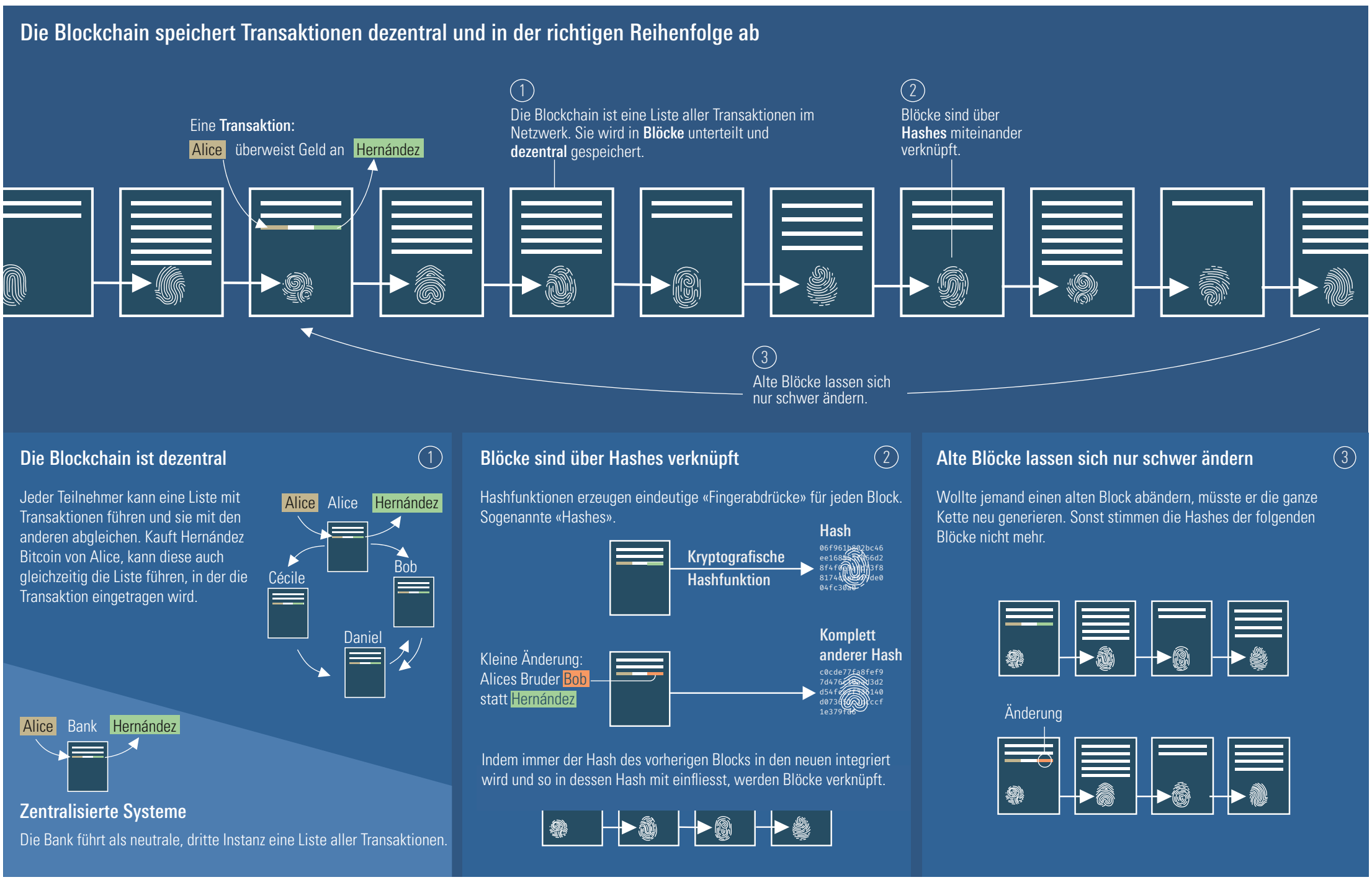

Bitcoins müssen grüner werden

Kryptowährungen sind mehr als spekulative Geldanlagen. Sie können Menschen in instabilen Regionen helfen und die Bankenwelt verändern. Umso wichtiger sind Ideen, ihren ungeheuren Strombedarf zu senken.

VON RUTH FULTERER UND JONAS OESCH

Bitcoins und andere Kryptowährungen erleben einen Hype. Keine Woche vergeht ohne Meldung über Kursrekorde. Doch es gibt einen Nutzen abseits der Spekulation.

Für Carlos Hernández war der Bitcoin Rettung der eigenen Existenz. Der Ökonom lebt in Venezuela, einem Land, das eine Hyperinflation durchmacht. 2018 betrug sie offiziell 130 000 Prozent, nach Schätzungen noch mehr. Ein Lebensmitteleinkauf zu 80 Franken würde bei dieser Inflationsrate ein Jahr später 104 000 Franken kosten. Hernández beschreibt in einem Artikel für die «New York Times», wie er mithilfe von Bitcoins seine Familie durchbringen konnte. Die Kryptowährung behielt ihren Wert, und er konnte sie über eine Tausch-Website jeweils vor dem Einkaufen in Bolívar umtauschen, um Essen zu kaufen. Seinem Bruder habe er so Geld für die Flucht nach Kolumbien mitgeben können, vor korrupten Grenzkontrolleuren sicher versteckt, nur mit den richtigen Zugangsdaten im Internet erreichbar.

