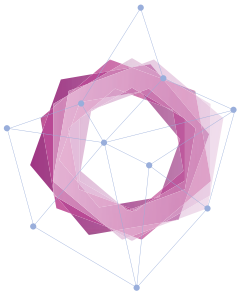
dena
Deutsche Energie-Agentur



Future Energy
Lab

Blockchains und ihren Stromverbrauch neu denken

Ein Leitfaden für das stromsparende Design dezentraler Dateninfrastrukturen – Kurzfassung

Impressum

Herausgeber
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin

Tel.: +49 (0)30 66 777-0
Fax: +49 (0)30 66 777-699

E-Mail: info@dena.de

Internet:
dena.de
future-energy-lab.de

Autoren:
Philipp Richard, dena
Moritz Schlösser (Projektleiter), dena
Hendrik Zimmermann, dena

Vincent Gramlich, Fraunhofer FIT
Felix Paetzold, Fraunhofer FIT
Prof. Dr. Jens Strüker, Universität Bayreuth & Fraunhofer FIT

Konzeption und Design:
die wegmeister gmbh

Letzte Aktualisierung:
September 2023

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2023) „Blockchains und ihren Stromverbrauch neu denken – Ein Leitfaden für das stromsparende Design dezentraler Dateninfrastrukturen – Kurzfassung“

Bundesministerium
für Wirtschaft
und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

Vorwort

Eines ist gewiss: Die Blockchain-Technologie ist eine der am meisten gehypten Technologien des letzten Jahrzehnts. Dabei wurde von einer digitalen Revolution, von einem globalen Phänomen gesprochen, das das Zusammenleben der Menschen verändern wird. An Blockchains wurde die Erwartung gestellt, dass sie im Internet die Machtkonzentration bei großen Konzernen auflösen, Daten zurück in das Eigentum von Individuen bringen und damit in Form des Web 3.0 das Internet reparieren könnten. Doch nicht nur das: Kryptowährungen sollten eine Alternative zu klassischen Währungen darstellen, die nicht von zentralen Institutionen wie (Zentral-)Banken oder Regierungen kontrolliert wird. Es wurde die Hoffnung geweckt, Millionen von Menschen, die in Entwicklungsländern oder autokratisch geführten Staaten leben, den Zugang zu einem fairen und zensurresistenten Finanznetzwerk zu verschaffen.

Doch wie ist die Situation heute? Blockchains finden in der Digitalstrategie der Bundesregierung keine Erwähnung mehr, das Vertrauen in Kryptowährungen ist nach dem Zusammenbruch der Kryptowährungsbörse FTX im November 2022 schwer beschädigt und die Kritik an der wirtschaftlichen und sozialen, vor allem aber an der ökologischen Nachhaltigkeit der Technologie wird immer lauter.

Insbesondere der Proof-of-Work-Mechanismus beim Hinzufügen neuer Blöcke verbraucht große Mengen an Strom und Hardware. Kritiker sehen in der Technologie keinen wirklichen Nutzen, der den Aufwand an Ressourcen rechtfertigt. Kryptowährungen gelten als zu volatil, um als echtes Zahlungsmittel verwendet zu werden, und dienen in den Augen der Kritiker lediglich als Spekulationsobjekte. Dem Web 3.0 wird sogar ein „dystopisches Potenzial“ in Bezug auf das Eigentum an persönlichen Daten und ihrer Monetarisierung zugeschrieben.[1] Angeblich ist die Blockchain für andere Anwendungen ungeeignet, weil beispielsweise eine ihrer Kerneigenschaften, die Unveränderlichkeit, gegen das „Recht auf Vergessenwerden“, einen wesentlichen Aspekt der Datenschutz-Grundverordnung (DSGVO), und damit gegen die Regeln der realen Welt verstößt.

Gemäß der Theorie der technologischen Entwicklung nach dem Gartner Hype Cycle[2] hat die Blockchain-Technologie inzwischen den „Gipfel der überzogenen Erwartungen“ überschritten und ist im „Tal der Enttäuschungen“ angekommen. Aber wie sieht die Zukunft aus? Um diese Frage zu beantworten und herauszuarbeiten, wofür die Blockchain-Technologie in der nächsten Phase des Hype Cycle, dem „Pfad der Erleuchtung“, genutzt werden kann, ist eine nüchterne wissenschaftliche Betrachtung der Vorteile und des Stromverbrauchs von Blockchains erforderlich. Wir hoffen, dass dies zu einer Versachlichung der mitunter hitzigen Debatten zwischen Befürwortern und Gegnern der Technologie beitragen wird und zu bestimmen hilft, welches Niveau das „Plateau der Produktivität“ letztendlich annehmen wird.[3]

Die vorliegende Studie konzentriert sich auf eines dieser Themen und liefert eine neue, wertvolle Grundlage für die Diskussionen rund um den Stromverbrauch von Blockchains. Diese Studie enthält einen Leitfaden, der es erleichtert, Blockchains möglichst energiesparsam und entsprechend den Anforderungen bestimmter Anwendungsfälle zu gestalten. Unsere Ergebnisse können als Grundlage dienen, um die Auswirkungen einer Blockchain auf Klima und Umwelt sowie ihre weiteren Eigenschaften wie Leistung und IT-Sicherheit mit denen alternativer Netzwerklösungen zu vergleichen, damit eine fundierte Entscheidung über die zu verwendende Technologie getroffen werden kann.

1 Dr. Malte Engeler (2022): Deutscher Bundestag, Anhörung zum Thema „Web 3.0 und Metaverse“, https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/921548-921548 (Zeitstempel: 14:24–14:30 Uhr).

2 https://www.gartner.com/en/research/methodologies/gartner-hype-cycle, letzter Zugriff am 7. August 2023.

3 https://www.gartner.com/en/research/methodologies/gartner-hype-cycle, letzter Zugriff am 7. August 2023.

