Netzwerk des Vertrauens: Blockchain

Im Zuge der Finanzkrise 2008 ersann ein Kryptografie-Experte unter dem Pseudonym Satoshi Nakamoto eine völlig neue, einzigartige und faszinierende Technologie: eine öffentliche und transparente Buchhaltung, deren Buchungen zwischen anonymen Parteien dezentral und sicher auf vernetzten Computern gespeichert werden. Seitdem haben unzählige Artikel die Genialität der Online-Währung Bitcoin gefeiert, das mitgelieferte Buchhaltungssystem namens Blockchain wurde nur am Rande erwähnt. Das änderte sich vor eineinhalb Jahren: Fast alle internationalen Banken testen Anwendungsfälle für die Blockchain-Technologie, ignorieren dabei aber die Währung Bitcoin. Sie forschen am disruptiven Potenzial der Blockchain-Technologie für ihre Geschäftsmodelle: dem Mechanismus, dank dem sich zwei Parteien – Menschen oder Applikationen – in Transaktionen ohne Zwischeninstanz vertrauen können.

Eintrittskarte für die Bitcoin-Blockchain

Der Austausch von Waren auf dem Weltmarkt wird in der Regel über Treuhänder abgewickelt, die das Vertrauen von Käufer und Verkäufer genießen. Die Rolle des Treuhänders kann beispielsweise eine Bank oder ein Notar einnehmen. Meistens sichert eine nationalstaatliche Zentralbank den Wert eines Geldbetrags ab. Egal ob Notar oder Bank: Eine dritte, vertrauenswürdige Partei tritt als Garant auf.

Die Blockchain-Technologie könnte dieses Prinzip grundlegend ändern: Dezentral abgelegte Datensätze synchronisieren sich in einer Blockchain völlig autonom. Dank der Verteilung können Daten nicht verloren gehen oder manipuliert werden. Dadurch braucht die Blockchain keine neutrale Zwischeninstanz.

Die Bitcoin-Blockchain ist ein öffentliches Buchhaltungssystem oder Register, an dem faktisch jeder mit einer sogenannten Wallet teilnehmen kann. Die Wallet ist ein Stück Software, das als Eintrittskarte für die Teilnahme am Bitcoin-Netzwerk dient. In der Wallet verwalten die Nutzer ihre Bitcoins. Sie besteht aus zwei Schlüsseln. Bei der Installation jeder Wallet wird der persönliche *Private Key* generiert. Er gibt Zugriff auf die Wallet. Der öffentliche oder *Public Key* wird mit Hilfe des Private Key generiert. Beide teilen sich eine mathematische Basis.

Jede Transaktion der Wallet wird mit dem Private Key signiert und kann so auf seine Richtigkeit geprüft werden. Der öffentliche Schlüssel kann jedem gezeigt werden, dank asymmetrischer Verschlüsselung kann er nicht auf den privaten zurückgerechnet werden. Einfacher ausgedrückt: Der öffentliche Schlüssel ist wie der Einwurfschlitz eines Briefkastens. Jeder kennt den Standort des Briefkastens, und jeder kann etwas einwerfen. Den Inhalt herausholen kann nur die Person, die über den privaten Schlüssel für die Rückseite verfügt.

Den Urhebern von Blockchain und Bitcoin liegt Anonymität am Herzen. Der öffentliche Schlüssel kann von jedem eingesehen werden, doch niemand weiß, wem der Schlüssel gehört. Damit bleibt die Anonymität von Transaktionen gesichert. Die Technologie ist also transparent und anonym zugleich.

Eine Wallet kann mittels des privaten Schlüssels mehrere öffentliche Schlüssel generieren. Sie erzeugt zum Beispiel pro Transaktion einen Schlüssel, damit jede Adresse jeweils nur einem Handelspartner bekannt ist. Der Besitzer des privaten Schlüssels hat Zugriff auf alle seine öffentlichen Schlüssel und das zugehörige Guthaben. Damit ist für den Handelspartner die Transaktion völlig transparent, für den Rest der Teilnehmer bleibt sie anonym.

