Neue Zürcher Zeitung

Eine einzige Überweisung in Bitcoins verbraucht so viel Energie wie ein Schweizer in eineinhalb Monaten

Kryptowährungen sind mehr als eine Spekulationsanlage. Sie können Menschen in instabilen Regionen helfen und das Bankenwesen grundsätzlich verändern. Umso wichtiger sind die Ideen, sie umweltfreundlicher zu machen.

Ruth Fulterer, Jonas Oesch

05.04.2021, 05.30 Uhr

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 erlebt. 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.

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.

Inhaltsverzeichnis

8. Lösungen sind dringend gefragt, denn Kryptowährungen werden sich weiter ausbreiten ↓

---

1. So viel Strom fressen Kryptowährungen ↑

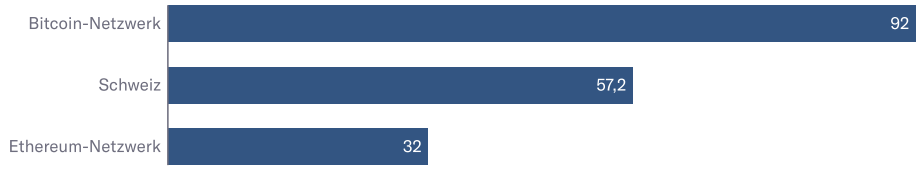
Jede einzelne Überweisung in Bitcoins benötigt etwa so viel Energie, wie ein Schweizer in eineinhalb Monaten verbraucht.

Stand: 1. 4. 2021
Quellen: Digiconomist, Bundesamt für Energie

Das Bitcoin-Netzwerk insgesamt verbraucht mittlerweile in einem Jahr mehr Strom als alle Schweizer zusammengenommen in derselben Zeit.

Das Bitcoin-Netzwerk verbraucht pro Jahr mehr Strom als die Schweiz

Jährlicher Energieverbrauch in Terawattstunden



Stand: 1. 4. 2021
Quellen: Digiconomist, Bundesamt für Energie

NZZ / joe.

Ethereum ist das zweitgrösste Krypto-Netzwerk. Darauf basiert auch die Währung Ether. Wie das Bitcoin-Netzwerk verbraucht Ethereum sehr viel Energie, Tendenz steigend.

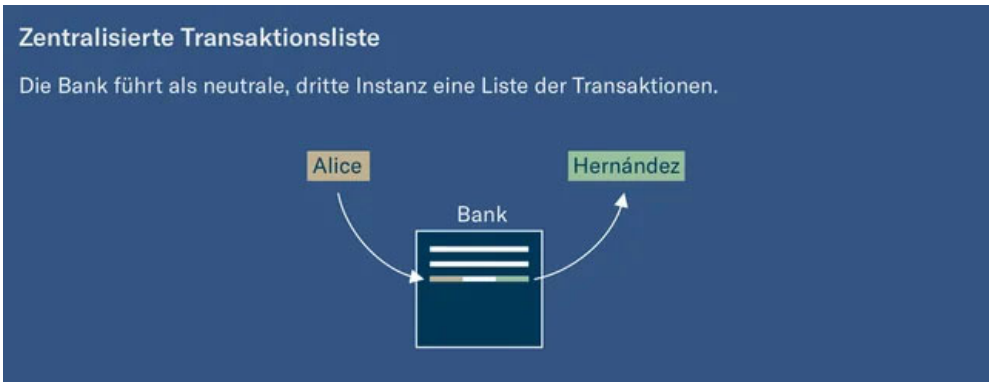
Dessen Erfinder, Vitalik Buterin, will das ändern: «Es ist eine enorme Verschwendung von Ressourcen, selbst wenn man nicht glaubt, dass Verschmutzung und Kohlendioxid Probleme sind. Es gibt echte Konsumenten, echte Menschen, deren Bedarf nach Elektrizität durch Kryptowährungen verdrängt wird», zitiert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

Doch warum sind diese Krypto-Netzwerke überhaupt so energieaufwendig?

