Die Blockchain-Technologie, die hinter Kryptowährungen wie Bitcoin steht, ist hip. Unternehmen und Berater der Finanzbranche und darüber hinaus versprechen ungeahnte Möglichkeiten dieser Innovation.Doch es gibt zwei Probleme: Oft ist gar nicht Blockchain drin, wo Blockchain draufsteht. Außerdem sind dezentrale, öffentliche Datenbanken wie die von Bitcoin systembedingt anfällig für groß angelegten Betrug.

Als Kodak im Januar ankündigte, eine Blockchain-basierte Plattform für Bildrechte mit eigener Kryptowährung anzubieten, verdreifachte sich der Aktienkurs des Unternehmens kurzzeitig. Auch im Handel mit Wertpapieren, Diamanten und Kunstwerken wird der Blockchain großes Potenzial zugeschrieben. Dabei hat vieles von dem, was als Blockchain gehypt wird, herzlich wenig mit der Bitcoin-Blockchain zu tun.

Grundidee der Bitcoin-Blockchain ist es, Vertrauen zwischen Vertragsparteien, die sich kennen, zu ersetzen durch eine Validierungsmethode, die auch zwischen völlig anonymen Partnern einer Transaktion funktioniert. Am Beispiel von Bitcoin geht das so. Etwa alle zehn Minuten werden von Nutzern beabsichtigte Transaktionen zu öffentlich einsehbaren Blöcken zusammengefasst, vergleichbar einer Seite in einem Kontobuch. Computer, die an das Bitcoin-Netzwerk angeschlossen sind, verifizieren die Echtheit, indem sie eine schwierige Rechenaufgabe lösen, die aus Informationen zu den im Block enthaltenen Transaktionen und zum vorangegangenen Block abgeleitet ist. So werden - im übertragenen Sinne - die einzelnen Seiten des Kontobuches fortlaufend mit einem Siegelfaden verbunden.

Wer Computerkapazität für die Verifizierung zur Verfügung stellt, und zuerst die Rechenaufgabe löst, wird mit einer Gebühr von den Auftraggebern der Transaktionen und durch neu geschaffene Bitcoin belohnt. Von dieser Belohnung mit neuen Bitcoin leitet sich der Name "Mining" ab, der auf die Analogie zum Schürfen von Gold verweist.

Viele falsche Etiketten

Die Daten liegen auf vielen Computern und werden überall mit neuen Daten ergänzt. Das ist eine sogenannte Distributed-Ledger-Technologie, übersetzt etwa "Methode dezentraler Kontobücher". Dass Bitcoin so hip ist, verleitet dazu, alles was mit dezentralen Transaktionsdatenbanken arbeitet, als "Blockchain" anzukündigen. Dabei ist nicht jede verteilte Datenbank eine öffentliche Blockchain vom Bitcoin-Typ. Viele sind einfach fortschrittliche, zentral kontrollierte aber verteilte Datenbanken, die vielfältige Zugriffe erlauben und dabei sicherstellen, dass alle Teile der Datenbank konsistent aktualisiert werden.

Daran ist nichts, was große Aktienkurssprünge von Unternehmen wie Kodak rechtfertigen würde. Gleichzeitig bedeutet das falsche Etikett aber auch, dass die nur vorgeblichen Blockchain-Anwendungen von einem schwerwiegenden Problem verschont bleiben dürften, das Kryptowährungen bedroht: der Gefahr von Mehrheitsattacken.

Erfolgreicher Mehrheitsangriff

Was bisher nur als theoretische Gefahr diskutiert wurde, hat sich im Mai tatsächlich ereignet. Es traf die Bitcoin-Abspaltung "Bitcoin Gold". Mit einer "51-Prozent-Attacke" erbeuteten Angreifer Bitcoin Gold im Wert von 18 Millionen Dollar. Bei einer solchen Attacke bringt der Angreifer

mehr als die Hälfte der Rechenleistung im relevanten Netzwerk unter seine Kontrolle. Dann kauft er mit seinen Krypto-Coins Waren oder andere Währungen. Im Nachhinein manipuliert er dann mit seiner Rechenleistungsmehrheit die Blockchain derart, dass seine Transaktionen daraus verschwinden. Die eigentlich ausgegebenen Krypto-Coins sind dadurch wieder in seinem Besitz, ebenso wie der bereits ausgehändigte Gegenwert. Die Verkäufer werden um ihr Geld betrogen.