Neben der Bitcoin-Blockchain gibt es weitere kryptografische Währungen, zum Beispiel Litecoin, Dogecoin oder Dashcoin. Darüber hinaus arbeiten unzählige Startups an Blockchain-Projekten. Das Ethereum-Projekt [Ethe] beispielsweise wickelt deutlich mehr Transaktionen pro Sekunde ab als die Bitcoin-Blockchain und kann in einem leicht verständlichen JavaScript-Dialekt programmiert werden. Viele junge Unternehmen verwirklichen mit Ethereum ihre Ideen, vor allem mit Smart Contracts.

Bitcoins sind ein Zahlungsmittel – und gleichzeitig eine dezentrale Datenbank. „Geld“ ist nur eine Anwendung neben vielen anderen. Die Smart Contracts der Blockchain-Technologie prüfen autonom und unbeirrbar kausale Zusammenhänge und lösen anschließend definierte Aktionen aus.
(`https://bitcoin.org/bitcoin.pdf`)

Kasten 1: Bitcoins

Vertrauen in Kettenreaktionen

Einzelne Transaktionen oder Buchungen werden mit dem privaten Schlüssel signiert und verifiziert. Im Bitcoin-Netzwerk laufen unzählige Transaktionen auf. Die beteiligten Rechner konkurrieren untereinander, wer am schnellsten die meisten Blöcke mit Transaktionen erstellt. Zum Erstellen eines Blocks ist eine enorme Rechenleistung notwendig, die die Korrektheit der Transaktion und der Blockberechnung gleichzeitig verifiziert und authentifiziert. Sichergestellt wird das mittels kryptografischer und mathematischer Berechnungen.

Die Belohnung von derzeit 25 Bitcoins pro Block erhält der Teilnehmer, dessen Kette die meisten angehängten Blöcke aufweist.