2. Bitcoin baut auf stromintensives Rätselraten

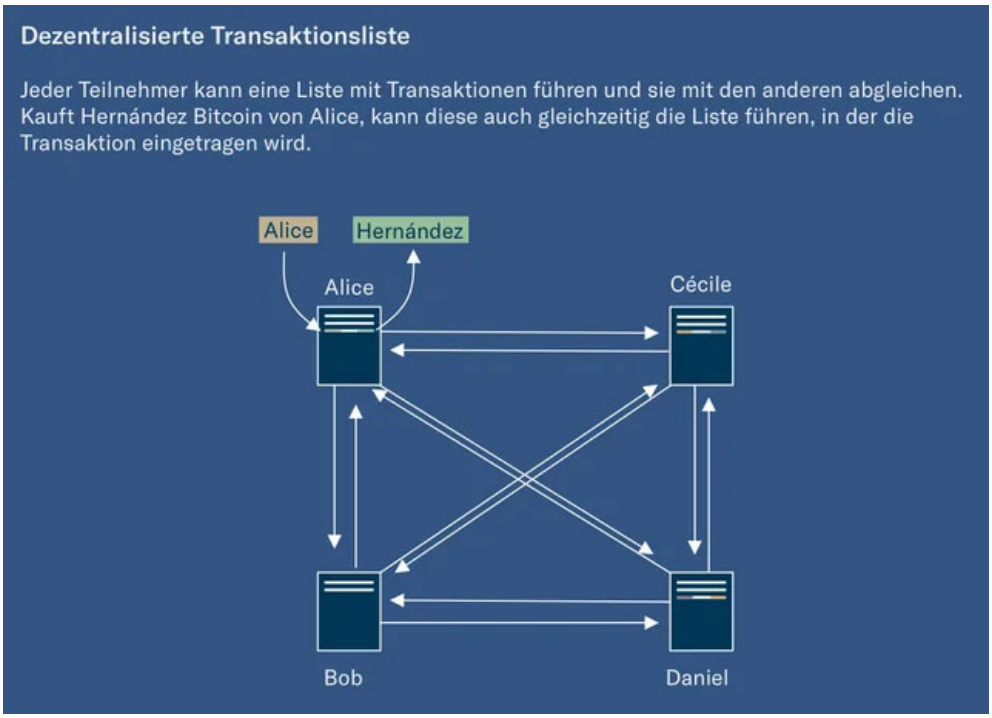
Um den massiven Stromverbrauch zu verstehen, muss klar sein, was die Krypto-Netzwerke überhaupt leisten wollen.

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.

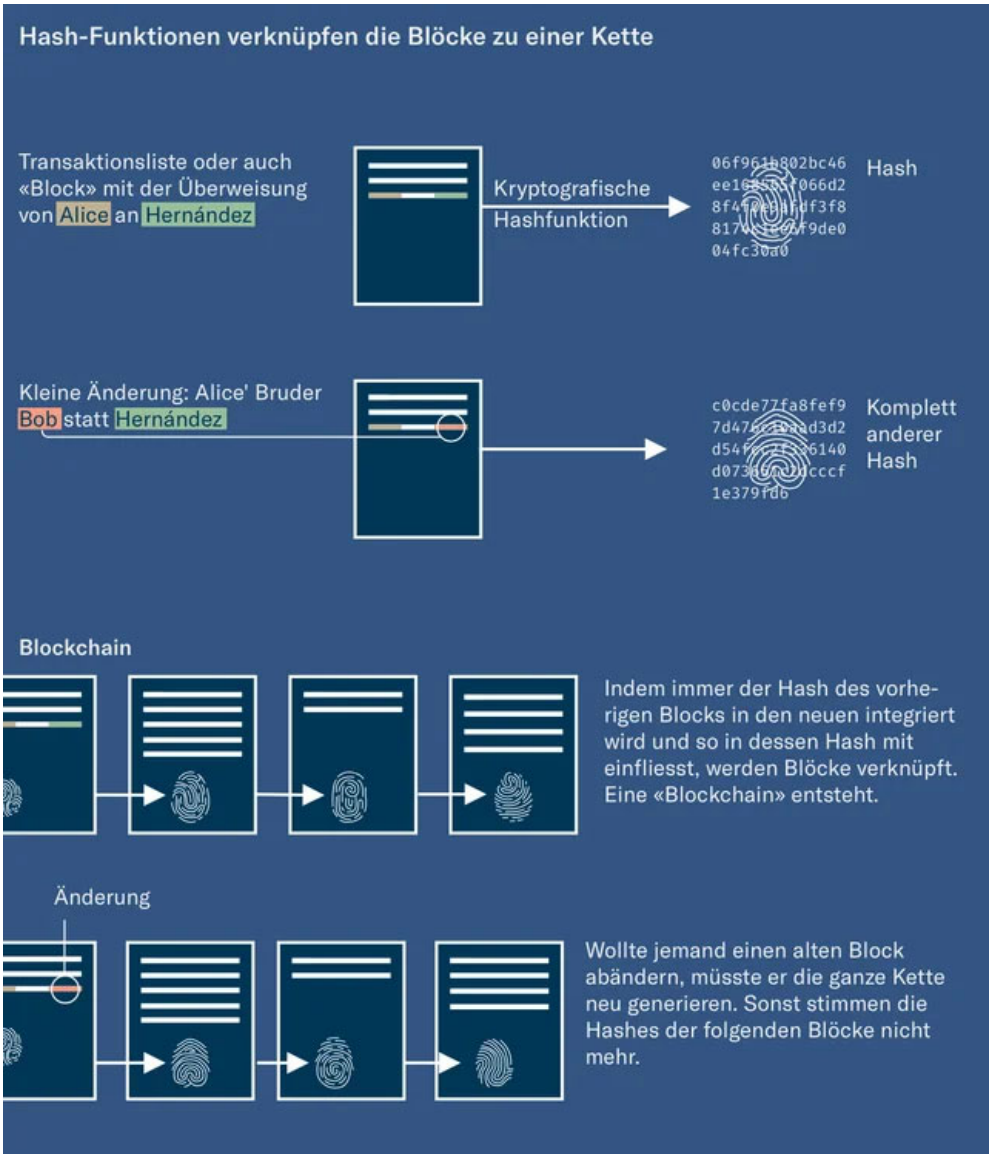
Die Liste ist in Abschnitte, sogenannte Blöcke, eingeteilt. Alte Blöcke lassen sich nicht einfach so abändern, weil alle neueren Blöcke mit dem vorhergehenden Block verknüpft sind, und zwar durch eine Zahl, den Hash.

