Reine Vertrauens-frage

Blockchain-Technik jenseits von Kryptogeld

Grundlagen ..... **Seite 74**
Industriepraxis ..... **Seite 78**
Eigenbau ..... **Seite 82**

Bild: Albert Hulm

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Glaubt man den Ankündigungen von Startups und großen Unternehmen, steht die gesamte Wirtschaft vor einem großen Umbruch: Blockchains sollen Handel, Logistik und Industrie revolutionieren – ganz ohne gegenseitiges Vertrauen der Akteure. Doch rund um Blockchain ranken sich viele Mythen, die verschleiern, welche Probleme die Technik wirklich lösen kann.

Von Jan Mahn

Seit September 2019 hat auch die deutsche Bundesregierung eine Blockchain-Strategie. Auf 24 Seiten erklären die Autoren, welche Möglichkeiten der Nutzung sie für die deutsche Wirtschaft sehen und welche gesetzlichen Rahmenbedingungen angepasst werden müssten (siehe ct.de/y7ds). Versprochen wird in der Einleitung, „einen ganzheitlichen Blick der Bundesregierung auf die Blockchain-Technologie“ abzuliefern.

Der Untertitel der Veröffentlichung zeigt, in welche Richtung das Papier geht: „Wir stellen die Weichen für die Token-Ökonomie“. In der Einleitung wird diese Token-Ökonomie genauer erklärt: „Mit Token könnten alle erdenklichen Werte, Rechte und Schuldverhältnisse an materiellen und immateriellen Gütern repräsentiert und deren Verkehrsfähigkeit vereinfacht werden.“ Es geht der Regierung also vor allem um Anwendungsfälle, in denen bisher Banken unterwegs waren.

Blockchain und Kryptowährung

Die Ausrichtung des Strategiepapiers auf Geldverkehr und Handel passt zur allgemeinen Wahrnehmung, Blockchain, Kryptowährung und Bitcoin seien irgendwie dasselbe. Das hat historische Gründe: Im Jahr 2008 veröffentlichte eine bis heute unbekannte Person oder Personengruppe unter dem Pseudonym Satoshi Nakamoto das Whitepaper für die Kryptowährung Bitcoin – dabei taucht der Begriff „Blockchain“ selbst überhaupt nicht auf, doch der Zusammenhang der Begriffe ist irgendwie hängengeblieben. Wie Bitcoin funktioniert, haben wir bereits ausführlich erklärt. Einen guten Überblick liefert ein kostenloser Online-Artikel, den Sie über ct.de/y7ds finden.

Auf den folgenden Seiten soll es um Anwendungsfälle gehen, in denen die Blockchain kein Ersatz für bestehende Währungen darstellt, sondern zur Problemlösung in Logistik und Industrie eingesetzt wird. Das Grundprinzip einer Blockchain hat nämlich mit Geld erst einmal nichts zu tun. Es handelt sich dabei zunächst nur um eine Datenreihe, an die nacheinander Blöcke mit Daten angehängt werden. Diese Daten können Messwerte sein, Frachtpapiere darstellen oder den Weg von Rohstoffen bis zum fertigen Produkt dokumentieren. Ab Seite 78 erfahren Sie, wie IBM und thyssenkrupp mithilfe einer Blockchain Fertigungsdaten für 3D-Druck so abspeichern, dass das geistige Eigentum geschützt bleibt.

Blockchain und Vertrauen

Das Einsatzgebiet einer Blockchain beginnt immer dort, wo es an Vertrauen zwischen den Akteuren fehlt. Basis der Blockchain ist eine Datenbank, die alle beteiligten Akteure auf ihren Servern lagern. Am Ende der Datenreihe können Blöcke von Daten angehängt werden. Damit nachträgliche Veränderungen der Blöcke erkannt werden, kommt etwas Kryptografie zum Einsatz: Beim Anlegen eines neuen Blocks wird der Inhalt zusammen mit dem Hashwert des Vorgängerblocks in eine Hashfunktion übergeben und der generierte Hash mit abgespeichert. Dadurch basieren alle Hashwerte auf den Hashwerten aller vorangegangenen Blöcke. Wer die Korrektheit der Kette überprüfen will, braucht nur den kompletten Datensatz und kann nacheinander alle Hashwerte nachrechnen. Wurde auch nur ein Bit manipuliert, stimmen alle folgenden Hashwerte nicht mehr.

