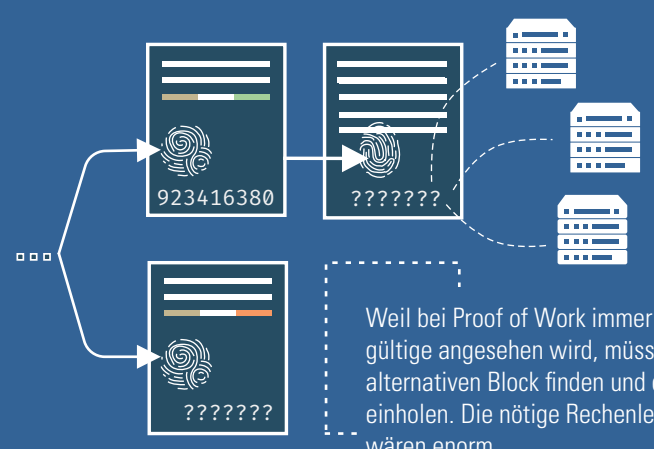
«Proof of Work» und «Proof of Stake» sind zwei Methoden, um Blockchains vor Betrug zu schützen

Proof of Work – Einen Block erzeugen

Ein Block ist nur gültig, wenn der Hash, der daraus entsteht, mit einer bestimmten Anzahl Nullen beginnt. «Miner» fügen so lange verschiedene Zahlen am Ende des Blocks ein, bis ein Hash entsteht, der den Kriterien entspricht. Dieses Durchprobieren verbraucht sehr viel Strom.

Alice probiert Zahlen durch, bis sie einen Block findet, dessen Hash mit 16 Nullen beginnt.

Proof of Work – Der Rechenaufwand wäre riesig

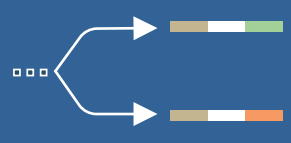


Alice findet als Erste einen gültigen Block. Sie kommuniziert ihn, inklusive ihrer Überweisung an Hernández, ins Netz. Die anderen Miner beginnen mit der Zahlensuche für den nächsten Block.

Weil bei Proof of Work immer die längste Kette als die gültige angesehen wird, müsste Alice eine Zahl für den alternativen Block finden und danach die anderen Miner einholen. Die nötige Rechenleistung und die Stromkosten wären enorm.

Wie ein Betrugsversuch unlukrativ gemacht wird

Alice versucht zu **betrügen** und ihr Geld im Nachhinein an ihren Bruder Bob statt an Hernández zu senden.



Proof of Stake – Einen Block validieren

Ein Block ist nur gültig, wenn er von einem zufällig ausgewählten «Validator» signiert wurde. Andere, ebenfalls zufällig ausgewählte Validatoren müssen den Block bestätigen. Um Validator zu werden, muss ein Einsatz in einer Kryptowährung hinterlegt werden.

Alice hinterlegt Geld in einer Kryptowährung als Einsatz.

Sie signiert einen Block, andere bestätigen ihn.

Alice erhält ihren Einsatz und eine Belohnung zurück.

Proof of Stake – Betrugsversuche kosten Geld

Einer der Validatoren registriert, dass Alice zwei Blöcke erzeugt hat, und vermerkt es mit einem Verweis auf den anderen Block.

Die restlichen Validatoren stimmen zu. Sie führen nur eine der Ketten weiter, und Alice wird blockiert.

Auch der Einsatz von Alice wird nicht freigegeben.

coin 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. Dieses Durchprobieren ist aufwendig. Es 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.

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 die Überweisung bestätigt, darf die Gebühren behalten. Die aus dem Nichts generierte Belohnung lässt die Geldmenge im Bitcoin-Netz steigen.

Alles für die Sicherheit

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.

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.

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.

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.

> Kryptowährungen setzen Banken und Firmen wie Paypal oder Western Union unter Druck.

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, einem 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. Wenn man an den Spielregeln von Ethereum Änderungen vornehmen will (zum Beispiel um von Proof of Work zu Proof of Stake umzusteigen), splittet sich die Blockchain. Es gibt danach das herkömmliche Ethereum und das neue. Das herkömmliche existiert so lange, bis niemand mehr neue Blöcke erzeugt. 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.

Lösungen sind dringend gefragt

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», sagt Schär. «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.» 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.