Der Leitfaden zum stromsparenden Design von Blockchains ist das Ergebnis einer intensiven Zusammenarbeit mit den Mitarbeiterinnen und Mitarbeitern des Fraunhofer-Instituts für Angewandte Informationstechnik (FIT), für die wir an dieser Stelle unseren Dank aussprechen. Unser Dank gilt auch dem Bundesministerium für Wirtschaft und Klimaschutz, das diese Studie finanziert hat.

Wir sind davon überzeugt, dass der Einsatz digitaler Technologien für den Erfolg der derzeit stattfindenden Energiewende, aber auch für den Wandel in anderen Sektoren als der Energiewirtschaft von wesentlicher Bedeutung ist. Wir plädieren jedoch dafür, den Stromverbrauch der digitalen Technologien zu minimieren. Die vorliegende Publikation soll daher zu einer kritischen Auseinandersetzung mit Blockchains und alternativen Netzwerkarchitekturen hinsichtlich ihrer Auswirkungen auf Klima, Umwelt und Menschen auf der Basis wissenschaftlicher Kriterien anregen. Nur so lässt sich der Nutzen der Digitalisierung gegen ihre ökologischen und sozialen Kosten abwägen.

Philipp Richard
Bereichsleiter Digitale Technologien & Start-up-Ökosystem

Moritz Schlösser
Experte Digitale Technologien

Blockchains und ihren Stromverbrauch neu denken

Die Digitalisierung ist einer der bedeutendsten Umbrüche unserer Zeit – in technologischer, sozialer, wirtschaftlicher und politischer Hinsicht. Dieser Megatrend hat weitreichende Auswirkungen auf alle Lebensbereiche. Digitale Technologien sind heute für die überwiegende Mehrheit unserer Wirtschaftszweige sowie für unser Zusammenleben in einer globalen Gemeinschaft unverzichtbar. Sie sind ein völlig neues Instrument zur Lösung sowohl neuer als auch seit langer Zeit bestehender Herausforderungen. Sie haben jedoch nicht nur eine soziale, sondern auch eine ökologische Kehrseite, da der Energieverbrauch aufgrund wachsender Anforderungen an die zugrunde liegende Dateninfrastruktur steigt. Darüber hinaus ist die digitale Wirtschaft durch Zentralisierung und Machtanhäufung gekennzeichnet, was eine Gefahr für offene Märkte und demokratische Systeme darstellen kann.

Verheißungen und Nachteile der Blockchain-Technologie

Die Blockchain-Technologie wird oft als Mittel gegen die zunehmende Konzentration der Macht über das Internet auf wenige Akteure angeführt. Blockchains sind so konzipiert, dass sie eine dezentrale, manipulationssichere und transparente Möglichkeit zur Speicherung und zum Austausch von Daten bieten. Diese Technologie stellt eine Alternative zur zentralen Kontrolle von Daten bereit, sei es im Finanzsektor, in der Technologiebranche oder in anderen Bereichen, in denen Daten ein wichtiges Gut sind. Da sie die Kontrolle über das Netzwerk verteilt, vermeidet die Blockchain-Technologie Datensilos und Single Points of Failure und erhöht so die Sicherheit und Verfügbarkeit der Daten sowie die Netzwerkzuverlässigkeit im Vergleich zu herkömmlichen Dateninfrastrukturen.

Die Blockchain-Technologie ist jedoch wegen ihres hohen Energieverbrauchs stark in die Kritik geraten. So ist beispielsweise Bitcoin, das bekannteste Blockchain-Netzwerk, zu einem der größten Energieverbraucher der Welt geworden und verbraucht eine Energiemenge, die etwa 36 Prozent des in Deutschland genutzten Stroms entspricht. Dadurch wurde die Nachhaltigkeit der Blockchain-Technologie infrage gestellt. Es ist wichtig, zu wissen, dass dieser hohe Energieverbrauch ein Merkmal des von Bitcoin verwendeten PoW-Konsensmechanismus (Proof of Work) ist, der Vertrauen in dezentrale Transaktionen erzeugt, indem er eine erhebliche Investition, und zwar in Form von Strom, erfordert. Es gibt jedoch energieeffiziente Alternativen zum PoW-Konsensmechanismus, zum Beispiel Proof of Stake (PoS). Die Smart-Contract-Plattform Ethereum stellte im September 2022 ihren Konsensmechanismus von PoW auf diesen alternativen Konsensmechanismus um, ein Upgrade, das auch als „Ethereum-Merge“ bezeichnet wird. Infolgedessen wurde der Stromverbrauch des Netzwerks um 99,998 Prozent gesenkt und somit bewiesen, dass extremer Stromverbrauch kein inhärentes Merkmal der Blockchain-Technologie ist.[4] Das bedeutet, dass der Stromverbrauch durch gezieltes Netzwerkdesign gesenkt werden kann.

Literaturlücken schließen

Trotz der Vorteile dieser Entwicklungen gibt es noch Lücken im Hinblick auf die Nutzung von Werkzeugen zur Senkung des Stromverbrauchs. Die vorhandene Literatur im akademischen und Anwendungsbereich bietet einige Anhaltspunkte dafür, wie der Stromverbrauch eines Blockchain-Netzwerks möglichst gering gehalten werden kann, konzentriert sich jedoch hauptsächlich auf die Entscheidung zwischen PoW und alternativen Blockchains. Andere Designoptionen, die sich auf den Stromverbrauch eines Netzwerks auswirken können, werden nicht berücksichtigt. Zudem liefert die Literatur nicht die erforderlichen Instrumente, um den Anwendungsfall zu analysieren, für den die Infrastruktur genutzt werden soll.

Durch unsere Studie werden diese Lücken in der Literatur geschlossen. Sie liefert zunächst die Anforderungen eines Anwendungsfalls an seine Architektur, einschließlich der Reduzierung des Stromverbrauchs. Auf der Grundlage der Anforderungen werden eine Reihe von Leitfragen, um diese Anforderungen abzuleiten, und ein Gestaltungsleitfaden für ein energieeffizientes Blockchain-Netzwerk, das die Anforderungen eines gegebenen Anwendungsfalls erfüllt, zur Verfügung gestellt.