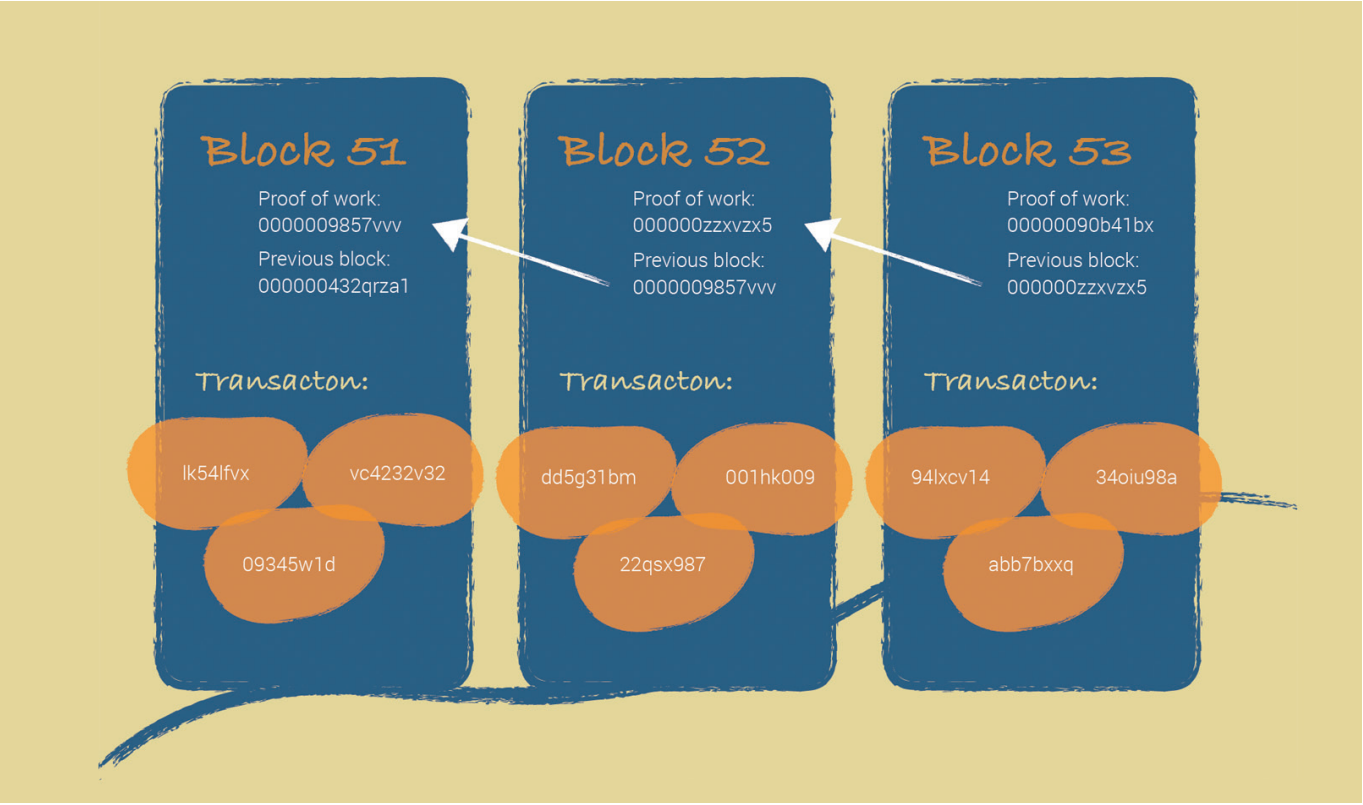

Abb. 1: Blöcke fortschreiben.

Der „Miner" hat also Bitcoins „geschürft." Die längste Blockchain, Deutsch: „Kette", wird vom Netzwerk festgelegt, sobald mehr als 50 Prozent der Rechner eine Blockchain nutzen. Die Computer entscheiden wirtschaftlich, denn nur, wer an die ausgewählte Kette Blöcke angehängt hat, erhält die Belohnung. Daher entscheiden die Rechner, mit welcher Kette des Netzwerks sie ihre Blöcke anhängen. Als Faustregel gilt, dass ein Vorsprung von sechs Blöcken mit keiner Rechenleistung mehr aufgeholt werden kann.

Die Anzahl an Bitcoins ist mathematisch auf 21 Millionen begrenzt. Das wirkt einer stetigen Entwertung wie bei den Fiat-Währungen Euro oder US-Dollar entgegen. Bitcoins und Fiat-Währungen sind im Gegensatz zu Warengeld Zahlmittel ohne inneren Wert.

Jeder Block hat als Prüfsumme eine mathematische Referenz auf den vorherigen Block und eine Prüfsumme auf die komplette Kette. Sobald ein Block an die Kette gehängt wurde, sind dessen Transaktionen unwiderruflich dokumentiert, genau wie all die anderen Transaktionen in den Blöcken vor ihm. Das sichert die Authentizität der Blockchain (**siehe Abbildung 1**).

Die Vertrauenswürdigkeit der Bitcoin-Blockchain manifestiert sich in ihrem seit sieben Jahren nicht gehackten Regelprotokoll. Das Protokoll verifiziert die einzelnen Transaktionen, prüft die Dokumentation dieser Transaktionen und kontrolliert das Generieren der einzelnen Blöcke. Um die Transaktion in einem Block an die Blockchain anzuhängen, muss das Netzwerk einen mehrheitlichen Konsens über das Resultat dieser Prüfungen erreichen.

Die Verbindung aus Buchhaltung mit Bonussystem ermöglicht den sicheren, schnellen und unveränderbaren Austausch von Informationen über ein völlig autonomes Computernetzwerk. Ein Treuhänder oder Dritter ist in diesem Szenario überflüssig (**siehe Abbildung 2**).

Transaktionen auf der Wäscheleine

Ein Bitcoin lässt sich in 100 Millionen Teile zerlegen. Eine Partei kann an jeden Bruchteil eines Bitcoins – auch Satoshi genannt – völlig unterschiedliche Dinge hängen, wie etwa Finanztransaktionen, Geburtsurkunden, Aktien oder Verweise auf eine Datei. Ein Bitcoin ist wie die Wäscheklammer an einer Leine, die ein Foto, einen Socken oder eben einen Euro-Schein festhält.

Der Handel mit Bitcoins und die Wertstellung zu den wichtigsten Fiat-Währungen US-Dollar, Euro und Yuan stellt die bekannteste Verknüpfung mit der Bitcoin-Blockchain dar. Neben Bitcoins gibt es viele andere sogenannte Crypto-Währungen, die auf einer ähnlichen Mechanik aufsetzen und auf einschlägigen Börsen gehandelt werden. Das Bitcoin-Netzwerk hat aktuell die größte Marktkapitalisierung und läuft derzeit am stabilsten.