3. Die Hashfunktion gibt jedem Block einen Fingerabdruck

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 die Mühe machen wollte, eine alternative Blockchain zu generieren, etwa mit Transaktionen, die sie oder ihn 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.

4. Mining: Weltweiter Wettstreit um den nächsten Block

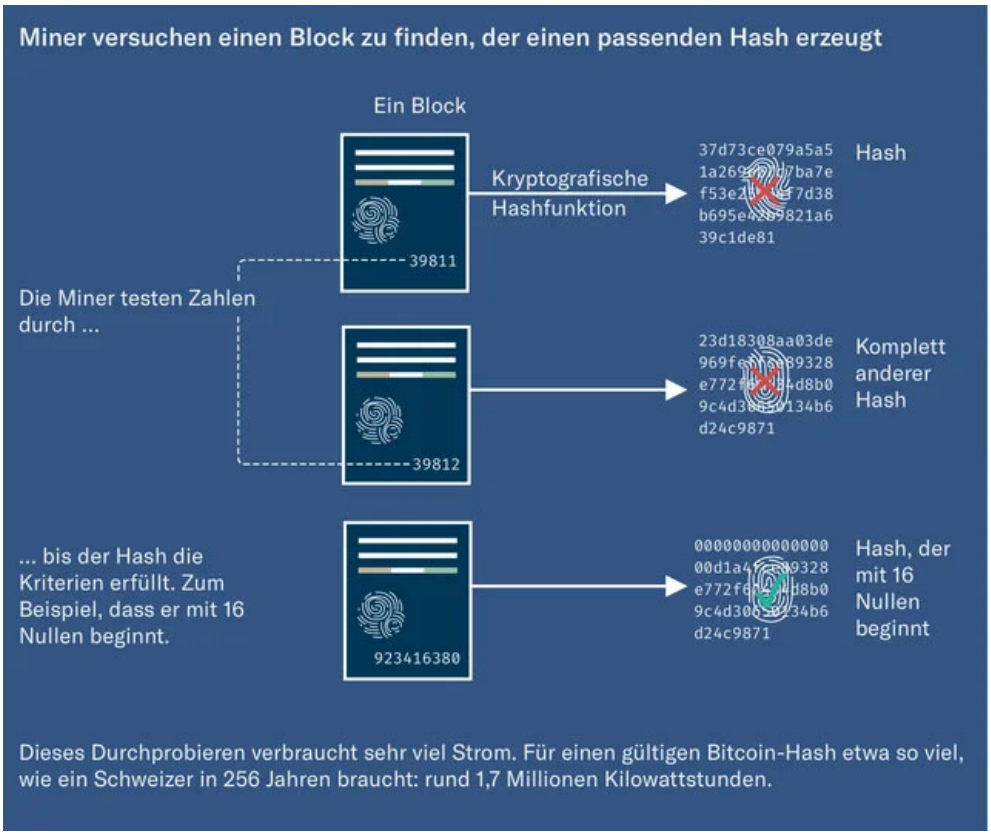
Das System funktioniert so: Alle Transaktionen, die es zu bestätigen gilt, zum Beispiel jene von Alice an Hernández, sind in einer Art Warteschlange versammelt. Wer sie bestätigen will, bündelt Tausende von ihnen zu einem Block und errechnet mit der Hashfunktion einen Hash daraus.

Zum Fortführen der Kette wird jedoch nicht jeder Hash akzeptiert, den die Hashfunktion ausspuckt. Sondern es gibt Vorgaben, wie er auszusehen hat. Bei Bitcoin zum Beispiel, dass er mit einer bestimmten Anzahl Nullen beginnt.

Um den passenden Hash zu finden, probieren Rechner verschiedene Kombinationen aus Transaktionen, ihrer eigenen ID und einer Zusatzzahl durch, bis irgendwann per Zufall ein Hash entsteht, der richtig aussieht.

