Kryptowährungs-Rechenzentrum neben einem Kohlekraftwerk in Kasachstan.

Wie viel Energie brauchen Blockchains?

Proof-of-Work ist am energieintensivsten | Für Kryptowährungen werden Blockchains heute schon eingesetzt, zugleich werden neue Anwendungsmöglichkeiten und Geschäftsfelder gesucht. In die Schlagzeilen geraten sie aber öfter wegen ihres Energieverbrauchs. Wie sieht es hier konkret aus? Und gibt es Entwicklungen zu sparsameren Blockchains?

RADOMÍR NOVOTNÝ

Blockchains sind Ketten von Datenblöcken mit Transaktionsinformationen, auf die öffentlich zugegriffen werden kann. Neue Transaktionen werden jeweils in einen Datenblock gepackt, mit einem Hash des letzten Blocks versehen und so an die existierende Kette hinzugefügt. In einer Blockchain wie Bitcoin sind also sämtliche Transaktionen enthalten. Kopien dieser Ketten werden dezentral auf vielen Computern gespeichert. Dieses Konstrukt ist darauf angelegt, dass verschiedene Parteien, die sich gegenseitig nicht vertrauen, ohne zentrale, vertrauenswürdige und vermittelnde Instanz Transaktionen ausführen können. Durch die Speicherung identischer Ketten an mehreren unabhängigen Orten und der Einbindung von kryptografischen Inhalten wird die Sicherheit markant erhöht – eine unerwünschte Manipulation an einer Version fällt anderen Benutzern schnell auf.

Als das Blockchain-Prinzip erfunden wurde, stand die Frage im Raum, wozu man es nutzen kann. Zunächst wurden Kryptowährungen realisiert. Später kamen mit neuen Blockchain-Konzepten auch ausführbare Programme hinzu, sogenannte Smart Contracts, die das Anwendungsfeld deutlich erweiterten: Heute werden Blockchains bei Notariaten, im Logistikbereich, bei Versicherungen, bei Herkunftsnachweisen und sogar in der Kunst eingesetzt.[1] Bei der digitalen Kunst konnte die Blockchain mit Smart Contracts ihren bisher grössten Erfolg verbuchen: Der auch als Beeple

Bild: Reuters/Pavel Mikheyev

bekannte Grafiker und digitale Künstler Mike Winkelmann konnte im Jahr 2021 eine Sammlung von 5000 Exemplaren seiner «Everyday»-Serie für 42329.453 Ether (was über 69 Mio. US$ entspricht) versteigern. Solche Preise begründen sich bei digitaler Kunst hauptsächlich durch die nachweisbare, fälschungssichere Eigentümerschaft und die Seltenheit des digitalen Objekts, kombiniert mit Inflationsängsten und dem Hype, der zu neuen Technologien gehört.

In welchem Mass sich Blockchains verbreiten werden, ist unklar. In einem Netzwoche-Interview äussert sich der Kryptologe Bruce Schneier skeptisch zum Einsatz von Blockchain: «Jedes Unternehmen, das heute auf die Blockchain setzt, könnte eigentlich auf sie verzichten. Niemand hatte jemals ein Problem, für das die Blockchain eine Lösung ist. Stattdessen nehmen die Leute die Technologie und machen sich auf die Suche nach Problemen.»[2] Diese Einschätzung wird beispielsweise für ihren Bereich auch von Software-Unternehmen geteilt, die im Energiesektor tätig sind und die die Blockchain für ihr Geschäft geprüft, aber abgelehnt haben.[3]

Der Hype wird aber nicht nur gedämpft, weil sich gewisse Aufgaben technisch einfacher als mit Blockchains lösen lassen, sondern weil die Grenzen des Konzepts klarer werden. Eine solche Limitierung ist der eingeschränkte Vertrauensbereich: Smart Contracts funktionieren nur innerhalb der virtuellen Blockchain-Welt vertrauenswürdig. Anwendungen, die mittels Sensoren mit der physischen Welt interagieren, müssen sich darauf verlassen können, dass die Sensordaten nicht manipuliert wurden bzw. dass die Sensoren korrekt funktionieren. Stimmt in der physischen Umgebung etwas nicht, bleibt dies der Blockchain verborgen und die Betreiber wähnen sich in falscher Sicherheit. Die sachliche Auseinandersetzung mit dem Blockchain-Konzept und seinen Beschränkungen führt deshalb zu einer allmählichen Ablösung des Hypes durch Ernüchterung.