Mittlerweile gibt es eine ganze Reihe von Start-ups, die ihre Geschäftsidee auf der Blockchain-Technologie aufbauen:

OBJEKTspektrum ist eine Fachpublikation des Verlags:
SIGS DATACOM GmbH · Lindlaustraße 2c · 53842 Troisdorf
Tel.: 02241/2341-100 · Fax: 02241/2341-199
E-mail: info@sigs-datacom.de
www.objektspektrum.de
www.sigs.de/publications/aboservice.htm
SIGS DATACOM
FACHINFORMATIONEN FÜR IT-PROFESSIONALS

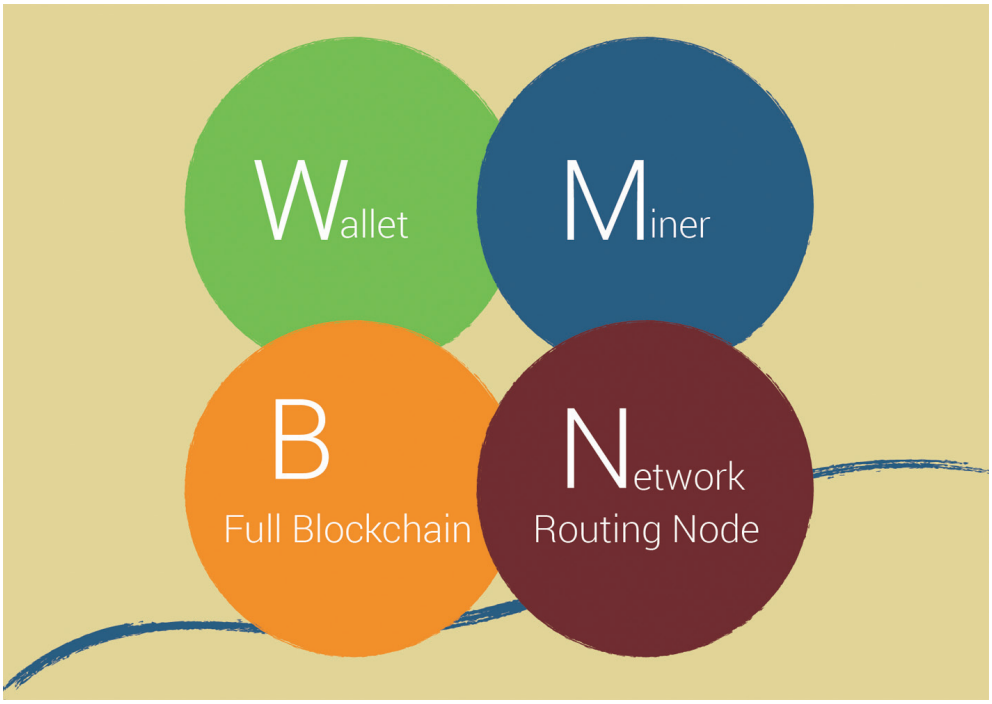

Abb. 2: Aufbau eines Bitcoin-Clients.

- Statt das eigene Apartment eigenhändig zu öffnen, könnte man AirBnB und die Blockchain verknüpfen und über intelligente Schlösser den Zugang automatisieren [SLock].
- Estland ist stark digitalisiert. Jeder Einwohner verfügt bereits über eine elektronische Identität. Die Regierung möchte Aktionärsabstimmungen gemeinsam mit Linq [Nas16] dezentral über die Blockchain-Technologie abwickeln und dadurch die Bürokratie minimalisieren.
- Die Nasdaq hat mit Linq eine Blockchain eingeführt und bereits eine Eigentumsübertragung von Wertpapieren erfolgreich darüber abgewickelt [Nas15].
- Start-ups wie „follow my vote“ [FMV] arbeiten an Wahlen über Blockchain-Technologie.

Das eingebaute Vertrauen der Crypto-Währungen lässt sich beispielsweise für eine Buchhaltung mit zweckgebundenen Budgets einsetzen: Bitcoins oder vergleichbare kryptografische Währungen sind programmierbares Geld. Programmierbar bedeutet: Man kann die Ausgabe an einen Zweck binden – zum Beispiel Budgets. Das Weiterbildungsbudget eines Mitarbeiters wird fest programmiert und kann nur bei bestimmten Anbietern ausgegeben werden. Das reduziert das Arbeitsaufkommen in der Buchhaltung. Das Unternehmen kann auch seine Budgets für Gehälter, Marketing und andere Ausgaben allokieren und so sicherstellen, dass sie wie vorgesehen verwendet werden. Als Sahnehäubchen kann die Bestimmung von Geldern sogar zeitlich begrenzt sein, damit ein Empfänger keine Budgets hortet.