Bestimmen der Anforderungen an die Dateninfrastruktur des Anwendungsfalls

Am Anfang der Studie werden die Datenanforderungen des Anwendungsfalls abgeleitet. Daraus ergeben sich fünf wesentliche Anforderungen an die Infrastruktur und sie definieren die Eigenschaften, die eine Infrastruktur mindestens aufweisen muss, um für einen Anwendungsfall geeignet zu sein. Erstens muss sie ein Maß an Vertraulichkeit bieten, das den speziellen Anforderungen des Nutzers entspricht und den Schutz vor unbefugtem Datenzugriff gewährleistet. Zweitens muss die Infrastruktur ein bestimmtes Maß an Integrität bewahren, um eine unbefugte Änderung oder Löschung von Daten zu verhindern. Drittens muss sie ein definiertes Maß an Datenverfügbarkeit gewährleisten, um die Zuverlässigkeit der Systeme und den Zugriff auf sie sicherzustellen. Viertens sollte die Infrastruktur die erforderliche Leistung bieten, um eine effiziente und zeitnahe Bereitstellung und Verarbeitung der Daten und somit einen reibungslosen Betrieb des Anwendungsfalls sicherzustellen. Schließlich sollte die Infrastruktur so konzipiert sein, dass sie die Umwelt so wenig wie möglich belastet. Im Hinblick darauf konzentriert sich diese

4 Crypto Carbon Ratings Institute (2022): The Merge: Implications on the Electricity Consumption and Carbon Footprint of the Ethereum Network.

Studie auf die Reduzierung des Stromverbrauchs. Dies sind die Mindestanforderungen. Es kann jedoch von Nutzen sein, sie zu übertreffen, indem beispielsweise ein höheres Maß an Integrität geboten wird, als für den Anwendungsfall erforderlich ist, sofern alle anderen Anforderungen erfüllt sind.

Die Dateninfrastruktur ist verantwortlich für ein bestimmtes Maß an ...

Abbildung 1: Die fünf Anforderungen an die Dateninfrastruktur

Leitfaden für die Gestaltung eines stromsparenden Netzwerks

Der Leitfaden ist in zwei Phasen unterteilt: In der ersten Phase wird der Use Case gründlich analysiert, für den die Dateninfrastruktur genutzt werden soll, und in der zweiten Phase wird das Netzwerkdesign behandelt:

- In Phase 1 erfolgt eine detaillierte Analyse des Use Case, für den die Dateninfrastruktur genutzt werden soll. Wir unterstützen diesen Prozess mit Fragen, die auf die grundlegenden Anforderungen und Randbedingungen eines Anwendungsfalls hinsichtlich seiner Dateninfrastruktur in einer Blockchain-basierten Lösung zugeschnitten sind.

- In Phase 2 wird das Netzwerkdesign behandelt, und zwar im Hinblick auf ein Permissioned-Blockchain-Netzwerk. Der mehrstufige Prozess umfasst die Überprüfung der Eignung eines Blockchain-Netzwerks für den Use Case, die Auswahl des geeigneten Blockchain-Typs und der zugehörigen Plattform sowie schließlich das Entwerfen des Permissioned-Netzwerks. Die zuvor festgelegten Anforderungen und Einschränkungen helfen bei der Bewertung verschiedener Designoptionen, erleichtern das Verständnis ihres Einflusses auf die Eigenschaften und stellen sicher, dass das endgültige Design eine geeignete Dateninfrastruktur für den Anwendungsfall bietet.

