

Energieverbrauch der Blockchainanwendung bei taXchain – der Plattform für Steuern und Zoll

----- Elena Rudyk – 2021 – Siemens -----

Wenn die Rede von der Blockchain-Technologie ist, denken die meisten sofort an Bitcoins und häufig an den damit verbundenen enormen Energieverbrauch¹. Dabei ist die Blockchain-Technologie alles andere als homogen, so dass pauschale Aussagen über ihren Energieverbrauch mit Vorsicht zu treffen sind. Der Artikel schafft Klarheit über den Energieverbrauch, speziell bei der von uns beabsichtigten Verwendung und zeigt, dass sie sogar naturschonend ist.

Die Blockchain-Technologie wurde durch ihre erste Anwendung, der Kryptowährung Bitcoin, 2009 bekannt. In den letzten zehn Jahren hat sich die Blockchain-Technologie erheblich weiterentwickelt und wird heute unterschiedlich eingesetzt, beispielsweise von Ethereum oder Hyperledger Fabric, die den Plattformen eine noch nie da gewesene Vielseitigkeit ermöglicht. Infolgedessen haben viele Forscher und Praktiker erkannt, dass die Blockchain-Technologie über ihre Verwendung in Kryptowährungen hinaus weitaus größeres Potenzial besitzt. Grundsätzlich ermöglicht die Blockchain-Technologie sichere Transaktionen und ist daher sowohl für Privatpersonen als auch für die Industrie und den öffentlichen Sektor interessant.

Da die Blockchain-Technologie immer noch von vielen mit Bitcoins in Zusammenhang gebracht und dieser nachgesagt wird, dass daraus ein hoher Energieverbrauch resultiert, gerät diese Technologie in Verruf hinsichtlich des Klimawandels und der Nachhaltigkeit². Doch was bedeutet ein hoher Energieverbrauch? Und besteht bei der Verwendung der Blockchain-Technologie bei der Anwendung von taXchain der gleiche Effekt?

¹ Sedlmeir, J./ Buhl, H. U. / Fridgen, G. / Keller, R. (2020): The Energy Consumption of Blockchain Technology: Beyond Myth;

<https://link.springer.com/article/10.1007%2Fs12599-020-00656-x>

² De Vries, A. (2018): Bitcoin's growing energy problem;

[https://www.cell.com/joule/fulltext/S25424351\(18\)301776?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435118301776%3Fshowall%3Dtrue](https://www.cell.com/joule/fulltext/S25424351(18)301776?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435118301776%3Fshowall%3Dtrue)

Physikalisch erfolgt der eigentliche Energieverbrauch durch die Umwandlung von Strom in Wärme. Damit wird Strom in (weniger wertvolle) Energie in Form von Wärme umgewandelt³.

Aus der technologischen Sicht gestaltet sich die Antwort etwas komplizierter. Um dies herauszufinden, müsste man zuerst verstehen, wie Blockchain funktioniert.

Blockchain

Blockchain bietet eine neue Möglichkeit, Transaktionen durchzuführen und aufzuzeichnen, wie z. B. das Versenden von Geld. Bei einer traditionellen Börse verifizieren und protokollieren zentrale Verwaltungen (z. B. Banken) mit Hilfe von Konten die Transaktionen. Blockchain macht eine zentrale Verwaltung sowie die Konten überflüssig. Stattdessen wird das Konto (Ledger) in einem verteilten Netzwerk von Computern, auf denen eine bestimmte Blockchain-Software läuft, gehalten, gemeinsam genutzt und validiert⁴.