Beispiel Internet der Dinge: Maschinen oder Software können mit dem Konzept „Vertrauen“ nichts anfangen. Das auf Empathie basierende Entscheidungskriterium hilft uns Menschen, den Alltag zu bewältigen. Ein Getränkeautomat und eine Drohne teilen diese Fähigkeit nicht mit uns. Mit der Blockchain-Technologie weiß eine

Links

[Ethe] Ethereum, Blockchain App Platform, siehe: `https://www.ethereum.org/`

[FMV] `https://followmyvote.com/online-voting-technology/blockchain-technology/`

[HaBl] A. Dörner, Handelsblatt, 25.5.2015, siehe:
`http://www.handelsblatt.com/unternehmen/industrie/fahrdienst-gett-vw-steigt-beim-uber-angreifer-ein/13639596.html`

[Nas15] Nasdaq Linq Enables First-Ever Private Securities Issuance Documented with Blockchain technology, 30.12.2015, siehe:
`http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326`

[Nas16] Nasdaq-Pressemeldung, 12.2.2016, siehe: `http://www.nasdaqbaltic.com/?id=3799701`

[SLock] Slock.it – Blockchain + IoT, siehe: `http://www.slock.it/`

Drohne sicher, dass der Automat, dem sie eine Kiste Coca-Cola liefert, auch dafür bezahlt hat. Der Getränkeautomat operiert eigenständig und bestellt Getränke nach. Er kann sicher sein, dass seine bezahlte Bestellung auch geliefert wird. Er etabliert sich als selbstständiger Teilnehmer am Wirtschaftsverkehr.

Szenario: Blockchain statt Notar

Die Kombination aus aufwendiger mathematischer Berechnung und verteilt gespeicherter Informationen macht die Blockchain unveränderbar und damit unbestechlich. Deswegen ist sie gut geeignet für Szenarien, in denen Informationen festgeschrieben werden – etwa bei der Dokumentation von Immobilienverkäufen.

Nüchtern betrachtet ist die Eigentumsübertragung von Immobilien in Deutschland und vielen anderen Ländern ein bürokratischer Albtraum: Unzählige Parteien sind an einem Verkauf beteiligt, die Dokumentation im Grundbuch ist rein papierbasiert und wirkt anachronistisch. Das Grundbuch führt die Eigentumsverhältnisse für alle Grundstücke, Eigentumswohnungen oder Häuser auf, die Einträge werden fortlaufend aktualisiert, also durch aktuelle Transaktionen ergänzt, und sind öffentlich einsehbar. Für diese Dokumentation hält jede Stadt und Gemeinde, jedes Bundesland, also letztlich der Staat, eine Behörde vor. Sie stellt sicher, dass die Eigentumsverhältnisse korrekt verbrieft sind und dass die Dokumente sorgfältig gelagert werden. Kurz: Das Grundbuchamt dokumentiert fortlaufende Transkationen fälschungs- und verlustsicher und ist für alle einsehbar. Korrektheit der Daten, fortschreibende Transaktionen/Dokumentation und Datensicherung – die Blockchain bietet diese Funktionen ebenfalls. Und das mit deutlich weniger Bürokratie, ergo Steuergeldern. Der Verkäufer identifiziert sich über eine elektronische Signatur auf der Webseite des Grundbuchamtes und sieht die auf ihn eingetragenen Immobilien. Der Verkäufer wählt die Option, ein Objekt zu verkaufen, und trägt Transaktionsdaten ein – etwa den Verkaufspreis, auf den sich beide Parteien vorab geeinigt haben. Im nächsten Schritt generiert das Blockchain-System

- einen Smart Contract und
- eine Empfängeradresse für die Verkaufssumme.

Diese Infos sendet der Verkäufer per SMS, Whatsapp oder E-Mail an den Käufer. Dieser identifiziert sich ebenfalls. Er kontrolliert, dass es sich um das gewünschte Objekt handelt und dass der Kaufpreis stimmt – und sendet die Verkaufssumme in Bitcoins an die Empfängeradresse. Im Hintergrund wacht der „Smart Contract“ über die Transaktion.