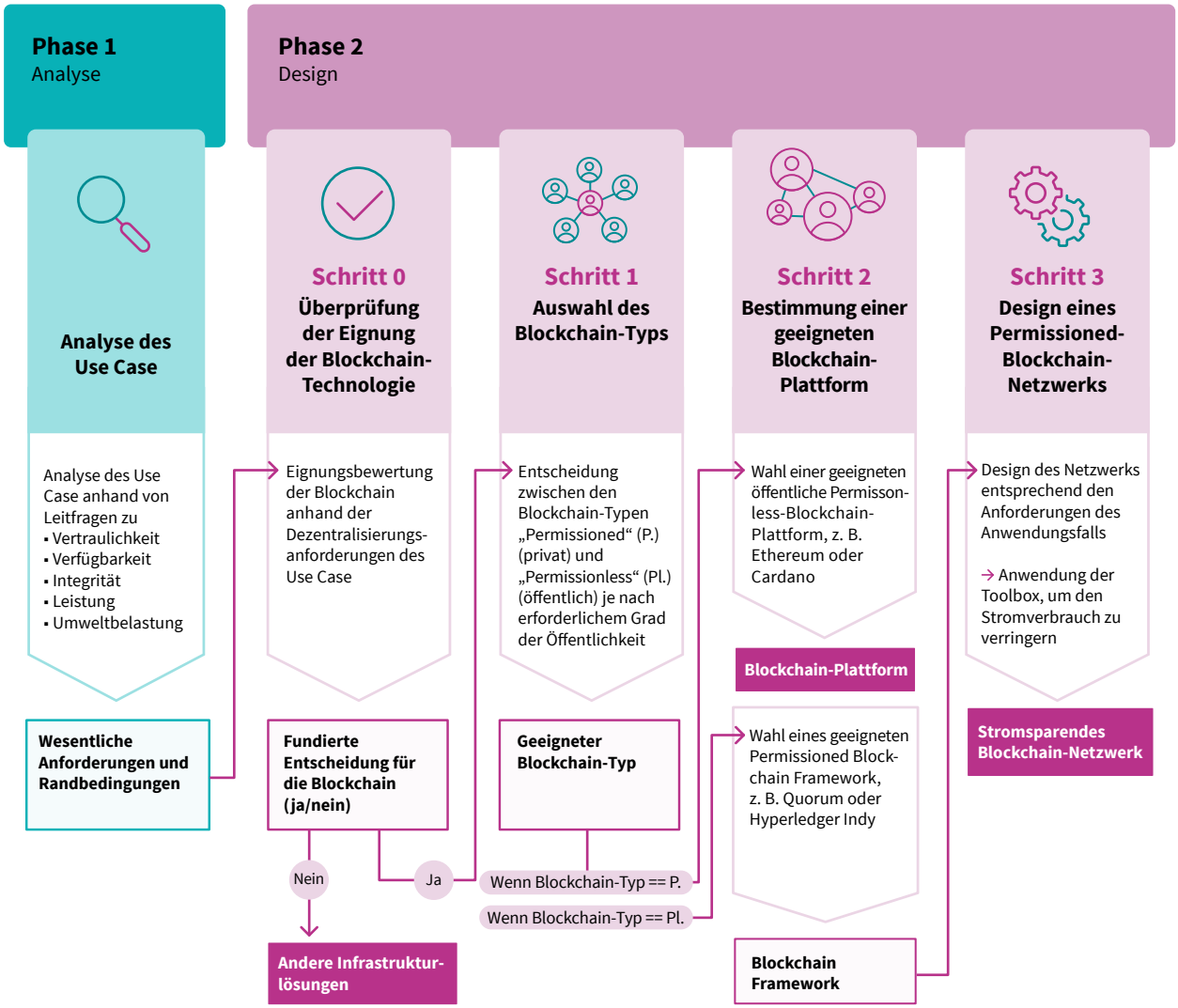


Abbildung 2: Die zwei Phasen beim Entwerfen eines Blockchain-Netzwerks

Phase 1: Analyse

In der ersten Phase werden die Anforderungen an die Dateninfrastruktur für den Anwendungsfall definiert. Diese Anforderungen müssen unter zwei Gesichtspunkten bestimmt werden: Erstens werden die grundlegenden Anforderungen eines Anwendungsfalls untersucht, zum Beispiel der erwartete Durchsatz an Transaktionen und die erforderliche Verfügbarkeit des Systems. Dadurch sollen die Merkmale bestimmt werden, die das endgültige Netzwerkdesign bieten muss. Zweitens werden die Beschränkungen der verfügbaren Designoptionen bestimmt, indem nicht praktikable oder ungeeignete Designs ausgeschlossen werden. So können beispielsweise durch die Anzahl der kooperierenden Organisationen die maximale Anzahl an Nodes und somit die Größe des Netzwerks begrenzt werden. Weitere Informationen zum Analysieren des Anwendungsfalls und zu den Leitfragen zur Unterstützung der Analyse finden Sie in Kapitel 4.3 der Langfassung.

Phase 2: Design

Schritt 0: Überprüfung der Eignung der Blockchain-Technologie

Bevor mit dem Design eines Blockchain-Netzwerks begonnen wird, muss die Eignung der jeweiligen Blockchain-Technologie für den Anwendungsfall sichergestellt werden, indem die Vor- und Nachteile der Dezentralisierung im Vergleich zu einer zentralen Infrastruktur erwogen werden. Die Dezentralisierung bietet zwar Vorteile wie höhere Transparenz, Unveränderlichkeit und Vertrauen, verursacht aber auch höhere Komplexität und betriebliche Herausforderungen, zum Beispiel einen höheren Stromverbrauch, da der Betrieb der Dateninfrastruktur auf mehrere Nodes verteilt ist.

Schritt 1: Auswahl des Blockchain-Typs

In der nächsten Phase wird festgelegt, welcher Blockchain-Typ – Permissioned oder Permissionless – für den jeweiligen Anwendungsfall am besten geeignet ist. Hier bietet das von Hunhevicz und Hall[5] entwickelte Modell einen wertvollen Ansatzpunkt. Dabei geht es in erster Linie um die Frage, ob alle Teilnehmer bekannt sind, und um den erforderlichen Grad an Überprüfbarkeit,

5 Hunhevicz JJ, Hall DM (2020): Do you need a blockchain in construction? Use case categories and decision framework for DLT design options. Advanced Engineering Informatics 45:101094. doi:10.1016/j.aei.2020.101094.

insbesondere durch öffentliche Transparenz aller Transaktionen. Außerdem wird das von Belotti et al.[6] vorgeschlagene Entscheidungsmodell hervorgehoben, bei dem auch die Abwägungen zwischen den verschiedenen Eigenschaften eines Blockchain-Netzwerks berücksichtigt werden.

Schritt 2: Bestimmung eines geeigneten Blockchain Framework

Wenn ein öffentliches Permissionless-Blockchain-Netzwerk erwogen wird, müssen die geänderten Rahmenbedingungen von PoW-Netzwerken (Proof of Work) beachtet werden. Durch den Wechsel von Ethereum von PoW zu Proof of Stake (PoS) wurde die Bedeutung von PoW-Netzwerken für den Datenaustausch zwischen Organisationen infrage gestellt. Da der Stromverbrauch von PoW-Netzwerken für den Konsensmechanismus immens ist, stellen sie ein Hindernis für die Minimierung der Umweltbelastung dar. PoS-Netzwerke, die Smart Contracts unterstützen, sind eine sinnvollere Wahl für öffentliche Netzwerke. Für fundierte Entscheidungen zum Blockchain-Typ ist die Kenntnis der relevanten Literatur und der aktuellen Entwicklungen erforderlich, zum Beispiel Studien von Gräbe et al.[7], Kubler et al.[8] und der dena[9].