Das Fehlen einer zentralen, vertrauenswürdigen Verwaltung bedeutet, dass Blockchain unter anderem einen "**Konsensmechanismus**" benötigt, um eine Einigung auf einen gemeinsamen Status zu erzielen, mit anderen Worten einen gemeinsamen Konsens. Weitere Aspekte, die zur Sicherheit in der Blockchain beitragen, sind beispielsweise Zertifikate. Im Fall von Bitcoin wird der Konsens durch eine Methode namens "Proof-of-Work" (PoW) erreicht, bei der Computer im Netzwerk - "Miner" - miteinander konkurrieren, um ein komplexes mathematisches Rätsel zu lösen. Jede Vermutung, die ein Miner zur Lösung des Rätsels anstellt, wird als "Hash" bezeichnet, während die Anzahl der Vermutungen, die der Miner pro Sekunde anstellt, als "Hashrate" bekannt ist. Sobald das Rätsel gelöst ist, wird der neueste "Block" von Transaktionen genehmigt und der "Kette" von Transaktionen hinzugefügt. Der erste Miner, der das Rätsel löst, wird mit neuen Bitcoins und Netzwerk-Transaktionsgebühren belohnt. Der Energieverbrauch des Bitcoin-Netzwerks ist daher sowohl ein Sicherheitsmerkmal als auch ein Nebeneffekt der ständig weiteransteigenden Rechenleistung der konkurrierenden Miner, um Transaktionen durch PoW zu validieren.

³ Truby, J. (2018): Decarbonizing bitcoin: law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies;
<https://www.sciencedirect.com/science/article/abs/pii/S2214629618301750?via%3Dihub>

⁴ Kamiya, G. (2019): Bitcoin energy use - mined the gap;
<https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap>

PoW Blockchain und ihr Energieverbrauch

Unter PoW versteht man das Recht, einen neuen Block aus einer Teilmenge der in der Warteschlange befindlichen Transaktionen zu erzeugen, wenn man eine Lösung für ein kryptographisches, rechenintensives Rätsel findet. Der Prozess der Suche nach einer Lösung wird "Mining" genannt. Dies führt zu einer Kopplung des Stimmgewichts an eine knappe Ressource - Rechenleistung und damit Energie - und verhindert somit Sybil-Angriffe. Der Mining-Prozess wird ökonomisch incentiviert, indem die Teilnehmer für jeden gefundenen und verbreiteten gültigen Block belohnt werden. Die Belohnung besteht typischerweise aus einer bestimmten Menge der zugehörigen Kryptowährung und den Gebühren für die damit verbundenen Transaktionen. Der Wert der ersteren ist proportional zum Marktpreis der Kryptowährung, so dass der Erfolg der Kryptowährungen auf den Finanzmärkten in den letzten Jahren einen sehr starken Anreiz zur Teilnahme am Mining geschaffen hat. Dies wiederum hat zu einem enormen Energieverbrauch geführt, der mit den zugrunde liegenden PoW-Blockchains verbunden ist.

Es ist wichtig festzuhalten, dass der hohe Energieverbrauch von PoW-Blockchains weder das Ergebnis von ineffizienten Algorithmen noch von veralteter Hardware ist, sondern durch ihr "energieintensives Design" zustande kommt. Durch diesen hohen Energieverbrauch werden die PoW-Blockchains vor Angriffen geschützt: Je nach Szenario muss ein Angreifer mindestens 50 % der gesamten Rechenleistung, die die teilnehmenden Miner für das Mining aufwenden - und damit den gleichen Anteil am Gesamtenergieverbrauch (unter der Annahme gleicher Hardware) - aufbringen, um das System erfolgreich manipulieren oder kontrollieren zu können⁵. So ist eine PoW-Kryptowährung umso besser gegen Angriffe geschützt, je wertvoller sie und je aufwendiger das Design ist.