Einen passenden Hash zu finden, ist aufwendig. Er kann nicht errechnet werden, sondern nur durch Durchprobieren gefunden werden. Das braucht Unmengen an Rechenleistung und Strom.

Vor allem, weil weltweit nicht nur ein Rechner nach dieser Zahl sucht, sondern viele zugleich. Es gibt unzählige sogenannter «Miner», also Rechner, die auf das Lösen genau dieses Rätsels getrimmt sind. Sie alle probieren verschiedene Kombinationen durch. Derjenige, bei dem die Hashfunktion als erstem einen passenden Hash ausspuckt, gewinnt. Er schickt die Lösung ans Netzwerk, das nachprüfen kann, ob alles stimmt. Dann beginnt das Spiel von neuem.



Stand: 1. 4. 2021

Es ist eine Art Lotterie. Der Gewinner hängt seinen neuen Block an die Kette und erhält dafür eine Belohnung in der

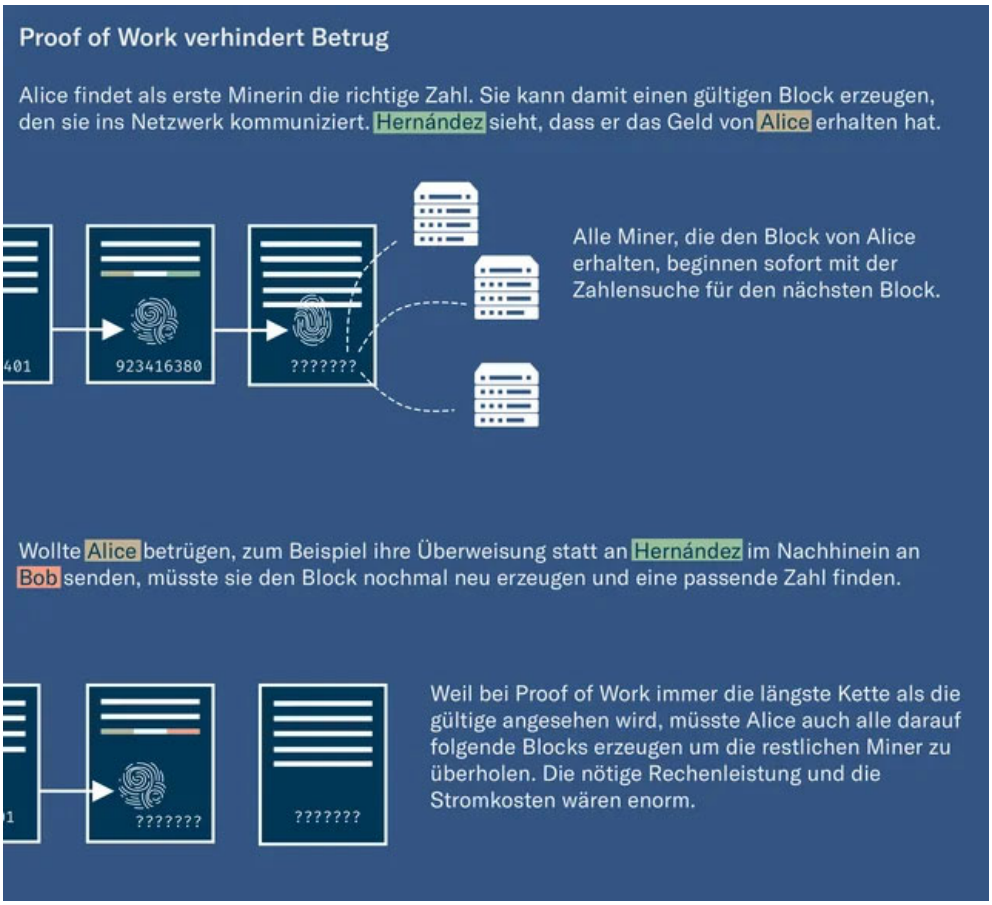
Kryptowährung. Derzeit beträgt diese im Fall von Bitcoin 6,25 Coins, umgerechnet gut 300 000 Franken. Dazu kommen Transaktionsgebühren. Wer Carlos' Überweisung bestätigt, darf dessen Gebühren behalten. Die aus dem Nichts generierte Belohnung lässt die Geldmenge im Bitcoin-Netz steigen.

5. Die hohe nötige Rechenleistung soll Betrug verhindern ↑

Der Betrag mag hoch erscheinen, aber ein guter Teil davon geht für den Strom drauf, den es kostet, sich am «Mining» zu beteiligen. Für den Miner bleibt nur eine Marge übrig. Wenn der Strom zu teuer ist, zahlt sich die ganze Sache nicht mehr aus. Deshalb stehen viele der Mining-Rechner in Gebieten mit billigem Strom, etwa in Island oder in der Nähe von Kohlekraftwerken in der Mongolei.

