Aktueller Kommentar

Die Blockchain-Revolution verstehen!

7. Juni 2018

Autor
Jochen Möbert
+49(69)910-31727
jochen.moebert@db.com

www.dbresearch.de

Deutsche Bank Research Management
Stefan Schneider

Trägt man in diesen Tagen über Bitcoin, Blockchain und Kryptowährungen vor, steht man vor der Frage: Diskutiert man die Technologie oder präsentiert man direkt die gesellschaftlichen und ökonomischen Implikationen? Seinen Zuhörern in wenigen Minuten einen Zugang zu einer komplexen Technologie zu vermitteln, ist riskant. Schnell verliert man sich in Alices Kaninchenbau aus den Augen. Doch die Zuhörer können ebenso ratlos zurückbleiben, wenn man direkt die potenziell revolutionären Implikationen anspricht. Aufgrund dieses Dilemmas und der Komplexität von Kryptosystemen wollen wir Ihnen hier die Technologie anhand von Metaphern näherbringen. Wir hoffen, dass Sie uns so auf die Reise ins Blockchain-Universum folgen.

Blockchains sind wie Dominosteine! Nicht das Weihnachtsgebäck ist gemeint, sondern die Spielsteine. Bei den Spielsteinen sind zwei unterschiedliche Varianten beliebt. In der ersten stellt man die Steine eng hintereinander auf, sodass man durch das Umwerfen eines Steins eine Kettenreaktion auslöst. Der Weltrekord liegt bei mehreren Millionen Steinen. In der zweiten Variante sind auf den Spielsteinen mehrere Zahlen oder Bilder abgedruckt, die gemäß den Spielregeln aneinandergelegt werden.

In gewisser Weise kombiniert eine Blockchain beide Varianten. Die Dominosteine werden eng nebeneinander aufgestellt, aber auf jedem Stein steht nun weder eine Zahl noch ein Bild, sondern „dieser Stein gehört in eine bestimmte Wallet“. Sie merken schon, worauf ich hinaus will. Die Dominokette repräsentiert die Blockchain, jeder Stein entspricht einem „Coin“ und die „Wallets“ sind die virtuellen Geldbeutel der Kryptowährung. Öffnet jemand seine Wallet, werden alle Coins angezeigt, die aktuell der Wallet in der Dominokette zugeordnet sind. Wechselt ein Coin den Eigentümer, stellen die sogenannten „Miner“ einen neuen Dominostein mit der neuen Information auf. Der alte Dominostein ist nun keiner Wallet mehr zugeordnet, hat in diesem Sinne also keinen Wert mehr. Er bleibt aber Teil der Dominokette, sodass die gesamte Historie der Blockchain erhalten bleibt. Da die Information im Internet frei verfügbar ist, kann sie jeder Miner, aber auch jeder normale Internetnutzer, stets abrufen.

Die Blockchain-Revolution verstehen!

Auf geht es zum nächsten Gesellschaftsspiel: Sudoku! Die Miner spielen parallel zum Dominospiel auch Sudoku. Für das Aufstellen der Dominosteine werden sie mit neuen Coins belohnt, deshalb konkurrieren sie untereinander. Die Belohnung bekommt derjenige, der als Erster eine Art superkomplexes Sudoku löst. Wie beim Feierabend-Sudoku sind einige Felder schon ausgefüllt und definieren damit die gesuchte Lösung. In der Blockchain-Welt ist diese Vorabinformation der Eigentümerwechsel der Coins. Da auch der Zeitpunkt des Eigentümerwechsels erfasst wird, steht auf jedem Dominostein eine andere Vorabinformation. Hat der Miner eine Lösung gefunden, schreibt er sie ebenfalls auf den Dominostein. Dabei ist es, wie beim Feierabend-Sudoku, für die Miner sehr schwer, die Lösung zu finden, aber sehr einfach, eine richtige Lösung als solche zu erkennen.

Warum schummelt, manipuliert und zerstört niemand die Dominokette?

