

**Geschäfte en bloc:**  
In der Blockchain werden etwa Geldüberweisungen in Datenpaketen gespeichert. Eine Kopie der Kette liegt bei allen, die selbst Datenblöcke erzeugen.

# LÜCKEN IN DER BLOCKCHAIN

TEXT: THOMAS BRANDSTETTER

Blockchains bilden das Rückgrat von Kryptowährungen wie Bitcoin, in ihnen lassen sich aber Geschäfte aller Art abwickeln. Sie kommen dabei nicht nur ohne Institutionen wie Banken oder Notariate aus, sondern sollen auch per se sicher vor Diebstahl und Betrug sein. Doch Anwendungen, die auf Blockchains basieren, sind keineswegs unangreifbar. Clara Scheidewind und ihr Team am Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum identifiziert Sicherheitslücken, die es bei solchen Anwendungen gibt.

Es ist der Versuch, die Geschäftswelt neu zu ordnen: Die Blockchain übernimmt Funktionen, die normalerweise Banken oder Notare erfüllen, etwa die Bestätigung von Transaktionen oder die Dokumentation digitaler Besitzverhältnisse. Die prominentesten Beispiele sind Kryptowährungen wie Bitcoin oder Ethereum. Bei der Blockchain handelt es sich also um

eine Art digitale Beglaubigung – allerdings nicht durch einzelne Institutionen, sondern durch eine Vielzahl von Akteuren, die sich weder kennen noch gegenseitig vertrauen müssen. Die Technik basiert dabei auf verschlüsselten oder zumindest digital signierten Datenpaketen, die dezentral verwaltet und überwacht werden. Vertrauenswürdige zentrale Instanzen werden also nicht mehr benötigt. Zudem soll die Blockchain in Form von Smart Contracts bestimmte Arten von Geschäften sicherer machen.

Tatsächlich beruht die Blockchain auf Kryptografie vom Feinsten. Wie die Perlen einer Kette reihen sich die Datenblöcke aneinander, die neben ihrem eigentlichen Inhalt auch noch den kryptografischen Fingerabdruck aller

vorherigen Blöcke enthalten. Einmal in die Welt gesetzt, lässt sich die Kette daher nicht mehr verändern. Jede Manipulation an einem Block würde sofort auffallen – zum einen, weil die nachfolgenden Blöcke dann nicht mehr zum Original-Block passen würden, und zum anderen, weil identische Kopien der Blockchain auf vielen unabhängigen Servern liegen. Daran beteiligt sind nicht nur Privatpersonen, sondern auch institutionelle Akteure wie Unternehmen oder öffentliche Einrichtungen. Speichern die Blöcke eine Historie von Geldtransfers, hat man eine Kryptowährung.

So weit, so sicher. Nur ist die Blockchain als makelloser Rückgrat ihrer Anwendungen noch nicht das Ende der →

Geschichte. „Die Kryptografie ist zwar sicher, aber sie sorgt eigentlich nur dafür, dass niemand die Historie nachträglich ändern kann“, sagt Clara Schneidewind, die am Max-Planck-Institut für Sicherheit und Privatsphäre die Heinz Nixdorf Research Group for Cryptocurrencies and Smart Contracts leitet. Die Mechanismen für die Erzeugung der Ketten etwa sind keineswegs so sicher wie ihr Ergebnis. Gleiches gilt für die Schnittstellen zur Außenwelt, über die etwa Bitcoins in andere Währungen umgetauscht werden können. Und wenn die Blöcke neben einfachen Transaktionen auch komplexere Konstrukte wie digitale Verträge beinhalten, finden Hacker dort immer wieder Schwachstellen. Gemeinsam mit ihrem Team hat Clara Schneidewind es sich deshalb zum Ziel gesetzt, Lösungen für sicherheitsrelevante Herausforderungen von Blockchain-Anwendungen zu finden.