Die hohen Kosten für das Mining helfen dabei, vor Betrug zu schützen: Um einen alten Block abzuändern, müsste eine Angreiferin die ganze darauf folgende Kette neu generieren – und damit noch schneller sein als alle anderen Miner zusammen, die an der richtigen Kette arbeiten. Dazu müsste sie mehr Rechenleistung ansammeln als die anderen. Dass das funktioniert, ist unwahrscheinlich.

Deshalb gehen Netzteilnehmer davon aus, dass die längste Kette die gültige ist, weil dort die unmanipulierten Transaktionen gespeichert sind. Diese Art der Absicherung heisst Proof of Work.



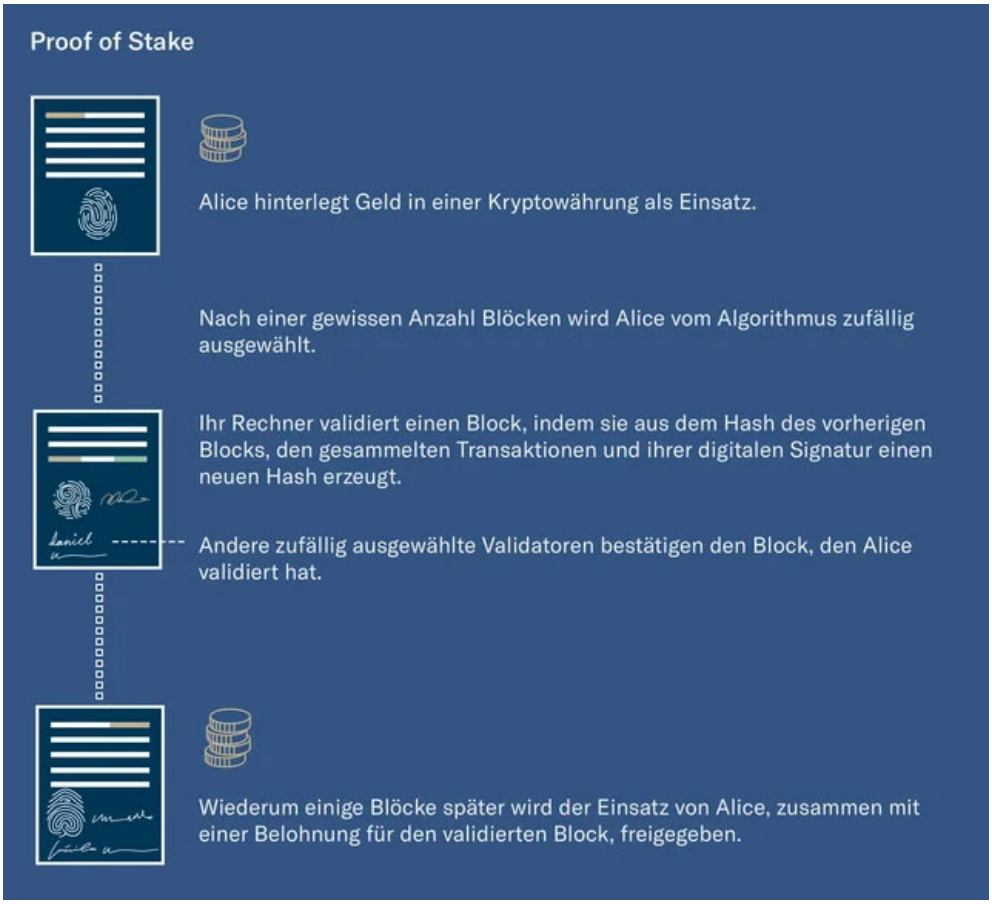
Der enorme Stromverbrauch von Kryptowährungen liegt also direkt im Schutzmechanismus Proof of Work begründet. Deshalb will die Stiftung hinter der Ethereum-Blockchain auf einen alternativen Mechanismus umsteigen, der den Betrug auf eine andere Art unrentabel machen soll. Man nennt ihn Proof of Stake.