Warum schummeln die Miner nicht? Erstens kontrollieren sie sich gegenseitig. Zweitens tätigen sie teure Investitionen in Hardware und Strom, um die superkomplexen Sudokus zu lösen. Diese Investitionen gingen zusammen mit dem Vertrauen in die Kryptowährung verloren. Daher verhalten sie sich regelkonform. Drittens ist es viel attraktiver, die neuen Coins für das Lösen der superkomplexen Sudokus einzustreichen. Würden sie trotzdem schummeln, könnten sie womöglich mehr Coins bekommen. Doch mit dem Auffliegen wären diese und die gesamte Investition in die Hardware wertlos.

Warum manipuliert niemand die Dominokette? Zieht jemand einen Stein aus der Kette, um darauf zu schreiben „Dieser Coin gehört mir“, dann wirft er die komplette Dominokette um. Zumindest ist dies in der Blockchain-Welt garantiert, denn alle Coins sind miteinander verkettet - daher der Name Blockchain. Eine nachträgliche Veränderung der Zuordnung der Coins falsifiziert somit die gesamte Blockchain. Deswegen werden die Kryptosysteme als „immutable“, also unveränderbar, bezeichnet.

Warum zerstört niemand die Dominokette? Die Selbstheilungskräfte sind stärker. Blockchains werden ständig attackiert. Aber Schäden werden schnell behoben, denn es gibt viele tausende Kopien von jeder Dominokette bzw. von jeder Blockchain. Diese Kopien liegen global verteilt auf den Rechnern der Miner und anderen Computern, zum Beispiel der Wallet-Anbieter. Diese Computer tauschen sich ständig über den aktuellen Zustand der Dominokette aus und bilden somit ein Netzwerk. Wird an einem Computer die Dominokette manipuliert, kopiert man die Originale von einem der anderen Netzwerkknoten. Das System funktioniert also wie das Heilen einer kleinen Wunde. Die umliegende Haut repariert das verletzte Gewebe zügig. Diese Netzwerkstruktur ist ein Grund, warum Kryptosysteme als dezentral bezeichnet werden.

Ein weiteres dezentrales Element ist die Governance-Struktur. Die Software und der Code vieler Blockchains sind Open Source. Jeder darf mitarbeiten und es arbeiten viele mit. Viele Köche verderben aber auch schnell den Brei. Zumal die Programmierer bei Softwareupdates nicht nur untereinander um einen Konsens ringen, sondern auch die Miner und Netzwerkknoten überzeugen müssen. Andernfalls ignorieren diese die Softwareupdates. Folglich ist die Governance-Struktur komplex und das System träge, aber auch sehr stabil und nahezu ohne Hierarchie.

Die Blockchain-Revolution verstehen!

Kryptografie sichert den Inhalt der Dominokette und den Eigentümerwechsel ab. Kryptografie wird erstens eingesetzt, um den Eigentümerwechsel mit einer digitalen Unterschrift zu bestätigen. Zweitens wird so die gesamte Historie aller Eigentümerwechsel verschlüsselt. Daher sind zwar alle Eigentümerwechsel im Internet abrufbar, aber die Eigentümer bleiben in der Regel anonym.

Das Kryptonetzwerk funktioniert ohne Dritte. Die Kryptowährungen sind, wie wir beschrieben haben, unveränderbar, dezentral und global. Somit sind sie grenzüberschreitend und sprengen den gewohnten nationalen juristischen Rahmen. Entsprechend schwer sind sie zu regulieren. Es bedarf zudem keinerlei Treuhänder oder „trusted third parties“, wie Zentralbanken oder Central Clearing-Stellen. Personen, die sich einen Coin schicken, müssen sich auch weder kennen noch einander vertrauen. Deswegen werden Kryptosysteme auch als „trustless“ bezeichnet!

Nun, mit einem solchen System kann man also in gewisser Weise Informationen, zum Beispiel einen Eigentümerwechsel eines virtuellen Coins, unwiderruflich speichern. Da zum Beispiel die Bitcoin-Blockchain neben den Eigentümerwechseln der Coins auch noch ein kleines Textfeld enthält, haben manche Kryptoevangelisten ihr Eheversprechen auf der Blockchain hinterlegt. Sie hoffen auf die Ewigkeit. Welche Informationen kann man noch auf einer Blockchain speichern? Die Antwort auf diese Fragen elektrifiziert die Kryptoenthusiasten und weil es viele potenzielle Anwendungsfälle gibt, sagen manche eine Blockchain-Revolution voraus.

Die Blockchain-Revolution verstehen!