Eine Schwachstelle ergibt sich gerade aus der wesentlichen Eigenschaft einer Blockchain: ihrer dezentralen Organisation. Alle Beteiligten haben die gleichen Informationen über ihren Inhalt, denn die Blockchain liegt

gleichzeitig in identischen Kopien auf vielen verschiedenen Servern – sogenannten Knoten. Auch sonst sind die Teilnehmer gleichberechtigt. Im Gegensatz zu staatlichen Währungen existiert keine höhere Instanz, die Entscheidungen treffen oder Recht sprechen könnte. Dennoch muss irgendjemand aktuelle Transaktionen in einem neuen Block dokumentieren und diesen der Kette hinzufügen, um die Blockchain am Laufen zu halten.

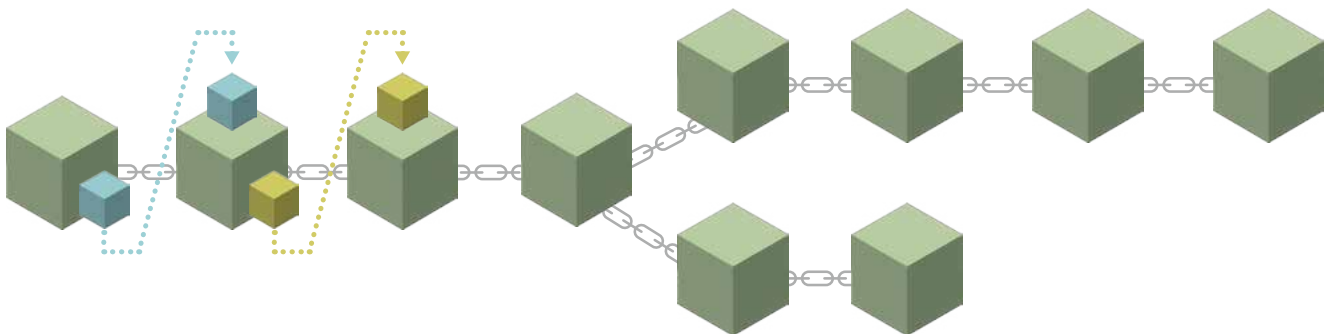
## Rechenkraft gewinnt

„Im Idealfall sollte das System zufällig jemanden auswählen, der den nächsten Block an Transaktionen erzeugen darf“, sagt Schneidewind. Das würde sicherstellen, dass die Erweiterung fair abläuft und niemand zensiert wird. In der Praxis ist diese zufällige Auswahl jedoch schwierig, da einzelne Teilnehmer sich etwa gleich mehrere Identitäten zulegen könnten, um sich einen Vorteil bei der Auslosung zu verschaffen. Das Interesse, selbst Blöcke zu erstellen, ist dabei so groß, weil die ausgewählten Teilnehmer dafür in der Regel mit neuem Kryptogeld belohnt werden. Wer den nächsten

Block erstellen darf, muss also auf andere Weise bestimmt werden. Der Proof-of-Work-Mechanismus etwa, der auch Bitcoin zugrunde liegt, wählt Teilnehmer nicht rein zufällig, sondern ihrer jeweils zur Verfügung stehenden Rechenkraft nach aus.

Die Rechenkraft wird für das sogenannte Mining benötigt: Die Blockchain erstellt automatisch ein schwieriges mathematisches Rätsel, und wer es zuerst löst, darf als Miner den nächsten Block mit den Transaktionen erstellen, die während seiner Berechnung getätigt wurden. Das Ergebnis dieser Rechenaufgabe ist gleichzeitig der kryptografische Fingerabdruck der bisherigen Kette. Die Berechnungen, die auch enorme Mengen an Energie verbrauchen, machen eine mögliche Manipulation extrem teuer. Genau das ist auch der eigentliche Kern der Sicherheit. „Das war damals eine sehr elegante Lösung für die Herausforderung von Bitcoin, zufällig Leute auszuwählen“, sagt Schneidewind.