Wenn die Wahl auf ein Permissionless-Blockchain-Netzwerk fällt, wird im nächsten Schritt das am besten geeignete Netzwerk ermittelt. Es sollten vorhandene Netzwerke mit der erforderlichen Sicherheit und Vertrauenswürdigkeit verwendet werden. Eine Übersicht über die relevanten Faktoren und Plattformen ist bei Gräbe et al.[10], Kubler et al.[11] und der dena[12] zu finden. Für Permissioned-Blockchain-Netzwerke empfehlen wir, eine Plattform, die den speziellen Anforderungen des Anwendungsfalls entspricht, auszuwählen. Dabei ist zu beachten, dass Permissioned-Blockchain-Netzwerke ein den Anforderungen des Anwendungsfalls entsprechendes, stromsparendes Design ermöglichen. Für diesen Blockchain-Typ stehen mehrere Frameworks zur Verfügung, beispielsweise Quorum, Hyperledger und Corda, die besondere Merkmale und Funktionen bieten und jeweils eigene Vor- und Nachteile haben.[13]

Schritt 3: Entwerfen eines Permissioned-Blockchain-Netzwerks

Das Entwerfen eines Permissioned-Blockchain-Netzwerks ist ein wichtiger Schritt beim Erstellen eines Netzwerks, das die speziellen Anforderungen des Anwendungsfalls erfüllt. In dieser Phase müssen durchdachte Designentscheidungen getroffen werden, um sicherzustellen, dass das Netzwerk die gewünschten Eigenschaften aufweist:

- Ein wichtiger Aspekt beim Entwerfen eines Netzwerks ist das Sicherstellen einer angemessenen **Vertraulichkeit der Daten**. Da Blockchains von Natur aus transparent sind, ist das Herstellen von Vertraulichkeit eine komplexe Herausforderung. Diese Herausforderung lässt sich mithilfe von Designoptionen bewältigen, die durch die Verwendung eines Permissioned-Blockchain-Netzwerks den Datenzugriff auf autorisierte Teilnehmer beschränken, Funktionen privater Kanäle in Permissioned-Blockchain-Netzwerken nutzen oder Techniken wie Datenverschlüsselung oder Zero-Knowledge Proofs einsetzen, um Daten zu verschleiern und gleichzeitig ihre Vertraulichkeit zu wahren.

- Die Wahrung der **Datenintegrität** erfordert einen geeigneten Konsensmechanismus, der auf die Netzwerkteilnehmer und die Sicherheitsanforderungen zugeschnitten ist. In Permissioned Blockchains werden häufig auf Proof-of-Authority (PoA) basierende Konsensmechanismen verwendet, da die Teilnehmer bekannt sind und somit keine Sybil-Resistance erforderlich ist. Die Flexibilität des PoA-Mechanismus ermöglicht Designs wie die Zuweisung von Stimmrechten an hochgradig vertrauenswürdige Teilnehmer oder ein Gleichgewicht zwischen Crash Fault Tolerance und Byzantine Fault Tolerance.

- Ein sorgfältiges Design der Netzwerkwerkstruktur gewährleistet die **Verfügbarkeit von Daten und Diensten**. Dezentralisierung ist eine wesentliche Voraussetzung für die Verfügbarkeit, da sie Funktionalität auf mehrere Nodes verteilt, die Abhängigkeit von einem einzelnen Node verringert und Single Points of Failure vermeidet. Insbesondere sollte die Anzahl der Nodes so gewählt werden, dass die gewünschte Zuverlässigkeit erreicht wird. Außerdem werden durch das Hosten von Nodes bei unterschiedlichen Anbietern in verschiedenen Regionen die Risiken verringert und die Ausfallsicherheit des Netzwerks wird erhöht.

- **Leistung** umfasst den Durchsatz und die Latenz des Netzwerks. Die Einstellungen für Blockgröße, Block Time und Netzwerklatenz können sich direkt auf die Netzwerkleistung auswirken. Ein Ausgleich zwischen Leistung und anderen Eigenschaften ist jedoch unbedingt erforderlich, da übermäßige Einstellungen die Zuverlässigkeit und andere Netzwerkeigenschaften beeinträchtigen können. Die Transaktionskomplexität muss ebenfalls berücksichtigt werden, um eine Überlastung der Netzwerk-Nodes durch redundante Berechnungen zu vermeiden.

6 Belotti M, Bozic N, Pujolle G, Secci S (2019): A Vademecum on Blockchain Technologies: When, Which, and How. IEEE Communications Surveys & Tutorials 21(4):3796–3838. doi:10.1109/COMST.2019.2928178.

7 Gräbe F, Kannengießer N, Lins S, Sunyaev A (2020): Do Not Be Fooled: Toward a Holistic Comparison of Distributed Ledger Technology Designs. In: Bui T (ed) Proceedings of the 53rd Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences.

8 Kubler S, Renard M, Ghatpande S, Georges J-P, Le Traon Y (2023): Decision support system for blockchain (DLT) platform selection based on ITU recommendations: A systematic literature review approach. Expert Systems with Applications 211:118704. doi:10.1016/j.eswa.2022.118704.

9 dena (2019): Blockchain in der integrierten Energiewende. Deutsche Energie-Agentur GmbH, Berlin.

10 Gräbe F, Kannengießer N, Lins S, Sunyaev A (2020): Do Not Be Fooled: Toward a Holistic Comparison of Distributed Ledger Technology Designs. In: Bui T (ed) Proceedings of the 53rd Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences.

11 Kubler S, Renard M, Ghatpande S, Georges J-P, Le Traon Y (2023): Decision support system for blockchain (DLT) platform selection based on ITU recommendations: A systematic literature review approach. Expert Systems with Applications 211:118704. doi:10.1016/j.eswa.2022.118704.

12 dena (2019): Blockchain in der integrierten Energiewende. Deutsche Energie-Agentur GmbH, Berlin.

13 Capocasale V, Gotta D, Perboli G (2023): Comparative analysis of permissioned blockchain frameworks for industrial applications. Blockchain: Research and Applications 4(1):100113. doi:10.1016/j.bcra.2022.100113.

- Die **Minimierung der Umweltbelastung** erfordert Designs, die den Verbrauch von Ressourcen wie Strom und Rechenhardware reduzieren können. Dies lässt sich erreichen, indem eine Überdimensionierung des Netzwerks vermieden und gezielte Entscheidungen zugunsten von Rechenzentren getroffen werden, die Energieeffizienz, stromsparende Hardware und eine nachhaltige Netzwerkinfrastruktur unterstützen. Unsere Toolbox hilft, die richtigen Entscheidungen für das Design zu treffen.