Somit entsteht ein Teil des Energieverbrauchs durch das Mining, also das Lösen der kryptografischen Rätsel. Der weitaus geringere Teil des Energieverbrauchs wird durch andere Aufgaben hervorgerufen, die auf den teilnehmenden Knoten durchgeführt werden, also hauptsächlich die Validierung neuer Blöcke und die entsprechende Aktualisierung ihrer

⁵ Sedlmeir, J./ Buhl, H. U. / Fridgen, G. / Keller, R. (2020): The Energy Consumption of Blockchain Technology: Beyond Myth;
<https://link.springer.com/article/10.1007%2Fs12599-020-00656-x>

lokalen Datenbanken. Ein weiterer Teil des Energieverbrauchs ist mit der Wartung der Knoten verbunden ist⁶. Wie hoch dieser tatsächlich ist, was in der Literatur aktuell noch umstritten ist, ist in unserem Fall unbedeutend. Wie hoch der tatsächliche Energieverbrauch ist, wird vor allem durch die Parameter "durchschnittliche Blockzeit", "Mindestgröße der Transaktionen" und "maximale Blockgröße" bestimmt⁷. So benötigt eine einzige Transaktion derzeit genug elektrische Energie, um den Bedarf eines durchschnittlich großen deutschen Haushalts für Wochen oder sogar Monate zu decken. Allerdings gibt es alternative Konsensmechanismen, deren Energieverbrauch im Vergleich zu PoW-Blockchains um Größenordnungen geringer ist, da sie durch ihr Design keine Energieintensität aufweisen⁸. Darüber hinaus unterscheidet man zwischen einer privaten und öffentlichen Blockchain.

Öffentliche Blockchain

Ein öffentliches Blockchain-Netzwerk ist ein Blockchain-Netzwerk, dem jeder jederzeit beitreten kann. Es gibt also keine Einschränkungen hinsichtlich einer Teilnahme. Darüber hinaus kann sogar jeder das Ledger sehen und am Konsensprozess teilnehmen⁹. Ethereum ist zum Beispiel eines der Beispiele für eine öffentliche Blockchain-Plattform. Die ausschlaggebende Eigenschaft der öffentlichen Blockchain-Unternehmen ist, dass sie sicherstellen, dass alle Teilnehmer die gleichen Rechte haben. Wenn also Bedarf an einem vollständig dezentralisierten Netzwerksystem besteht, ist die öffentliche Blockchain die richtige Lösung, zumal das Ledger auch jeder sehen kann, so dass die Transparenz zu jeder Zeit erhalten bleibt. Das bedeutet, dass öffentliche Blockchains, wie z. B. Bitcoin, den Teilnehmern folgende drei Aktionen erlauben, sofern sie über genügend Rechenleistung verfügen:

⁶ De Vries, A. (2018) Bitcoin's growing energy problem; [https://www.cell.com/joule/fulltext/S25424351\(18\)301776?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435118301776%3Fshowall%3Dtrue](https://www.cell.com/joule/fulltext/S25424351(18)301776?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435118301776%3Fshowall%3Dtrue)

⁷ Georgiadis, E. (2019) How many transactions per second can bitcoin really handle? Theoretically. <https://eprint.iacr.org/2019/416>. Accessed 05 Feb 2020

⁸ Sedlmeir, J./ Buhl, H. U. / Fridgen, G. / Keller, R. (2020): The Energy Consumption of Blockchain Technology: Beyond Myth; <https://link.springer.com/article/10.1007%2Fs12599-020-00656-x>

⁹ Iredale, G. (2021): Public Vs Private Blockchain: How Do They Differ?; <https://101blockchains.com/public-vs-private-blockchain>

Integrität - wer Transaktionen validiert und Governance-Entscheidungen im Netzwerk trifft; Lesezugriff - wer oder welche Geräte können Transaktionen im Netzwerk sehen; und Schreibzugriff - wer oder welche Geräte können Transaktionen an das Netzwerk übermitteln. Reine private Blockchains, wie Hyperledger, beschränken den Zugang in allen drei Szenarien auf eine definierte Gruppe von Teilnehmern¹⁰ und damit genau das, was auch taXchain ausmacht und benötigt. Hierfür greift man in den meisten Fällen auf Proof-of-Authority¹¹, um von dem „Validator“ die Erlaubnis zu erhalten, Transaktionen auszuführen.