Wenn nun aber ein Angreifer über mehr Rechenkraft verfügte als alle anderen Teilnehmer zusammen, würde ihn



Verschlüsselte Kette: Ein neues Glied der Blockchain enthält einen kryptografischen Fingerabdruck des vorhergehenden, angedeutet durch die blauen und gelben Quader. Bei der Erzeugung neuer Datenblöcke können Verzweigungen entstehen. Nach kurzer Zeit erlangt ein Strang aber einen Vorsprung und wird dann alleine fortgeschrieben.

das in die Lage versetzen, das System ins Trudeln zu bringen. Er könnte dann nämlich parallel zur öffentlichen Blockchain heimlich eine eigene, private Kette bauen. Diese würde inhaltlich zwar weitgehend mit der öffentlichen Blockchain übereinstimmen, der Angreifer könnte seine eigenen Transaktionen aber unterschlagen. Gleichzeitig könnte er nach Belieben weiter über die originale Blockchain einkaufen, wo diese Transaktionen zunächst auch bestätigt würden. Aufgrund seiner überlegenen Rechenleistung würde seine eigene Kette währenddessen allerdings schneller wachsen als die öffentliche. Für den Fall, dass die bei den unterschiedlichen Teilnehmern dezentral gespeicherten Versionen einer Blockchain nicht alle gleich lang und damit nicht auf demselben aktuellen Stand sind, schreibt das Konsensprotokoll vor, immer an der längsten existierenden Kette weiterzuarbeiten. Deshalb würde das Kollektiv die Version des Angreifers, sobald er sie veröffentlicht, automatisch als die gültige Kette betrachten und übernehmen – auch wenn der Betrüger seine eigenen Transaktionen dort weggelassen hätte. Seine zuvor bereits bestätigten Zahlungen wären in der neuen Blockchain also nie passiert, während er die dafür gekauften Waren behalten könnte. „Ob es tatsächlich Akteure gibt, die genug Macht auf sich konzentrieren können, um eine solche Attacke durchzuführen, ist allerdings unklar“, sagt Schneidewind.

## Verdunkelungsgefahr

Eine weitere Möglichkeit, Blockchain-Netzwerke anzugreifen, ist die sogenannte Eclipse-Attacke. Dabei isoliert ein Angreifer gezielt einen einzelnen Teilnehmer im Netzwerk von allen anderen. Der Angreifer umgibt das Opfer quasi mit eigenen, manipulierten Knoten und schneidet es so von der realen Blockchain ab – daher der Name „Eclipse“, also Verdunkelung. Das isolierte Opfer erhält dann nur noch Informationen, die der Angreifer kontrolliert, und bekommt eine verfälschte Sicht auf den Zustand der Blockchain. So kann der Angreifer beispielsweise eine Zahlung vortäu-

schen und das Opfer dazu bringen, ihm ohne tatsächliche Gegenleistung eine Ware zu überlassen. „Für solche Attacken benötigt man jedoch eine enorme Infrastruktur und muss Router oder spezifische Standorte angreifen“, sagt Schneidewind. „Das macht sie sehr komplex und oft schlichtweg zu teuer.“

Doch Kryptowährungen lassen sich – zumindest theoretisch – auch einfacher manipulieren. Neben dem exorbitanten Energieverbrauch hat der Proof-of-Work-Mechanismus nämlich auch noch einen anderen Nachteil: Es kann zu längeren Wartezeiten kommen, bis das aktuelle Rätsel gelöst ist und ein neuer Block generiert wird. Aktuelle Transaktionen können dann nicht sofort in der Blockchain niedergeschrieben werden, sondern hängen erst einmal eine Weile lang in der Luft. „Wenn man Kryptowährungen für sofortige Zahlungen nut-

zen möchte, müsste man theoretisch minutenlang an der Kasse warten, bis die Zahlung sicher ist“, sagt Schneidewind. „Sonst besteht das Risiko eines Betrugs.“ Indem ein bössartiger Nutzer eine frisch ausgesendete, aber noch unbestätigte Transaktion in seiner Wallet-App zeigt, könnte er einem Händler etwa vorgaukeln, dass er die Überweisung für eine Ware bereits getätigt hat, die gleiche Coin, also ein spezifisches digitales Geldstück, auf das sich Transaktionen von Kryptowährungen oft beziehen, kurz darauf aber noch einmal verwenden. Hat ein Betrüger dann auch noch einen guten Draht zu einem Miner, könnte es ihm gelingen, die zweite Transaktion zuerst in die Blockchain aufnehmen zu lassen. Er hätte damit de facto ein und dieselbe Münze zweimal verwendet. „Damit wäre der erste Zahlungsver-such ungültig“, sagt Schneidewind. „Wirklich sicher ist man sich also erst, wenn die Transaktion fest in der Blockchain steht.“