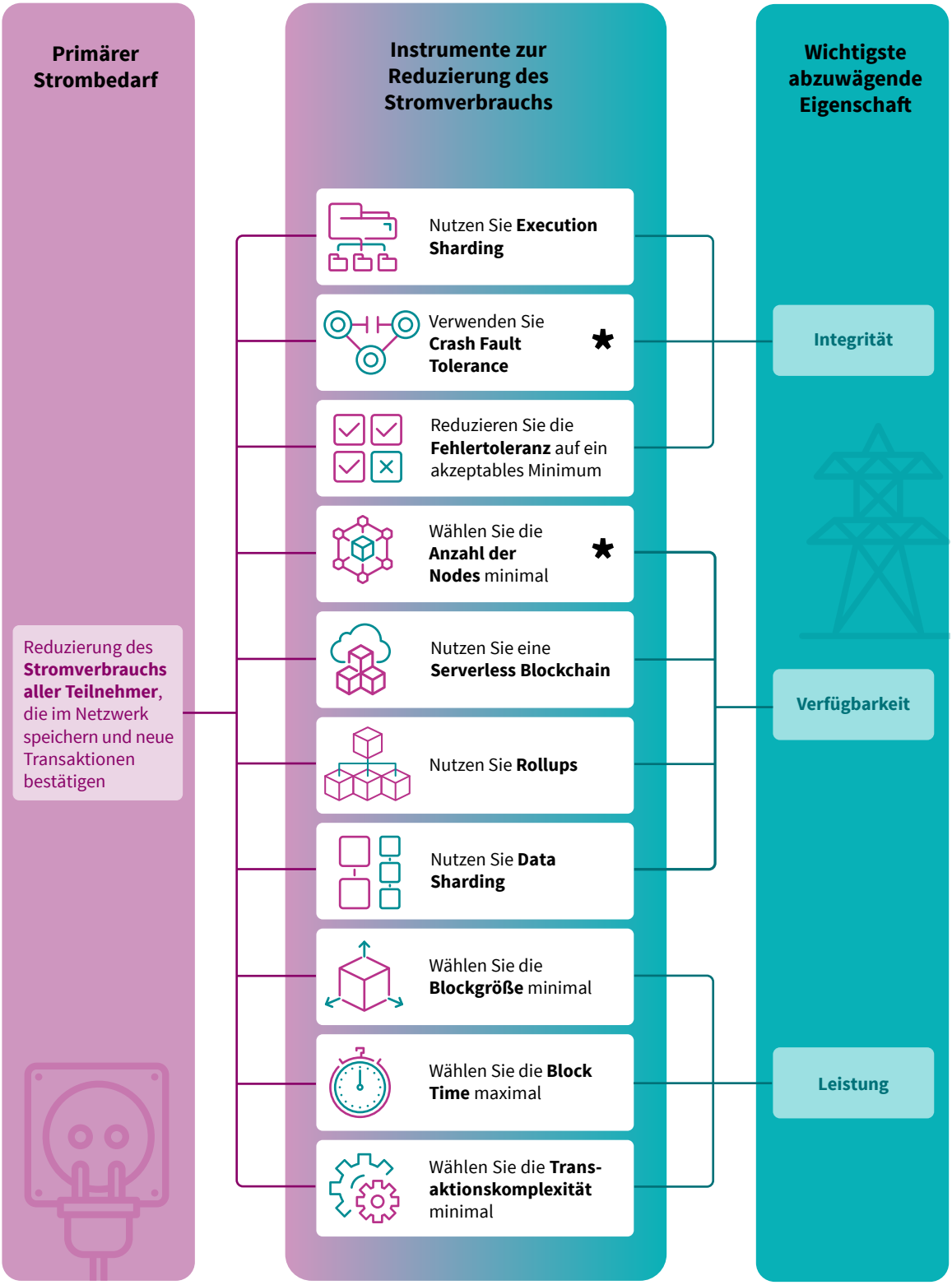
Toolbox für das Design stromsparender Blockchain-Netzwerke

Unsere Toolbox bietet einen umfassenden Satz von Instrumenten zur Reduzierung des Stromverbrauchs in Nicht-PoW-Netzwerken. Mit diesen Instrumenten können Netzwerkdesigner ihre Systeme so einrichten, dass sie den Anforderungen von stromsparenden Anwendungsfällen gerecht werden. Wir haben im Hinblick auf die Optimierung des Stromverbrauchs die Instrumente der zugehörigen Hauptabwägung zugeordnet, sodass Netzwerkdesigner ihre Anwendbarkeit bewerten und eine umfassende Analyse durchführen können.

Die Integrität eines Blockchain-Netzwerks mit unveränderlichem Datenspeicher beruht auf verschiedenen kryptografischen Verfahren und dem zugehörigen Konsensmechanismus, der eine Kommunikation zwischen allen Teilnehmern erfordert. Um den Stromverbrauch zu senken, zielen unsere Instrumente darauf ab, die Komplexität der Kommunikation und Berechnung zu reduzieren: Während die Designoptionen **Fehlertoleranz** und **Typ der Fehlertoleranz** mit dem Konsensmechanismus in Beziehung stehen, bringt die Einführung von **Execution Sharding** eine Aufteilung des Konsensprozesses des Netzwerks in mehrere separate Shards mit sich.

Die Sicherstellung der Daten- und Systemverfügbarkeit in einem Blockchain-Netzwerk wird vor allem durch Dezentralisierung erleichtert. Die folgenden Instrumente reduzieren den Grad der Dezentralisierung in verschiedener Hinsicht und minimieren damit auch redundante Berechnungen. Eine Methode besteht darin, die **Anzahl der Nodes** zu verringern, sodass der Stromverbrauch direkt gesenkt wird. **Serverless Blockchains** sind eine weitere Form der Zentralisierung, die eine hohe Verfügbarkeit bietet, jedoch die mit diesen Anbietern verbundenen potenziellen Ausfallrisiken mit sich bringt. Darüber hinaus führen **Roll-ups** und **Data Sharding** zu einem gewissen Grad an Zentralisierung in Untergruppen des Netzwerks. Roll-ups konsolidieren die Verarbeitung bestimmter Transaktionen auf einen einzigen Node-Betreiber, während Data Sharding die Datenspeicherung auf eine Gruppe von Nodes beschränkt.