Verschiedene Arten von Blockchains

Konsensmechanismen stellen bei Blockchains unter anderem sicher, dass ein Angreifer die Blockchain-Inhalte nicht durch eine sogenannte Sybil-Attacke manipulieren kann. Der erste Mechanismus, der bei Blockchains – konkret: bei Bitcoin – eingeführt wurde, ist Proof-of-Work, PoW. Dabei muss Arbeit in Form von Rechenleistung eingesetzt werden, um Transaktionen zu validieren und neue Blöcke der Blockchain anzufügen. Für die investierte Arbeit erhält der beteiligte spezialisierte Computer, der ein kryptografisches Rätsel durch «Versuch und Irrtum» zuerst löst, einerseits eine Belohnung in einer Kryptowährung, andererseits Transaktionsgebühren von den Teilnehmern, deren Transaktionen in den Block aufgenommen wurden. Die Belohnung motiviert Nutzer dazu, dieses energieintensive Mining zu betreiben. Löst ein Miner das Rätsel zuerst, kann er den Block auf dem Netzwerk veröffentlichen. Anschliessend können die anderen Nodes des Netzwerks ohne grossen Aufwand kontrollieren, ob die Aufgabe korrekt gelöst wurde. So entsteht der Konsens im Bitcoin-Netzwerk.

Da diese Art der Konsensfindung sehr rechen- und somit energieintensiv ist, wurden weitere Mechanismen entwickelt. Die populärste Alternative heisst Proof-of-Stake, PoS. Dieser Mechanismus wird bereits in gewissen Kryptowährungen wie EOS, Tezos und Tron eingesetzt, die bezüglich Marktkapitalisierung in den Top 20 liegen.

Dabei wird statt Rechenleistung das verfügbare Kapital als Kriterium

Innenansicht des Rechenzentrums der BTC KZ Crypto Mining Company bei der Stadt Ekibastus, Kasachstan, im November 2021.

Bitcoin-Mining in Kanada: Rechenzentrum in Medicine Hat, Provinz Alberta, im Jahr 2018.

Bilder: Reuters/Pavel Mikheyev/Curtis Huisman, Wikimedia Commons

genutzt. Miner braucht es da also nicht mehr. Ein Zufallszahlengenerator bestimmt, wer die nächste Validierung der Transaktionen durchführen darf. Je höher das Vermögen, desto höher ist die Wahrscheinlichkeit, dass jemand als Prüfer auserkoren wird. Wie bei Proof-of-Work erhalten die Prüfer bei der Veröffentlichung eines Blocks eine Blockbelohnung und eine Transaktionsvergütung. Für eine erfolgreiche Sybil-Attacke müsste ein Angreifer mehr als die Hälfte der Gesamtsumme einer Kryptowährung besitzen, um sich durchsetzen zu können. Dies ist äusserst unwahrscheinlich.

Energiehungrigste Anwendung

Aber wie steht es quantitativ um den Energieverbrauch von Blockchain? Dieser Frage ging eine vom Bundesamt für Energie in Auftrag gegebene Studie nach.[1] In der Studie wird der Energieverbrauch auf die drei grundsätzlichen ICT-Ursachen aufgeteilt: die Speicherung, die Kommunikation zwischen den Nodes sowie dem Rechnen, insbesondere des PoW.

Bezüglich Speicherung berücksichtigt die Studie die Replikation der gesamten Blockchain seit ihrer Einführung. Im Juni 2021 war beispielsweise die Bitcoin-Kette 350 GB gross. Sie wächst jährlich um rund 66 GB. Aktuell ist das gesamte Bitcoin-System auf rund 12 000 Nodes gespeichert, von denen die meisten permanent eingeschaltet sind. Berücksichtigt man den Mix an Hardware, auf der die Nodes laufen, ergibt sich laut der Studie ein Stromverbrauch für die Bitcoin-Speicherung, der im ungünstigsten Fall bei ca. 3,15 GWh jährlich liegt, aber wahrscheinlich deutlich geringer ist. Bei moderneren Blockchains wie Ethereum 2.0 kommen Shards zum Einsatz. Da muss nicht mehr die gesamte Blockchain auf jedem Node gespeichert werden, sondern nur ein bestimmtes Segment.

Auch die Kommunikation braucht Energie: Bei einer PoW-Blockchain muss der bestätigte neue Block an alle Nodes verschickt werden, was rund 0,11 kWh braucht. In einem Jahr verbraucht also Bitcoin für die Kommunikation weniger als 6 MWh, eine vernachlässigbare Energiemenge.