»Das Einsatzgebiet einer Blockchain beginnt immer dort, wo es an Vertrauen zwischen den Akteuren fehlt«

Damit ein solches System ohne Vertrauen der Akteure auskommt, braucht es einen Algorithmus, der entscheidet, wer den nächsten Block anhängen und damit eine neue Wahrheit schaffen darf. Bei Bitcoin heißt das Verfahren „Proof of Work“. Wer einen Block erzeugen will, muss eine Rechenoperation ausführen und ein passendes Ergebnis liefern. Wer diese Aufgabe, die regelmäßig schwieriger gemacht wird, zuerst löst, darf den neuen Block schreiben und wird in Bitcoin entlohnt.

Blockchain und Energie

Das Suchen nach einer mathematischen Lösung für das Proof-of-Work-Verfahren erfordert große Mengen Rechenleistung und damit Energie – einer der großen Kritikpunkte an der digitalen Währung.

Blockchains, die in Unternehmen eingesetzt werden, funktionieren grundsätzlich anders: Sie sind meist nicht öffentlich, haben also einen begrenzten Teilnehmerkreis und werden „Private Blockchain“ oder „Federated Blockchain“ genannt (mehr zu den begrifflichen Feinheiten auf Seite 78). Statt auf energieintensives Proof of Work setzen sie auf „Proof of Stake“ – im einfachsten Fall kann das eine einfache Mehrheitswahl aller beteiligten Server sein. Blockchains sind also nicht grundsätzlich Energievernichter.

Deutlich wird das Funktionsprinzip solcher Federated Blockchains an einem Beispiel: Ein Logistikunternehmen, das Kühltransporte anbietet, macht Geschäfte mit einem Lebensmittelhersteller und liefert die Ware an einen Supermarkt. Der Hersteller möchte sicherstellen, dass die Ware während der ganzen Fahrt nicht wärmer als 4 Grad wird. Auch der Supermarkt hat ein Interesse daran, dass die Ware gut gekühlt in seinem Lager ankommt.

Bisher basierte der ganze Transport auf Vertrauen der Akteure: Beim Einladen der Lebensmittel unterzeichnete der Hersteller ein Dokument und übergab es an den Fahrer des Lkw. Dieser begann seine Fahrt, bestimmte regelmäßig die Temperatur und trug sie auf dem Frachtdokument ein. Beim Supermarkt angekommen, quittierte

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Hinter der Weboberfläche soll eine Blockchain arbeiten. Das muss der Kunde dem Supermarkt Carrefour glauben, einen Beweis gibt es nicht.

jemand Empfang und Einhaltung der Kühlkette. Der Fahrer hätte in diesem Fall leicht betrügen, falsche Messwerte eintragen und die energieintensive Kühlung zwischendurch abschalten können.

Die drei Unternehmen planen jetzt, eine Blockchain zu nutzen, um Manipulationen zu verhindern. Sie einigen sich auf die Regeln: Gespeichert werden soll jeder Transport mit zusätzlichen Informationen. Außerdem soll ein Sensor minütlich die Temperatur im Frachtraum erfassen. Die drei Beteiligten richten die Blockchain-Infrastruktur in ihren Rechenzentren ein und stellen mit konventioneller Netzwerktechnik sicher, dass nur sie Zugriff auf die Umgebung haben. Dass Blockchains per se sicher sind, weil darin irgendwas mit Kryptografie passiert, gehört nämlich ins Reich der Mythen. Eine solche Federated Blockchain muss gegen Zugriffe von außen gesichert sein wie jede andere Datenbankanwendung. Jeder Akteur bekommt einen Schlüssel, mit dem er sich anmeldet.

Jetzt bekommen alle Lkws Temperatursensoren, ein GPS-Modul und ein Modem, mit dem sie per Funk Messwerte und Standorte verschicken können.

Jedes Ereignis, etwa ein neuer Messwert, kann die Ausführung eines Programms auslösen – je nach System nennt man diese Programme Chaincode oder Smart Contract. Ein solcher Programmschnipsel könnte zum Beispiel dafür sorgen, dass der Messwert gespeichert und bei Überschreiten einer Grenze dem Spediteur eine Strafe abgezogen wird.

Wie Sie selbst Chaincode für ein einfaches Beispiel aus dem Alltag umsetzen können, erfahren Sie ab Seite 82.