Die Leistung eines Nicht-PoW-Netzwerks ist eng mit der Rechenlast verbunden, die jeder Node bewältigen muss, und dies wirkt sich direkt auf den Stromverbrauch aus. Die Toolbox bietet Instrumente zur Neukalibrierung des maximalen Durchsatzes durch Anpassung der **Blockgröße** und der **Block Time**, und dies korreliert direkt mit einer nahezu linearen Verringerung der Rechenlast und Speicherauslastung. In ähnlicher Weise wirkt sich die Minimierung der **Transaktionskomplexität** direkt auf die Rechenlast eines Node aus.



* Das Sternchen kennzeichnet die Designoptionen, die nur in einem Permissioned-Blockchain-Netzwerk verwendet werden können.

Abbildung 3: In der Studie aufgezeigte Instrumente für das Design eines stromsparenden Nicht-PoW-Netzwerks

Handlungsempfehlungen

Wir präsentieren auf der Grundlage der Ergebnisse der Studie mehrere Empfehlungen für unterschiedliche Interessengruppen, um die Stromeffizienz und Nachhaltigkeit der Blockchain-Technologie zu steigern:

- Da unsere Studie nicht alle Aspekte des Stromverbrauchs der Blockchain-Technologie abdeckt, ermutigen wir Forscher, diese Bereiche weiter zu untersuchen. Dabei können insbesondere die Möglichkeiten zur Stromeinsparung durch die von uns aufgezeigten Designinstrumente bewertet oder neue Methoden zur Steigerung der Stromeffizienz einer Blockchain entwickelt werden. Wir regen auch die Entwicklung neuer Frameworks für den Vergleich verschiedener Formen der Dateninfrastruktur an, um eine umfassendere Beurteilung ihrer relativen Effizienz zu ermöglichen. Schließlich kann die interdisziplinäre Forschung dazu beitragen, die Stromeffizienz, die potenziellen Nutzungsmöglichkeiten und die Vorteile von Blockchain-Technologien aus verschiedenen Blickwinkeln zu betrachten und die Umstände zu bestimmen, unter denen eine zusätzliche Nutzung möglicherweise gerechtfertigt ist.

- Normungsorganisationen und politische Entscheidungsträger können dann anhand der Ergebnisse dieser Forschung die Standardisierung, das Benchmarking und die Regulierung der Blockchain-Technologie vorantreiben. Dies kann Kennzahlen für den Stromverbrauch oder die Kohlendioxidemissionen der verschiedenen Blockchains beinhalten, sodass Unternehmen oder Organisationen, die diese Technologie nutzen, ihre CO_2-Bilanz berechnen können. Die Ergebnisse können auch zur Bewertung von Blockchain-Anwendungen genutzt werden, insbesondere im Vergleich zu alternativen Dateninfrastrukturen.

- Entwickler von Blockchain Frameworks sollten auch den Stromverbrauch ihrer Software berücksichtigen. So können sie Features einbeziehen, die direkt auf die Reduzierung des Stromverbrauchs abzielen. Zudem können sie zur allgemeinen Nachhaltigkeit der Blockchain-Technologie beitragen, indem sie praktische Leitlinien für stromsparende Designs bereitstellen und Instrumente entwickeln, mit denen Nutzer den Stromverbrauch des Netzwerks überwachen können.

- Nutzer und Betreiber von Blockchain-Netzwerken sollten bei der Auswahl eines Netzwerks verschiedene Aspekte der Umweltbelastung, zum Beispiel Stromverbrauch und Kohlendioxidemissionen, berücksichtigen. Unsere Studie ermöglicht ein solches gezieltes Netzwerkdesign. Sie zeigt, dass ein gezieltes Netzwerkdesign diese Belastungen verringern und gleichzeitig die Eignung für bestimmte Anwendungsfälle sicherstellen kann. So können Nutzer und Betreiber von den Vorteilen einer dezentralen Infrastruktur profitieren und gleichzeitig die ökologische Nachhaltigkeit ihrer Prozesse erhöhen. Wir empfehlen außerdem, dass Nutzer Auskunft von den Netzbetreibern über ihren Stromverbrauch verlangen können. Dies ermöglicht nicht nur eine fundierte Auswahl der Netzwerke, sondern schafft auch Anreize für Entwickler, den Stromverbrauch als wichtigen Aspekt zu berücksichtigen.

Die oben empfohlenen Maßnahmen sollten von den verschiedenen Interessengruppen gemeinschaftlich und nicht individuell ergriffen werden. Weitere Untersuchungen werden sicherlich noch vorhandene Wissenslücken schließen. Forscher müssen jedoch die Anforderungen von Normungsorganisationen und politischen Entscheidungsträgern berücksichtigen. Zudem erhalten Entwickler von Blockchain Frameworks sowie die Betreiber und Nutzer der resultierenden Netzwerke die Möglichkeit, wertvolle Erkenntnisse zur Anwendbarkeit sowie zu den Begrenzungen und den noch bestehenden Unzulänglichkeiten von Instrumenten und Vorschriften für die Energieeffizienz von Blockchains zu vermitteln. Die dena ermutigt hiermit alle Interessengruppen, die in irgendeiner Weise Einfluss auf den Stromverbrauch von Blockchains nehmen können, sich an einer „Allianz der Willigen“ zu beteiligen und an einer koordinierten Anstrengung zur Maximierung der Nachhaltigkeit der Blockchain-Technologie teilzunehmen. Eine solche Allianz erfordert ein geeignetes Ökosystem, das die verschiedenen Interessengruppen miteinander verbindet, und wir unterstützen dies gerne, indem wir als Vermittler fungieren und die erforderlichen Formate und Foren bereitstellen.