Es überrascht nicht, dass das für den PoW-Konsensmechanismus erforderliche Rechnen mit Abstand am meisten Energie erfordert. Ein hoher Energieverbrauch ist ja eine unerlässliche Komponente des Konzepts. Roger Wattenhofer, Professor für verteilte Computersysteme an der ETH Zürich, dessen Team die asynchrone Proof-of-Stake-Blockchain-Architektur Cascade [4] entwickelt hat, schätzt, dass PoW für rund 99,99 % des Blockchain-Energieverbrauchs verantwortlich ist. Die aktuelle Situation schildert er so: «Unter den Top-10-Kryptos gibt es nur noch wenige mit Proof-of-Work, da alle modernen Kryptowährungen Proof-of-Stake verwenden oder gleich ‘permissioned’ sind. Ausser Bitcoin wäre da noch Dogecoin mit PoW, und zurzeit noch Ethereum, das allerdings bald zu PoS wechselt. Bitcoin ist 30-mal grösser als Dogecoin, man kann also sagen, dass das Energieproblem beinahe ausschliesslich ein Bitcoinproblem ist.»

Wenn der Wert einer Kryptowährung steigt, wird das Problem noch verschärft, denn dann lohnt es sich, noch mehr Energie für das Schürfen aufzuwenden, solange die Stromkosten den erhofften finanziellen Gewinn nicht überschreiten. Obwohl immer effizientere Rechner für das Schürfen eingesetzt werden – zunächst wurden gewöhnliche PCs eingesetzt, dann leistungsfähigere Grafikkarten und seit 2013 ASIC-basierte Systeme – kann ihre Effizienzsteigerung nicht mit der Entwicklung des Energieverbrauchs Schritt halten.

Die BFE-Studie schätzt den aktuellen Stromverbrauch des PoW-Mechanismus im ungünstigsten Fall auf 30 GW, was einer jährlichen Energie von 263 TWh entspricht. Realistisch dürften 100–150 TWh jährlich sein. Zum Vergleich: Im Jahr 2020 betrug der gesamte Stromverbrauch der Schweiz 55,7 TWh. Andere Konsensmechanismen wie PoS sind um Grössenordnun-

RÉSUMÉ

De combien d’énergie les blockchains ont-elles besoin ?

Une étude et des développements

Les blockchains sont déjà utilisées pour les cryptomonnaies et, parallèlement, de nouvelles applications et de nouveaux domaines d’activité sont recherchés. Mais elles font plus souvent la une des journaux en raison de leur consommation d’énergie. Une étude commandée par l’Office fédéral de l’énergie s’est penchée sur la question de la consommation d’énergie des blockchains en termes quantitatifs. Dans cette étude, la consommation d’énergie est répartie entre les trois causes fondamentales : le stockage, la communication entre les nœuds et le calcul. C’est le calcul nécessaire à la preuve de travail (proof of work, PoW) qui nécessite le plus d’énergie, à savoir, selon l’étude, 263 TWh par an dans le cas le plus défavorable. Il est toutefois réaliste de tabler sur 100 à 150 TWh par an. Une consommation d’énergie élevée est en effet une composante indispensable du concept. Roger Wattenhofer, professeur à l’ETHZ, estime que la preuve de travail est responsable d’environ 99,99 % de la consommation d’énergie. Selon lui, parmi les dix cryptomonnaies les plus courantes, il n’y en a plus que quelques-unes qui utilisent la preuve de travail, car toutes les cryptomonnaies modernes utilisent la preuve d’enjeu (proof of stake, PoS) ou sont tout de suite « permissioned ». Le problème énergétique est donc presque exclusivement un problème du Bitcoin.

La manière la plus efficace de réduire drastiquement et durablement la consommation d’énergie des cryptomonnaies serait de migrer le mécanisme de consensus de la preuve de travail vers la preuve d’enjeu. Ce changement devrait avoir lieu début 2022 pour la deuxième plus grande cryptomonnaie, l’Ether, qui fonctionne sur le système Ethereum. Dans le cas du Bitcoin, ce changement est peu probable, notamment parce que dans ce système, les mineurs ne veulent pas perdre leurs investissements dans le hardware utilisé pour le minage. NO

gen sparsamer, da bei ihnen keine Kryptorätsel gelöst werden müssen und ihr Stromverbrauch weder mit der Netzwerkgrösse noch mit dem Wert der entsprechenden Kryptowährung wächst.