Blockchain und Vertrauen

Das Beispiel zeigt aber auch, welche Probleme durch die Technik ungelöst sind: In jeder Anwendung, bei der es um Dinge in der realen Welt geht (nahezu alle Blockchain-Szenarien, die keine Kryptowährungen sind), braucht man eine Schnittstelle nach draußen – in der Forschung werden diese Berührungspunkte als Oracle bezeichnet. Das kann ein Hardware-Sensor oder eine Software sein (zum Beispiel ein API, das externe Daten wie das Wetter abholt). Alle Probleme, die an der Schnittstelle von Blockchain und Realität auftreten, bezeichnet man daher als Oracle-Problem. Und davon gibt es einige:

Der Fahrer im Lieferkettenbeispiel könnte den Sensor abschrauben, in eine kleine Kühlbox im Fahrerraum legen und die Kühlung im Lkw zum Energiesparen abschalten. Findet man dafür keine technische Lösung, können sich die drei Akteure den ganzen Aufwand mit der Blockchain sparen. Sie hätten das Vertrauensproblem nur mit viel Aufwand verlagert.

Fassaden

Das Problem geht aber weit darüber hinaus: Angenommen, der Supermarkt wollte die Blockchain nutzen, um seinen Kunden zu beweisen, woher die Ware stammt. Er könnte QR-Codes auf alle Verpackungen kleben lassen, die für jedes Produkt eine individuelle Nummer enthalten. Die Nummern würden schon beim Hersteller einem Transport zugewiesen.

Der Kunde könnte jetzt den Code einscannen und eine Webseite würde ihm die Historie des Produkts liefern. Doch ohne Vertrauen funktioniert auch das nicht: Der Kunde sieht schließlich nicht wirklich den Inhalt der Blockchain und kann auch keine Kopie herunterladen, da der Zugriff ja aus gutem Grund auf die drei Akteure beschränkt ist. Er sieht nur einen von einem Webserver aufbereiteten Datensatz. Der Server gehört dem Supermarkt und kann auf die Blockchain zugreifen. Der Kunde muss dem Supermarkt also glauben, dass der Datensatz wirklich aus der Blockchain stammt. Die Messwerte könnten genauso gut aus einem Zufallsgenerator kommen. Außerdem muss er darauf vertrauen, dass der Barcode auch wirklich zu der transportierten Ware gehört. Einen Barcode zu kopieren ist schließlich einfacher als eine Manipulation der kryptografisch gesicherten Blockchain. Das Gesamtsystem ist jedoch nur so sicher wie das schwächste Glied.

Nicht-Lösungen

Man könnte annehmen, dass Unternehmen, die eine Blockchain-Lösung einsetzen wollen, diese Probleme vorher abwägen und entweder Lösungen finden oder stattdessen auf konventionelle Technik setzen, die sich mit wenig Aufwand einrichten lässt. In der Realität scheint die Faszination, die von Blockchain ausgeht, aber oft größer als die Vernunft: So hat der französische Supermarkt Carrefour ein Lebensmitteltracking für einige hochpreisige Produkte eingeführt. Der Kunde kann einen QR-Code scannen und sieht auf einer ansprechenden Webseite den Lebenslauf eines Huhns. Die Daten sollen, so behauptet es die Pressemitteilung, manipulationssicher in einer Blockchain liegen. Auf einer Konferenz nutzten wir die Gelegenheit und fragten nach, wo diese Blockchain denn gespeichert ist. Die Antwort: im Rechenzentrum von Carrefour. Nicht etwa verteilt auf Infrastruktur von Supermarkt, Lieferanten, Schlachthof und Zuchtbetrieb. Dem Kunden bleibt also nichts anderes, als der schönen Fassade zu vertrauen.

Eine SQL-Datenbank hätte das Problem also mit weit weniger Aufwand gelöst, hätte aber sicher keine Pressemitteilung hergegeben. Die Überschrift „Carrefour setzt jetzt auf eine SQL-Datenbank mit API“ klingt einfach nicht attraktiv. Das scheint das Grundproblem zu sein: Nur in wenigen Fällen (exemplarisch sei das Beispiel auf Seite 78 genannt) entsteht wirklich ein Mehrwert, wenn Unternehmen sich zusammentun und ein gemeinsames Problem mit einer Blockchain lösen – nämlich immer dann, wenn fehlendes Vertrauen dazu führt, dass man einen unabhängigen Dritten (Notar, Bank, Prüfinstitut) dafür bezahlen müsste, Vertrauen herzustellen. In der Praxis sind Erfolgsgeschichten bisher rar. Nicht-Lösungen wie die von Carrefour, bei denen es mehr um Aufmerksamkeit als um technische Notwendigkeit geht, dagegen omnipräsent.

(jam@ct.de) c't

Whitepaper und weiterführende Artikel:
ct.de/y7ds

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover