziehbaren Kriterien folgen. Da in der Regel den Nodes vertraut wird, werden zur Konsensfindung Verfahren wie zum Beispiel „Byzatine Fault Tolerance" genutzt.

Wird eine Node als kompromittiert angemahnt, so gibt es eine Gruppe an Entscheidern, welche 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.

Sicherheit und Vertrauenswürdigkeit von Blockchains

Damit eine Blockchain langfristig sicher und vertrauenswürdig bleibt, 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 muss langfristig Post-Quanten-Kryptografie (PQC, Verschlüsselungsverfahren, die selbst von Quantencomputern praktisch nicht zu entschlüsseln sind) genutzt werden.
- Die Sicherheit der Blockchain-Technologie hängt auch von der **Geheimhaltung der privaten Schlüssel** der Public-Key-Verfahren ab. Der Schutz des privaten Schlüssels sollte mit Hilfe von Security-Token und High-Level-Sicherheitsmodulen realisiert werden.
- Ein weiterer wichtiger Punkt ist die **vertrauenswürdige Anzeige der Transaktionen**. Hierzu werden einfache und vertrauenswürdige **Blockchain-Viewer** benötigt.
- Außerdem müssen bei den Konsensfi - dungsverfahren die Randbedingungen überprüft werden, um Manipulationen auszuschließen.

Anwendungsformen und Anwendungen der Blockchain

Smart Contracts

In den Blöcken einer Blockchain lassen sich nicht nur Werte, sondern beliebige Elemente in den Transaktionen speichern. So ist es möglich, Quelltext (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.

Smart Contracts sind Verträge zur „automatisierten" Umsetzung von Vertragsbedingungen über Programmcode. Damit sollen in der Zukunft Juristen mehr oder weniger 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 fli - ßen, 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 bestimmten Betrag auf das Konto einer anderen Node überweist, würde dies der ent-

sprechende 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.

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 nicht über das nötige Wissen für den Umgang mit einer solchen IT-Technik verfügen, wird die Blockchain-Technologie auch als **„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 Dollar 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 mit einem einfachen Klick.

Microsoft möchte mit seinem Angebot insbesondere 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. Das Angebot soll sich – mit mehr Sicherheit und einer schnelleren Verwaltung – gezielt an Unternehmen richten. 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. Endscheidet sich ein Unternehmen, den Dienst in Anspruch zu nehmen, wird eine einzelne isolierte Umgebung aufgebaut, deren Miete 10.000 Dollar im Monat kostet.

Smart Contracts 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 oder Tokio Anlaufstellen entstehen, in denen Unternehmen und Entwickler Hilfestellungen zu verschiedenen Problemstellungen bekommen.

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

Anwendungen, die eine Blockchain nutzen

Da es in vielerlei Hinsicht Bemühungen gibt, Firmen und Entwickler für die Blockchain zu begeistern, stellt sich die Frage, was sich mit der Blockchain-Technologie alles realisieren lässt.

Kryptowährung

Angefangen hatte alles mit der Realisierung der Bitcoin-Kryptowährung, die Banken als dritte Instanz – also als Vermittler zwischen zwei Parteien – überflüssig macht. 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, Clearing-Gesellschaften zu ersetzen, die sich bisher um die Geld- und Wertpapiertransfers gekümmert haben. So lässt sich der Transfer verkürzen, 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 jedoch 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 zu – mithilfe von kryptographischen Schlüsseln, anderen Parteien, wie zum Beispiel Geschäftsbanken. 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 bestehende Transaktionen nicht eingesehen werden können. Andere Parteien, die die Blockchain verändern wollen, können Light Nodes oder Service Nodes einrichten.

Zurzeit wird mithilfe der Amazon Cloud „Elastic Cloud" in einem kleinen Rahmen getestet. Wird die Nutzung des RSCoin entschieden, wird binnen achtzehn Monaten ein Pilotprojekt gestartet. Im Bereich rund um die Bezahlung von Dienstleistungen, Inhalten und Rohstoffen werden ebenfalls Überlegungen und Lösungen präsentiert.

Gehalt in Bitcoin – „PayrollAPI"

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-Blocker-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 eine Online-Wallet angedockt, worüber die Inhalte mit einem Klick bezahlt werden. Den Dienst von Satoshipay zahlt der Inhalte-Anbieter mit 10 Prozent seines Verdienstes. Gefördert wird das Startup von Axel Springer und Visa. Die 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, zum anderen ist die Reichweite dieser im Vergleich zu Autos mit Verbrennungsmotoren geringer.

Ladesäulen werden von verschiedenen Energiekonzernen angeboten, wobei jedes Unternehmen eine andere Art der Bezahlung hat. Bei längeren Fahrten, bei denen öfter an einer Ladestation haltgemacht werden muss, ist es also schwierig, eine Säule zu finden die zum eigenen Bezahlsystem passt. 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 beispielsweise im Cent-Bereich und 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 die betreffenden 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 auf diese Weise die gefahrenen Kilometer berechnen und den Vertrag entsprechend anpassen.

Als Paywall (Bezahlmauer/Bezahlschranke) wird ein Mechanismus bezeichnet, mit dem bestimmte Inhalte einer Website nur nach dem Bezahlen einer Gebühr oder dem Abschluss eines Abonnements sichtbar sind (Paid Content).[4]

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 Permissionless Blockchain er-

stellt wird, damit jeder, der registriert ist, unkompliziert mitbieten kann.

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 sowohl schriftlich als auch digital vor. Im Grunde genommen haben wir keine Kontrolle darüber, wer was sehen darf. Kauft ein Jugendlicher einen Film, der erst ab 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 BlockCypher-Blockchain-Service. So soll unter anderem ermöglicht werden, sich mit dem Handy auszuweisen; der Identifikat - onsnachweis 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 Identifizi - ren 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 Daten 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 leichtmacht, Fälschungen aufzudecken oder Betrüger schnellstmöglich in Kontrollen zu entlarven. Selbst Datenbanken werden gehackt und Tausende von Informationen verändert.

Bei der Diamantenhandel-Blockchain werden alle aufgenommenen Diamanten mit Informationen über den Besitzer, die Qualität und mehr als vierzig Merkmale, die diesen Diamanten auszeichnen, versehen.

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 770.000 Diamanten wurden bereits eingetragen. Minengesellschaften, Händler und Versicherer unterstützen diese Art der Verwaltung.

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.

Die beschriebenen Anwendungen der Blockchain zeigen deutlich, dass die Blockchain-Technologie in der Zukunft ein hohes Potenzial für interessante Anwendungen hat. ■

Literatur

1 *C. Kammler, N. Pohlmann: „Kryptografie wird Währung – Bitcoin: Geldverkehr ohne Banken". IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 6/2013*

2 *U.J. Froitzheim: „Ungünstige Verkettung". Heise Medien, 1/2017*

3 *J. Heckmann, M. Kaulartz: „Selbsterfüllende Verträge – Smart Contracts: Quellcode als Vertragstext". c't, Heise Medien, Heft 24/2016*

4 *https://de.wikipedia.org/wiki/Paywall*

ROBIN PALKOVITS
studiert Informatik an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit der Blockchain.

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

ISABEL SCHWEDT
studiert Informatik an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit der Blockchain.