Standorte lösen sich ab

Dieser enorme Energieverbrauch bei PoW hat Auswirkungen: Nachdem China – damals das Land mit den meisten Bitcoin-Mining-Rechenzentren – den Handel mit Kryptowährungen verboten hat, zogen die Schürfer in Länder, die ihrem Anliegen wohlgesinnter sind. Eine der Begründungen der chinesischen Regierung für diese einschneidende Entscheidung war der immense Treibhausgas-Ausstoss der erforderlichen Stromerzeugung. Gemäss dem Cambridge Bitcoin Electricity Consumption Index führt seit dem 13. Oktober 2021 die USA mit einem Anteil von 35,4% die Rangliste an, gefolgt von Kazakhstan (18,1%) und Russland (11%).[5]

Kasachstan wurde also zum zweitgrössten Bitcoin-Produzenten weltweit, was bei einem Strompreis von rund 5 Rp. pro Kilowattstunde kaum überrascht. Mit dem Ergebnis, dass das nationale, hauptsächlich mit Kohlekraft betriebene Stromnetz an seinen Anschlag gekommen ist. Der Vize-Energieminister Murat Zhurebekov führte die Erhöhung des Verbrauchs um 8% im Jahr 2021 zwar auch auf den gestiegenen Haushaltsverbrauch zurück, aber die offiziell registrierten 50 Kryptowährungs-Schürfunternehmen, zusammen mit den nicht registrierten, im Graubereich operierenden Bitcoin-Firmen dürften die Hauptverantwortlichen für dieses Verbrauchswachstum sein.[6]

Wie weiter?

Die wohl effektivste Weise, um den Energieverbrauch von Kryptowährungen drastisch zu senken, wäre eine Migrierung des Konsensmechanismus von Proof-of-Work auf Proof-of-Stake. Da die Speicherung und die Kommunikation bei Kryptowährungen verglichen mit dem Mining vernachlässigbar sind, besteht in diesen Bereichen kaum Handlungsbedarf. Genau diese Umstellung wird nun durch die 2015 erschienene, zweitgrösste Kryptowährung Ether, die auf dem Ethereum-System läuft, angestrebt. Der Wechsel soll Anfang 2022 stattfinden.

Bezüglich Bitcoin, dem grössten Verbraucher, ist man hingegen pessimistisch. Roger Wattenhofer präzisiert: «Bei Bitcoin habe ich keine Hoffnungen. Die Bitcoin-Community streitet sich schon um Kleinigkeiten, ich würde einen (grossen) Wechsel auf Proof-of-Stake quasi ausschliessen.» Als Grund für diese negative Einschätzung gibt Wattenhofer die Macht der Miner bei Bitcoin an, die ihre Investitionen in Mining-Hardware nicht verlieren wollen.

Die Wahl einer Kryptowährung hat also einen enormen Einfluss auf den entsprechenden Blockchain-Energieverbrauch. Um dies ins Bewusstsein der Nutzer zu bringen, könnte man beispielsweise – analog zu Haushaltsgeräten – ein Blockchain-Energielabel für die Logos der Kryptowährungen einführen. Dann dürfte der Aufkleber «Bitcoin accepted here» mit einem grossen Z gekennzeichnet sein.

Referenzen

[1] Vlad Coroamă, Blockchain energy consumption – an exploratory study, BFE, 27. 9.2021.
[2] Oliver Schneider, «Warum das IoT tötet und wir für Google zahlen sollten», Bruce Schneier im Interview, Netzwoche, 11.2.2019.
[3] Radomír Novotný, «Mehr als nur Energieverrechnung», Bulletin SEV/VSE, 8/2021, S. 41.
[4] Jakub Sliwinski, Roger Wattenhofer, «Asynchronous Proof-of-Stake», Stabilization, Safety, and Security of Distributed Systems, Springer Verlag, 2021.
[5] Adela Suliman, «U.S. overtakes China to become world's largest bitcoin mining hub, report finds», Washington Post, 14. Oktober 2021.
[6] Paolo Sorbello, Kazakhstan's Power Shortages: Crypto Miners and Geopolitics, The Diplomat, 19. Nov. 2021.

Literatur

Bernhard Bircher-Suits und Felix Ertle, «Traum von der ‹grünen› Kryptowährung», NZZ, 13.8.2021.

Autor

Radomír Novotný ist Chefredaktor Electrosuisse.
→ Electrosuisse, 8320 Fehraltorf
→ radomir.novotny.electrosuisse.ch