Private Blockchain und PoA

Eine private Blockchain ist eine spezielle Art der Blockchain-Technologie, bei der ein Verbund (z.B. an mehreren Organisationen, bzw. Unternehmen oder Partnern) die Kontrolle über das Netzwerk hat¹². Es bedeutet also, dass es nicht für die Öffentlichkeit zugänglich ist.

Grundsätzlich benötigen alle privaten Blockchain-Lösungen eine Autorisierung, um sich beim Betreten der Plattform zu identifizieren. Deshalb werden private Blockchain-Lösungen für Kanäle („Channels“) mit mehreren Partnern zusammen entwickelt, die man nur autorisiert betreten können soll. Folglich gibt es bei privaten Blockchain-Plattformen Regeln, die andere Plattformen nicht haben. Alle Knotenpunkte müssen sich an entsprechende Regeln halten, um den ordnungsgemäßen Ablauf zu gewährleisten.

Schlussfolgerung für die taXchain-Blockchain

Der Unterschied der beiden Mechanismen zeigt also, dass bei der PoA das Anfügen eines neuen Blocks, der aufgrund seiner Größe sowie der Transaktionsmenge, im Gegensatz zum entsprechenden Vorgang bei einer PoW, einen geringen Stromverbrauch erzeugt. Bei der privaten Blockchain „taXchain“, firmenübergreifenden Plattform für Steuer- und Zollprozesse,

¹⁰ Morris, J./ Hartnett, S. (2019): The argument for public blockchains in the energy sector; <https://www.greenbiz.com/article/argument-public-blockchains-energy-sector>

¹¹ Eine Alternative wäre beispielsweise Proof of Network

¹² Vgl. auch https://hyperledger-fabric.readthedocs.io/en/release-2.2/channel_update_tutorial.html

handelt es sich also nicht um das energiefressende Konsenskonstrukt, wie bei den öffentlichen Blockchains.

Nicht nur durch ihren geringen Energieverbrauch, ist die Anwendung der Blockchain-Technologie von taXchain naturschonend: die Dokumente sollen nämlich nunmehr digital und nicht papierbasiert ausgetauscht werden.

Alphabetisches Quellenverzeichnis

De Vries, Alex (2018:) Bitcoin's growing energy problem;
[https://www.cell.com/joule/fulltext/S25424351\(18\)301776?returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435118301776%3Fshowall%3Dtrue](https://www.cell.com/joule/fulltext/S25424351(18)301776?returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435118301776%3Fshowall%3Dtrue)

Georgiadis, Evangelos (2019): How many transactions per second can bitcoin really handle? Theoretically.
<https://www.semanticscholar.org/paper/How-many-transactions-per-second-can-bitcoin-really-Georgiadis/cd19b9bd1c726df7c6e9d14d9bcfd5104b599a96>

Iredale, Gwyneth (2021): Public Vs Private Blockchain: How Do They Differ?;
<https://101blockchains.com/public-vs-private-blockchain>

Kamiya, George (2019): Bitcoin energy use - mined the gap;
<https://www.iea.org/commentaries/bitcoin-energy-use-mined-the-gap>

Morris, Jesse/ Hartnett, Sam (2019): The argument for public blockchains in the energy sector;
<https://www.greenbiz.com/article/argument-public-blockchains-energy-sector>

Sedlmeir, Johannes/ Buhl, Hans Ulrich / Fridgen, Gilbert / Keller, Robert (2020): The Energy Consumption of Blockchain Technology: Beyond Myth;
<https://link.springer.com/article/10.1007%2Fs12599-020-00656-x>

Truby, Jon (2018): Decarbonizing bitcoin: law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies;
<https://www.sciencedirect.com/science/article/abs/pii/S2214629618301750?via%3Dihub>