Diese Verträge sind schlichte Wenn-dann-Verknüpfungen. Sie übernehmen die Rolle des unparteiischen Dritten und lösen das Vertrauensproblem zwischen Käufer und Verkäufer: Beide Parteien kennen sich in der Regel nicht. Bei großen Summen ist es nur verständlich, wenn der Verkäufer das Eigentum nur übertragen möchte, wenn er den Kaufpreis erhalten hat. Andererseits möchte der Käufer nur zahlen, wenn der Verkäufer das Objekt auch tatsächlich überträgt.

Heute wenden sich beide vertrauensvoll an einen Notar, der die Transaktion als Treuhänder für sie abwickelt. Die Smart Contracts der Blockchain-Technologie lösen das Vertrauensproblem über schlichte, wenn auch manipulationssichere Wenn-dann-Verknüpfungen: Der Smart Contract überträgt das Eigentum im Grundbuch automatisch, wenn die Bitcoin-Zahlung des Käufers eingegangen ist. Der Verkäufer kann die Überschreibung nicht mehr zurückziehen. Zahlt der Käufer nicht, erleidet der Verkäufer keinen Verlust. Die Anforderungen beider Parteien sind erfüllt.

Zukunftsmusik gefällig? Autonom fahrende Taxis

Die meisten Autos stehen im Durchschnitt knapp 22 Stunden pro Tag nutzlos auf Parkplätzen, verschwenden wertvollen Raum und verlieren an Wert. Bereits heute reduzieren Carsharing-Anbieter die Anzahl von Fahrzeugen in den Innenstädten durch Mehrfachnutzung von Fahrzeugen. Mobilitätsdienstleister wie Lyft oder Uber adressieren mit einer optimierten Auslastung der Fahrzeuge dieses Problem in Ballungsräumen.

Die Blockchain-Technologie würde eine sich selbst verwaltende Lösung erlauben: Mit der Entscheidung der Bundesregierung zur Förderung des autonomen Fahrens sind seit diesem Jahr autonome Taxis denkbar: Sie holen Fahraufträge aus einem Netzwerk. Den Fahrpreis legen die Taxen anhand von Bedingungen fest, die in der Blockchain festgelegt sind. Zum Beispiel setzen sich die Kosten aus Ausgaben für Leasing, Energiekosten und Verschleiß zusammen. Pro Kilometer kommt so ein Preis im Cent-Bereich zustande, während Uber heute 2,15 US-Dollar pro Meile berechnet. Der Grund: Das Taxi braucht keinen Fahrer mehr. In diesem Szenario besitzt auch niemand das Fahrzeug; es ist ein eigener Wirtschaftsteilnehmer, Inspektionsintervalle oder Sicherheitsprüfungen sind fest programmiert. Es muss also keinen Gewinn abwerfen, sondern braucht sich nur selbst zu unterhalten.

Dank der Blockchain-Technologie vertraut EON dem Fahrzeug und lädt es mit Strom auf, ATU montiert neue Reifen. Schließlich garantiert die Blockchain die Bezahlung der Dienstleister, aber auch den Geldempfang für die geleisteten Transportkilometer.

Zukunftsmusik? Oder sogar verrückt? Genau das haben General Motors und Lyft auf der Consumer Electronics Show (CES) im letzten Januar angekündigt. Der Autobauer investiert 500 Millionen US-Dollar in das Fahrdienstnetzwerk Lyft, um autonome Taxis zu entwickeln. Volkswagen investiert in das Wachstum des Uber-Rivalen Gett [HaBl] – zukunftsweisende Mobilität bezeichnen die Wolfsburger als eine von drei wichtigen Säulen für die weitere Entwicklung des Konzerns. ||

Der Autor

|| Dirk Röder
(dirk.roeder@maibornwolff.de)
von MaibornWolff berät Unternehmen bei Veränderungen durch die digitale Transformation. Mit spielerischen Mitteln wie dem Digital Venture Game oder Blockchain Game entwirft er neue Geschäftsmodelle, digitalisiert Produkte oder passt bestehende an neue Gegebenheiten an.