---

## AUF DEN PUNKT GEBRACHT

Blockchains bilden unter anderem das Rückgrat von Kryptowährungen und verteilen die Funktion von Institutionen wie Banken oder Notariaten auf viele Teilnehmer; sie sollen per se sicher sein. Bei ihrer Erzeugung und den Anwendungen, die auf ihnen laufen, kann es aber Sicherheitslücken geben.

Unter anderem könnten Angreifer mit großer Rechenkraft Knoten des Teilnehmernetzes kapern und einzelnen Teilnehmern Zahlungen vorgaukeln. Die größten Sicherheitslücken ergeben sich bei fehlerhaft programmierten Anwendungen wie etwa Smart Contracts, durch die Cyberkriminelle bereits mehrere Millionen US-Dollar erbeutet haben.

Ein Max-Planck-Team identifiziert Sicherheitslücken in der Blockchain und entwickelt Protokolle, die Geschäfte sicherer machen sollen, etwa für Transaktionen zwischen verschiedenen Blockchains.

---

Warten Zahlungsempfänger die Dokumentation in der Blockchain immer ab, ehe sie die Gegenleistung erbringen, kann eine solche Attacke kaum stattfinden. Das zeigt etwa die Geschichte der mit Abstand prominentesten Kryptowährung: Bitcoin. Von anonymen Entwicklern in die Welt gesetzt, war sie auch die erste funktionierende Umsetzung des Proof-of-Work-Mechanismus. „Das ist inzwischen über 17 Jahre her, und obwohl sie ein durchaus lukratives Ziel darstellt, wurde diese Blockchain noch nie gehackt“, sagt Nils Urbach, Professor für Wirtschaftsinformatik an der Frankfurt University of Applied Sciences und einer der Leiter des Fraunhofer Blockchain-Labors.

Die Gründe dafür sind allerdings nicht rein technischer, sondern auch ökonomischer Natur. Denn selbst wenn ein einzelner Akteur die nötige Rechenleistung für eine Attacke aufbringen könnte, würde ein Angriff auch seinen eigenen Interessen schaden. So würde der Marktwert der betroffenen Währung wohl rasch einbrechen, und damit würden auch seine eigenen Coins und seine auf das Mining spezialisierte Hardware ihren Wert verlieren. Und auch der rasante →

technologische Fortschritt scheint aktuell keine Bedrohung für Bitcoin darzustellen. So wird etwa den in Entwicklung befindlichen Quantencomputern das Potenzial zugesprochen, klassische kryptografische Verfahren aushebeln zu können. „Theoretisch könnten sie die Signaturverfahren der Blockchains knacken“, sagt Urbach. Signaturen dienen als Beweis dafür, dass jemand berechtigt ist, über ein bestimmtes Geldstück zu verfügen. Werden sie geknackt, könnte ein Angreifer also das Geld anderer Leute ausgeben. Hier spielt den Kryptowährungen allerdings in die Hände, dass die Entwicklung der Quantencomputer nur sehr langsam voranschreitet und es auch bereits alternative, quantensichere Signaturen gibt.

Künstliche Intelligenz wiederum kann der Verschlüsselung einer Blockchain zwar nichts anhaben. Mit ihr ließe sich jedoch in großen Datenmengen nach Schwachstellen in den Anwendungen suchen, die auf ihnen aufbauen. Solche kleineren Sicherheitslücken von Kryptowährungen sind allerdings auch ohne KI schon identifiziert worden. Das betrifft oft die Schnittstellen zwischen der Blockchain und der restlichen digitalen Welt, etwa wenn klassische Währungen in Bitcoin umgetauscht werden. „Das sind nicht selten Einfallstore für Hacker, was in der Vergangenheit auch schon passiert ist“, sagt Urbach.