6. Die energiesparende Alternative: Proof of Stake

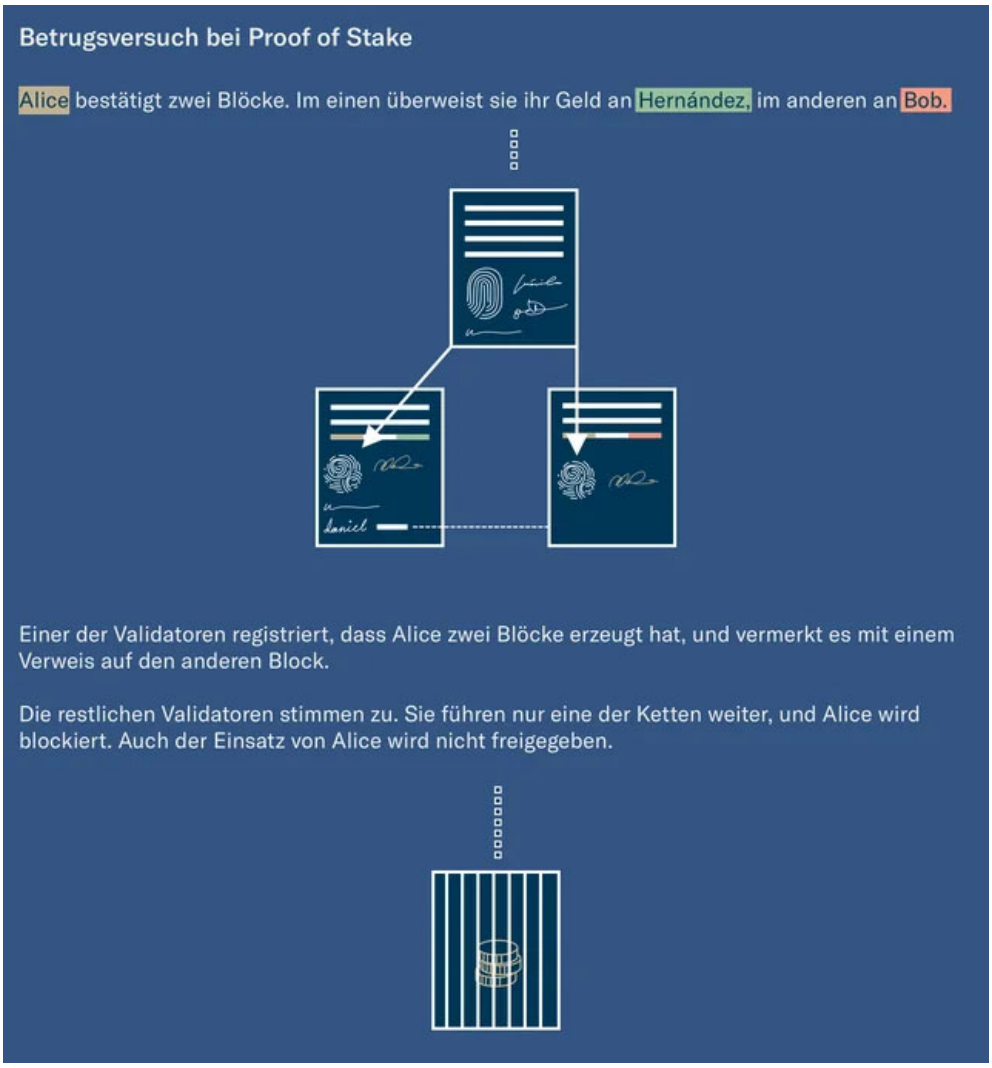
Bei diesem ist statt Rechenleistung ein Geldeinsatz («Stake») notwendig, um als sogenannter Validator durch ein Computerprogramm die Kette prüfen und neue Blöcke erzeugen zu dürfen. Proof-of-Stake-Verfahren können verschieden aussehen. Im Folgenden geht es um jenes, das den Stromverbrauch der Blockchain Ethereum und der dazu

gehörigen Kryptowährung Ether auf einen Bruchteil reduzieren soll.

Das funktioniert so: Wer an der Kette bauen will, muss einen Geldeinsatz hinterlegen. Dieses Geld wird nur zurückerstattet, wenn an der richtigen Kette weitergebaut wurde, also jener, die auch die Mehrheit der anderen Netzteilnehmer akzeptiert. Wer korrekt handelt, bekommt den Geldeinsatz zurück und als Belohnung Transaktionsgebühren obendrauf.



Wenn ein Validator betrügen möchte und nachweislich zwei verschiedene Ketten bestätigt, kann sein Einsatz durch eine Mehrheit der anderen Validatoren blockiert werden. Wer betrügt, riskiert also sein hinterlegtes Geld.



Das Regelwerk von Ethereum 2.0 ist noch um einiges umfangreicher. Die Essenz ist jedoch immer, dass Validatoren zumindest einen Teil ihres Einsatzes verlieren, wenn sie sich nicht konform verhalten.

Zusammengefasst gibt es mit Proof of Work und Proof of Stake also zwei verschiedene Methoden, um Betrug unrentabel zu machen. Es steht jeweils viel Geld auf dem Spiel. Entweder jenes, das man in Mining-Hardware und Strom investiert hat, oder jenes, das man als Einsatz hinterlegt hat. Wer sich an die Regeln hält, soll jeweils mehr verdienen, als durch Betrug möglich ist.