Marktmacht fairer verteilen

Kryptowährungen und die Technologie, auf der sie basieren, machen Menschen unabhängiger vom lokalen Geldsystem. Künftig könnten sie das Zahlungssystem verändern und Zwischenhändler ausschalten und damit die Marktmacht im Internet fairer verteilen. Das Problem dabei: Kryptowährungen brauchen absurd viel Energie. Jede einzelne Überweisung in Bitcoins benötigt etwa so viel Energie, wie ein Schweizer in eineinhalb Monaten verbraucht. Das Bitcoin-Netzwerk insgesamt verbraucht mittlerweile in einem Jahr mehr Strom als alle Schweizer zusammengenommen in derselben Zeit.

Ethereum ist das zweitgrösste Krypto-Netzwerk. Dessen Erfinder, Vitalik Buterin, sagt im Magazin des internationalen Ingenieurverbands IEEE: «Es ist eine enorme Verschwendung von Ressourcen, selbst wenn man nicht glaubt, dass Verschmutzung und Kohlendioxid Probleme sind. Es gibt echte Konsumenten, echte Menschen, deren Bedarf nach Elektrizität durch Kryptowährungen verdrängt wird.»

> Jede Überweisung in Bitcoins benötigt etwa so viel Energie wie ein Schweizer in eineinhalb Monaten.

Doch warum sind diese Krypto-Netzwerke überhaupt so energieaufwendig?

Um den massiven Stromverbrauch zu verstehen, muss klar sein, was die Krypto-Netzwerke überhaupt leisten wollen. Der weltweite Zahlungsverkehr basiert grösstenteils auf unserem Vertrauen in Finanzinstitutionen. Sie sind es, die sicherstellen, dass jemand Guthaben überweisen und jemand anderes das Guthaben empfangen kann. Wenn Carlos Hernández sich online etwas bestellt, vertraut er darauf, dass der Verkäufer nicht einfach behaupten kann, dass kein Geld angekommen ist. Eine Instanz, etwa eine Bank, stellt sicher, dass alle Kontostände korrekt sind. Sie hat die Übersicht und koordiniert. Diese zentrale Drittpartei wollen Krypto-Netzwerke aber ausschalten. Das macht unabhängig von Institutionen und ihren Servern. Dafür nutzen sie die sogenannte «Blockchain», eine dezentrale Art der Speicherung.

Eine Blockchain ist eine Liste von Transaktionen. Ist eine Überweisung gemacht, bleibt das in der Blockchain vermerkt. Die Liste ist einsehbar, allerdings ist die Identität der Teilnehmer unbekannt. Sie alle verstecken sich hinter einer ID aus Nummern und Buchstaben. Die Überweisungen können nicht gelöscht werden, weil alle Beteiligten eine eigene Kopie lokal speichern.

Die Herausforderung ist, sicherzustellen, dass die Liste nur korrekt bearbeitet werden kann und alle denselben Stand haben. Sonst würde sie nicht als verlässliches Dokument taugen. Deshalb gibt es bestimmte Regeln, wie an der Liste geschrieben werden kann. Die Liste ist in Abschnitte, sogenannte Blöcke, eingeteilt. Alte Blöcke lassen sich nicht einfach so abändern, weil alle neueren Blöcke mit dem vorhergehenden Block verknüpft sind, und zwar durch eine Zahl, den Hash.

Ein Hash entsteht, wenn man Text oder Zahlen, in diesem Fall eine Liste von Transaktionen, in eine kryptografische Hashfunktion einspeist. Er «gehört» zur Liste so eindeutig wie ein Fingerabdruck zu einer Person. Es ist einfacher, von einem Menschen auf seinen Fingerabdruck zu schliessen, als den Urheber eines Fingerabdrucks zu finden. Und das gilt auch für einen Hash. Diesen kann man leicht errechnen, aber den Rückweg nicht. Den Ursprungswert kann man nach derzeitigem Wissensstand mathematisch nicht ermitteln.

Wer einen Eintrag in einem alten Block ändern wollte, müsste auch alle darauf folgenden Blöcke abändern und somit eine alternative Blockchain konstruieren. Was aber, wenn jemand sich diese Mühe machen wollte, etwa, um sich zu bereichern?

Die Blockchains von Bitcoin und Ethereum haben jeweils einen Schutzmechanismus eingebaut, der das impraktikabel macht. Dieser Mechanismus ist der Grund für den heute sehr hohen Energieverbrauch. Das Erzeugen der Hashes, also der Schlüsselzahlen, die die Blöcke miteinander verbinden, wird nämlich künstlich erschwert.

Rennen um den nächsten Block

Das System funktioniert so: Alle Transaktionen, die es zu bestätigen gilt, sind in einer Art Warteschlange versammelt. Wer sie bestätigen will, bündelt Tausende von ihnen zu einem Block und errechnet mit der Hashfunktion einen Hash daraus. Zum Fortführen der Kette wird jedoch nicht jeder Hash akzeptiert, den die Hashfunktion ausspuckt. Sondern es gibt Vorgaben, wie er auszusehen hat. Bei Bit-