72

## Automatisierte Geschäfte

Die Anwendung von Blockchains ist dabei längst nicht auf die Verwaltung von Kryptowährungen beschränkt. In ihren Blöcken lassen sich etwa auch automatisierte Abläufe für Geschäfte aller Art, sogenannte Smart Contracts, abspeichern. Smart Contracts sind nichts anderes als ein Programmcode auf einer Blockchain, der wie ein automatisierter Treuhänder agiert. Das bedeutet, man legt vorher fest, was mit einem Geldbetrag passieren soll, und das System führt diese Anweisungen exakt aus. Ein typisches Anwendungsbeispiel ist Crowdfun-

ding: Viele Menschen überweisen an eine Zielperson, die das Geld aber erst abheben kann, sobald das Funding-Ziel erreicht ist. Wird es verfehlt, bekommt automatisch jeder sein Geld zurück. Damit das zuverlässig funktioniert, muss die Programmierung des Contracts allerdings wasserdicht sein. „Durch Fehler, die sich in die Contracts einschleichen, entstehen aber leider immer wieder Sicherheitsrisiken“, sagt Urbach.

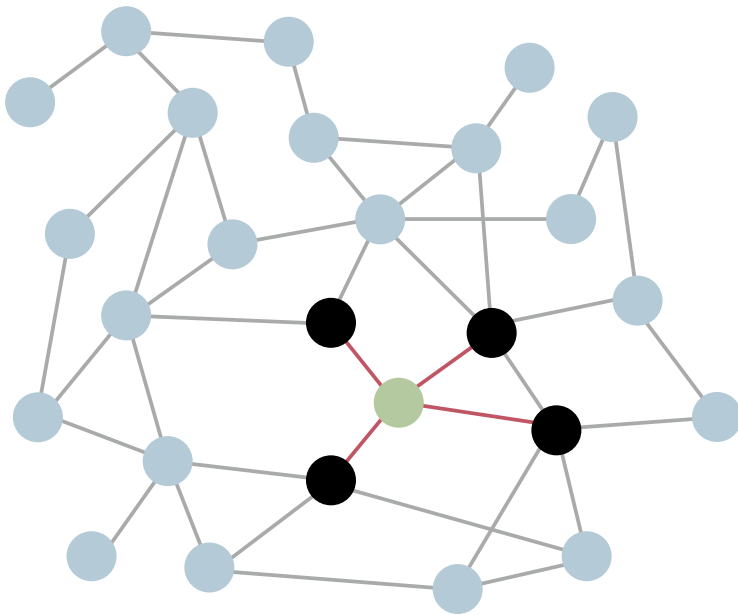
Ein prominentes Beispiel dafür ist der DAO-Hack von 2016: The DAO, eine

dezentrale, autonome Organisation auf Blockchain-Basis, wollte per Crowdfunding Geld einsammeln, doch Angreifer fanden einen Softwarefehler und nutzten ihn schamlos aus. Der Smart Contract war nämlich so programmiert, dass er allen Beteiligten das Recht einräumte, ihr eingezahltes Geld auch vorzeitig wieder zurückzuverlangen. Allerdings stimmte dabei die Reihenfolge nicht: Um Betrug zu verhindern, sollte der neue Kontostand eigentlich zuerst festgehalten und erst danach das Geld überwiesen werden. Da das Programm aber einen



FOTO: JUDITH WALLERUS

Sucht die Schwachstellen der Kette: Clara Schneidewind erforscht, welche Sicherheitslücken es in der Blockchain und ihren Anwendungen gibt.



Verdunkelte Nachbarschaft: Betrug in der Blockchain ist unter anderem durch den Eclipse-Angriff möglich. Dabei könnten Cyberkriminelle im Teilnehmernetz die nächsten Nachbarn eines Mitwirkenden kapern und diesem mit einer manipulierten Blockchain etwa Zahlungen vorgaukeln.