Man stelle sich vor, Grundbucheinträge oder Börsentransaktionen würden tatsächlich, wie oft verheißen, auf eine derartige Blockchain-Technologie umgestellt. Das Potenzial für Betrug und Sabotage wäre enorm.

Eric Budish von der Booth School of Business der Universität Chicago hat nun ein Modell vorgestellt, das klärt, unter welchen Bedingungen Mehrheitsattacken auf eine Bitcoin-Blockchain Gewinn versprechen. Es gilt die Annahme, dass so lange neue Rechenleistung in das Mining-Netzwerk kommt, bis sich damit kein Geld mehr verdienen lässt. Damit ist die Gesamtrechenleistung im Gleichgewicht ermittelbar, in Abhängigkeit von der Belohnung, die wiederum stark vom Bitcoin-Kurs abhängt. Was es kostet, sich genug Rechenleistung für eine Mehrheit zu verschaffen, lässt sich anhand der Preise für einschlägige Chips herausfinden.

Ein weiterer wichtiger Parameter ist die Frage, wie der Bitcoin-Kurs auf einen erfolgreichen Angriff reagieren würde. Denn den Gewinn kann der Angreifer standardmäßig nur in Form von Bitcoin realisieren. Werden diese durch den Vertrauensverlust infolge der Attacke wertlos, gibt es keinen Gewinn. Das ist der Grund, warum solche Attacken in Foren und Publikationen bisher für unwahrscheinlich gehalten wurden.

Im Fall von Bitcoin Gold reagierte der Kurs nicht allzu heftig auf die Attacke. Allerdings würde ein starker Kursverfall eine andere Gewinnmöglichkeit eröffnen. Auf Kursrückgänge von Bitcoin kann man auf Futures-Börsen spekulieren, oder man kann sich in Bitcoin verschulden. Fällt der Kurs, kann man seine Verpflichtung sehr billig erfüllen.

Über eine Milliarde Dollar Angriffskosten

Die Mehrheit der Rechenleistung zu kontrollieren ist bei Bitcoin viel teurer als bei Bitcoin Gold. Budish kommt für Bitcoin derzeit auf 1,5 bis 2,2 Milliarden Dollar, mit Mengenrabatt weniger. Allerdings ist auch der potenzielle Ertrag höher, denn man kann mit Bitcoin mehr und Teureres einkaufen als mit kleinen Konkurrenten. Das Problem, so Budish, liegt darin, dass die Kosten einer Attacke mit dem Transaktionsvolumen einer Blockchain nur linear wachsen. Der Ertrag eines erfolgreichen Angriffs kann dagegen auch überproportional steigen, etwa wenn der Bitcoin-Kurs oder die Größe der einzelnen Transaktionen, die man damit abwickeln kann, stark aufwerten.

Das hat fatale Konsequenzen: "Das Modell legt nahe, dass Bitcoin einer Mehrheitsattacke zum Opfer fallen würde, wenn es ökonomisch hinreichend wichtig würde", resümiert Budish das Ergebnis: "Das bedeutet, dass es intrinsische Grenzen dafür gibt, wie wichtig Bitcoin werden kann." Den weltweiten Zahlungsverkehr in relevantem Maßstab darüber abzuwickeln, scheidet schon wegen des enormen Energiebedarfs aus.

Budishs Modell ergibt außerdem, dass die Transaktionsprämie, die die Bitcoin-Handelspartner den Minern zahlen müssen, sehr hoch bleiben und sogar noch steigen muss, damit sich Attacken nicht lohnen. Aber auch, dass Bitcoin ein ähnlich wichtiges Wertaufbewahrungsmittel wie Gold werden könnte, hält Budish für sehr unwahrscheinlich, weil dies Attacken lohnend machen würde.

Ehtereum, die Blockchain der Kryptowährung Ether, die für allgemeine Anwendungen abseits der Kryptowährungen besonders beliebt ist, funktioniert wie Bitcoin und hat damit das gleiche Problem. Die Ethereum-Blockchain soll zwar seit Längerem so umgestellt werden, dass nicht mehr die größte Rechenleistung am ehesten zum Zuge kommt, sondern diejenigen mit den meisten Coins. Bisher ist diese Umstellung aber nicht geglückt. Sie könnte zwar das Problem der Energieverschwendung wesentlich entschärfen. Das Problem von möglichen Mehrheitsattacken würde aber nicht gelöst, so Budish.