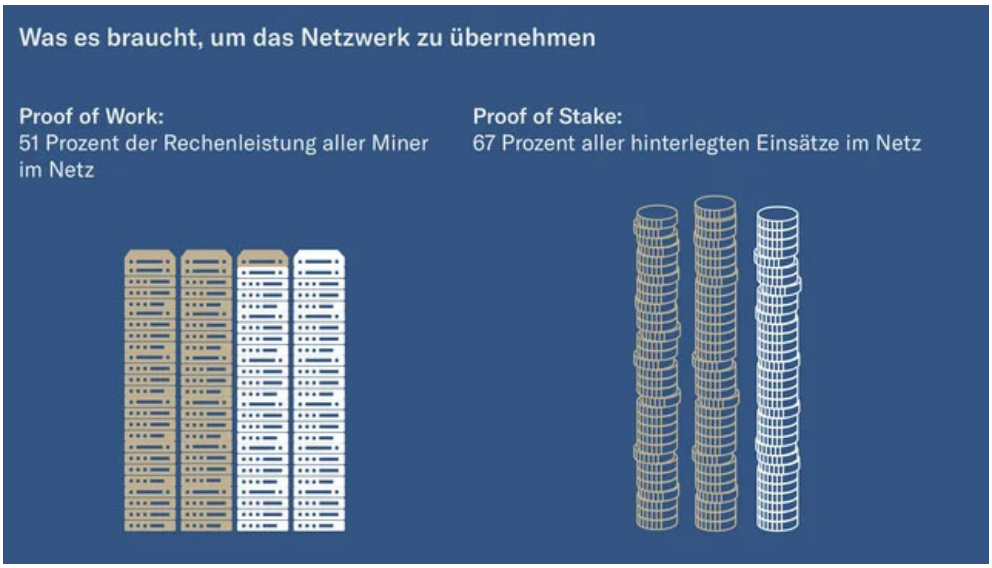
7. Warum Proof of Stake noch kaum verbreitet ist ↑

Es gibt mehrere Gründe, warum das energieintensive Mining nicht schon längst Geschichte ist: Erstens ist der Proof of Stake recht neu. Zweitens gibt es Kritik an dieser Methode der Validierung. Und drittens kann so ein Wechsel nicht einfach von den Erfindern beschlossen werden.

Vielen Bitcoin-Nutzern ist der Proof of Work heilig. Sie sehen in ihm ein vollendetes Design, einfach und komplett dezentral. Gerade die Fans aus der Anfangszeit verbinden Bitcoins mit einer libertären Utopie einer Gesellschaft, in der weder der Staat noch grosse Unternehmen viel zu sagen haben. Abweichungen von der ursprünglichen Blockchain macht sie argwöhnisch, weil sie die dezentrale Struktur in Gefahr sehen.

Pascal Hügli, der sich seit Jahren mit Bitcoin beschäftigt und ein Buch dazu geschrieben hat, spricht eine Tendenz zur Akkumulierung an, wenn jene belohnt werden, die im System viel Geld besitzen. Das sei beim Proof of Work nicht der Fall: «Die Ausgaben für Energie stellen sicher, dass Miner auch Coins verkaufen müssen, um sich zu finanzieren. So konzentriert sich das Geld nicht so einfach bei wenigen Teilnehmern.»

Grosse Diskussionen gibt es um die Sicherheit. Ganz gegen Angreifer gefeit sind weder Proof of Stake noch Proof of Work. Wenn eine Person oder ein Netzwerk von Personen es schafft, zu viel Macht zu erlangen, scheitern die Sicherheitsmechanismen. Im Fall von Proof of Work müssen mindestens 51 Prozent der Rechenleistung im System unter Kontrolle der Angreifer sein, im Fall von Proof of Stake 67 Prozent des Vermögens im System. Was leichter anzusammeln ist, lässt sich schwer sagen.



Argwohn besteht auch um die Bezeichnung Proof of Stake. Diese umfasst nämlich sehr verschiedene Systeme. In diesem Artikel sprechen wir von Ethereum 2.0, ein System, das grossen Wert auf Dezentralität legt. Dazu ist nötig, dass die Blockchain in vielen Kopien offen gespeichert und nicht von einer zentralen Macht kontrollierbar ist. Doch hinter dem Begriff Proof of Stake verstecken sich mitunter auch Systeme, die diesen Kriterien nicht genügen, etwa jene von Firmen, die ihre eigene Blockchain einfach lokal bei sich speichern. Kritiker fürchten deshalb Verwirrung und Etikettenschwindel bei diesem Begriff.

Und es gibt noch einen Grund, warum es Proof of Work noch länger geben wird: So eine Entscheidung kann nicht einfach von oben getroffen werden. Das ist gerade der Clou an dezentralen Netzwerken. Solange genug Teilnehmer an einer Kette bauen und sie akzeptieren, kann sie nicht einfach abgeschaltet werden. Änderungen wie der Umstieg der Blockchain von Ethereum starten als Parallelsysteme. Die Kette spaltet sich in zwei korrekte Ketten, und wenn alles nach Plan der Entwickler geht, werden immer mehr Nutzer

auf das energiearme System umsteigen, während das andere ausläuft.