Fehler enthielt und den Kontostand erst nachträglich aktualisierte, ließ es einen kurzen Moment entstehen, in dem der Angreifer noch eine weitere Rücküberweisung veranlassen konnte, bevor der Contract die erste Auszahlung registriert hatte. So konnte er das Geld gleich mehrmals hintereinander zurückerhalten und Kryptowährung im Wert von 50 Millionen US-Dollar erbeuten.

Probleme mit Smart Contracts sind auch einer der Forschungsschwerpunkte von Clara Schneidewind. In einer aktuellen Arbeit hat sie sich mit ihrem Team vom Max-Planck-Institut für Sicherheit und Privatsphäre einen besonders schwierigen Fall vorgenommen: Smart Contracts, die über unterschiedliche Blockchains hinweg funktionieren sollen. „Es ist schwierig genug, den Code für eine einzelne Blockchain richtig zu schreiben“, sagt die Wissenschaftlerin. „Es wird aber noch einmal ein ganzes Stück komplizierter, wenn unterschiedliche Kryptowährungen im

Spiel sind.“ Denn in diesem Fall müssen zwei Contracts – einer auf jeder Blockchain – miteinander kommunizieren. Damit Nutzer dann sicher interagieren können, sind komplizierte kryptografische Protokolle erforderlich. Mit BitMLx hat Schneidewinds Team ein Protokoll für solche Cross-Chain-Kommunikationen entwickelt. Vereinfacht lässt sich die Funktionsweise am Beispiel eines Tausches unterschiedlicher Kryptowährungen veranschaulichen: Person A hat Bitcoin, Person B besitzt einen entsprechenden Betrag in der Kryptowährung Ethereum. Sie wollen tauschen, vertrauen sich aber nicht. Das lässt sich durch ein kryptografisches Geheimnis lösen, eine Art Passwort, das man kennen muss, damit man das Geld des anderen abheben kann und auch kein Dritter drankommt. Am Anfang kennt es nur Person A und legt als Erste ihr Geld auf eine Art Treuhandkonto in der Blockchain. Dann legt Person B ihren Betrag ebenfalls auf ein Treuhandkonto. Erst

wenn A sich diesen holt, wird das Geheimnis automatisch für B sichtbar, die nun ihrerseits das Geld von A abheben kann. „Wir haben bewiesen, dass mit unserem Protokoll ein ehrlicher Nutzer bei der Ausführung eines solchen Vertrags niemals Geld verlieren wird – egal was andere Beteiligte tun“, sagt Schneidewind.

So tragen Clara Schneidewind und ihr Team dazu bei, bestehende Sicherheitslücken von Smart Contracts und Kryptowährungen nach und nach zu schließen. Selbst würde die Informatikerin dennoch nicht in Bitcoin und Co. investieren wollen. Als Forscherin sei es ihr wichtiger, unvoreingenommen zu bleiben. Wer selbst große Mengen einer Währung hält, kann schließlich schnell in einen Interessenskonflikt geraten. Wer würde schon eine Sicherheitslücke publizieren, die den Wert des eigenen Vermögens vernichtet? Es gibt allerdings auch noch einen weiteren Grund für ihre Abstinenz: „Wenn man von der Forschungsseite aus sieht, was alles schiefgehen kann, lässt man lieber die Finger davon.“ ←

73

## GLOSSAR

### BLOCKCHAIN

heißt eine Datenbank von Geldtransaktionen und anderen Geschäftsvorgängen, die dezentral bei allen Teilnehmern gespeichert werden. Geldtransfers und andere Änderungen an Besitzverhältnissen werden dabei in neu generierten kryptografisch geschützten Blöcken gespeichert.

### PROOF OF WORK

ist eine Methode, bei der die Teilnehmer einer Blockchain ihre Rechenkraft unter Beweis stellen müssen. Bei der Blockchain wird eine kryptografische Aufgabe gelöst und so gleichzeitig der verschlüsselte Fingerabdruck der bisherigen Kette erzeugt. Wer die Aufgabe zuerst löst, darf den nächsten Block erzeugen und wird dafür mit Kryptogeld entlohnt.

### SMART CONTRACT

wird ein Programm genannt, das einen automatisierten Geschäftsprozess, wie etwa den Wechsel von Besitzverhältnissen, in der Blockchain abbildet.