Wahrscheinlich ist darum, dass mehrere Systeme nebeneinander existieren werden. Die Krypto-Community wird auf jeden Fall genau beobachten, was mit Ether 2.0 geschieht. Wenn die Währung in den kommenden Jahren ihre Stabilität und Sicherheit hält, könnten mehr Niedrigenergie-Blockchains entstehen.

8. Lösungen sind dringend gefragt, denn Kryptowährungen werden sich weiter ausbreiten

Neben Proof of Stake gibt es auch andere Ideen, um Blockchain-Transaktionen energetisch günstiger zu machen. Damit beschäftigt sich auch Fabian Schär, Professor an der Universität Basel. Er erforscht, wie offene Blockchain-Systeme und Krypto-Assets das Finanzsystem verändern werden. Es handelt sich um sogenannte Layer-2-Lösungen – also Methoden, welche die Sicherheit von der Ursprungs-Blockchain nutzen, ohne dass alle Transaktionen auf dieser abgewickelt werden müssen.

«Einfach erklärt, blockieren besonders aktive Teilnehmer einen Vermögenswert auf der Blockchain. Dieser dient als Sicherheit. Abhängig von dem genauen System können dann entweder ganze Transaktionen oder einzelne Berechnungsschritte ausgelagert und entweder gar nicht oder nur teilweise auf der Blockchain eingetragen werden», sagt Schär. Die Auslagerung sei dabei so ausgestaltet, dass ein allfälliger Regelverstoss einer Partei durch die jeweils anderen Parteien mathematisch bewiesen und auf die hinterlegte

Sicherheit der betrügerischen Partei zugegriffen werden könne.

Das Auslagern von Transaktionen in Layer 2 machen den Gebrauch von Krypto-Netzwerken nicht nur energieeffizienter, sondern auch schneller und billiger – ein wichtiges Argument für jene, die noch viel Potenzial in der Technologie sehen.

Bitcoin entstand ab 2008, in den Nachwehen der Finanzkrise. Die Blockchain-Technologie ist immer noch jung. Es wird gerade viel ausprobiert. Schär sagt: «Die Breite der Anwendungen der Blockchain wird meist überschätzt – zugleich wird unterschätzt, wie sehr sich die betroffenen Sparten verändern werden.» Er meint damit vor allem den Finanzmarkt und den Einfluss zentraler Finanzprotokolle.

Kryptowährungen setzen Banken und Firmen wie Paypal oder Western Union unter Druck, die für das Verschicken von Geld teilweise sehr hohe Gebühren verlangen. Wenn sie hier untätig bleiben, könnten sie den Anschluss verpassen. Das werde der Branche langsam bewusst, meint Hügli. Er hat für sein Buch «Ignorieren auf eigene Gefahr: Die neue dezentrale Welt von Bitcoin und Blockchain» unter anderem Grafiker aus Pakistan beauftragt und ganz selbstverständlich mit Bitcoin bezahlt.

Mehr zum Thema

DIE NEUSTEN ENTWICKLUNGEN

Bitcoin klettert erstmals über 60 000 Dollar

Nachdem das Rally des Bitcoin zwischenzeitlich gestoppt wurde, erreichte die Kryptowährung am Wochenende einen neuen Höchstwert. Die wichtigsten Fakten zum Hype und zur Kryptowährung.

Werner Grundlehner / Thomas Schürpf 13.03.2021

Digitale Collage des amerikanischen Künstlers Beeple für 69,3 Millionen Dollar versteigert

Im Kunstmarkt ist ein neues Kapitel aufgeschlagen worden. Eine Datei des amerikanischen Künstlers Beeple wurde an einer Versteigerung des Auktionshauses Christie's am Donnerstag für knapp 70 Mio. $ einem Käufer zugeschlagen.

Christin Severin 11.03.2021

Auf der Suche nach dem «fairen» Wert des Bitcoins

Die Kryptowährung ist innert Monatsfrist von 20 000 auf über 41 000 Dollar geklettert. Ist der Bitcoin wirklich das neue «digitale Gold»?

Werner Grundlehner 09.01.2021

GASTKOMMENTAR

Die Schweiz hat das Potenzial, der weltweit führende Blockchain-Hub zu werden

Die Schweiz hat das Glück, dass mit der Blockchain-Technologie vor ihrer Haustüre eine der nächsten grossen Technologien mit vielen grossartigen Ideen und Startups entsteht. Diese Chance muss das Land packen.

Johann Niklaus Schneider-Ammann 08.02.2021

Die digitale Aktie ist da – und es läuft nicht wie erwartet

Die Tokenisierung hat in der Schweiz ein rechtliches Fundament erhalten – trotzdem ist es still um digitale Vermögenswerte geworden.

Werner Grundlehner 16.03.2021