Glossar

Begriff	Definition
Blockchain	Ein verteiltes, dezentrales digitales „Kassenbuch“ (Ledger), in dem Transaktionen zwischen mehreren Computern oder Nodes aufgezeichnet werden. Jede Transaktion wird in einem Block gespeichert, der mit vorherigen Blöcken verknüpft ist, sodass eine Kette von Blöcken (die Blockchain) entsteht.
Blockchain Frameworks	Softwarestacks, mit denen man eigene Permissioned-Blockchain-Netzwerke erstellen kann. Sie ermöglichen die Anpassung an spezielle Anforderungen. Beispiele hierfür sind Corda, Quorum und Hyperledger, das mehrere Teilprojekte umfasst, einschließlich Hyperledger Indy, Fabric und Sawtooth.
Blockchain-Plattformen	Vorhandene Permissionless-Blockchain-Netzwerke, die als Dateninfrastruktur für einen neuen Anwendungsfall, zum Beispiel Ethereum oder Polkadot, genutzt werden können.
Blockchain-Typ	Die Klassifizierung der Blockchain-Typen nach Dezentralisierung, Konsensmechanismus (Permissioned oder Permissionless) und Datenzugriff (privat oder öffentlich).
Blockgröße	Die maximale Menge an Daten, die ein einzelner Block in einer Blockchain enthalten kann. Die Blockgröße bestimmt zusammen mit der Block Time den Durchsatz eines Netzwerks.
Block Time	Die definierte Zeitspanne, bevor der Blockchain ein neuer Block von Daten hinzugefügt wird. Die Block Time bestimmt zusammen mit der Blockgröße den Durchsatz der Blockchain.
Byzantine Fault Tolerance (BFT)	Eine Eigenschaft eines Blockchain-Netzwerks, die den ordnungsgemäßen Betrieb und das Erreichen von Konsens auch dann ermöglicht, wenn einige der teilnehmenden Nodes betrügerisch sind oder böswilliges Verhalten zeigen, und die verhindert, dass sie die Integrität und Funktionalität des Netzwerks untergraben.
Crash Fault Tolerance (CFT)	Diese Eigenschaft ermöglicht den ordnungsgemäßen Betrieb eines Blockchain-Netzwerks und das Erzielen von Konsens auch dann, wenn einige Nodes aufgrund von Fehlern, zum Beispiel Abtrennung eines Teils des Netzwerks oder Absturz von Nodes, ausfallen.
Dateninfrastruktur	Sie besteht aus Hardware-, Software- und Netzwerkschichten, die speziell für die Verwaltung, Speicherung und Verarbeitung von Daten vorgesehen sind. Die Infrastruktur muss je nach den Anforderungen des Anwendungsfalls die erforderlichen Eigenschaften bieten, um die Funktionalität des Anwendungsfalls sicherzustellen. Sie kann als zentrale oder dezentrale (z. B. Blockchain) Struktur gestaltet werden.
(Digitaler) Anwendungsfall / Use Case	Eine digitale Anwendung oder die Verwendung eines digitalen Systems zum Erreichen eines bestimmten Ziels oder zum Ausführen einer bestimmten Aufgabe.
Integrität	Der Schutz der Daten vor unbefugter Änderung, Löschung oder Hinzufügung, um ihre Korrektheit und Konsistenz sicherzustellen.

Begriff	Definition
Konsensmechanismus	Der Algorithmus oder das Protokoll in einem Blockchain-Netzwerk, mit denen zwischen den Teilnehmern Übereinstimmung über den Zustand der Blockchain erzielt wird und Transaktionen bestätigt werden. Sie sorgen für die Integrität und Sicherheit des Netzwerks.
Leistung	Eine Eigenschaft der Dateninfrastruktur, die für eine effiziente und zeitnahe Verarbeitung und Bereitstellung der Daten sorgt, um einen übergangslosen Betrieb zu ermöglichen. Die Leistung kann Aspekte wie die Latenz des Netzwerks, das heißt die zum Verarbeiten einer Transaktion durch das Netzwerk erforderliche Zeit, umfassen.
Node	Ein Teilnehmer in einem Blockchain-Netzwerk, der über eine Kopie der gesamten Blockchain verfügt und an der Bewertung und Übertragung von Transaktionen teilnimmt. Ein Light Node lädt nur einen Teil der Blockchain und ein Full Node lädt die gesamte Blockchain herunter.
Proof of Authority (PoA)	Ein in Permissioned-Blockchain-Netzwerken verwendeter Konsensmechanismus, bei dem eine vorab ausgewählte Gruppe von Nodes mit bekannter Identität und Befugnis Transaktionen bestätigt und auf Grundlage ihrer Reputation oder ihrer Berechtigungen neue Blöcke erstellt.
Proof of Stake (PoS)	Ein Konsensmechanismus, bei dem die Teilnehmer (Staker) auf Grundlage der Token, die sie im Netzwerk halten (Staking), Transaktionen bestätigen und neue Blöcke erstellen. Dadurch soll das Erzielen von Konsens in einer Permissionless Blockchain energieeffizienter als mit dem PoW-Mechanismus erfolgen. Bekannte Beispiele hierfür sind Ethereum und Cardano.
Proof of Work (PoW)	Dieser Konsensmechanismus wird in vielen öffentlichen Blockchains, zum Beispiel Bitcoin oder Dogecoin, verwendet. Dabei lösen die Teilnehmer (Miner) rechenintensive Puzzles, um die Berechtigung zum Bestätigen von Transaktionen und zum Erstellen neuer Blöcke zu erhalten. Dies erfordert erhebliche Rechenleistung und verursacht daher einen hohen Stromverbrauch.
Roll-ups	Roll-ups aggregieren Transaktionen über einen oder mehrere Roll-up-Operators, die den Nachweis ihrer Richtigkeit in der Haupt-Blockchain speichern. Das Überprüfen der aggregierten Nachweise ist weniger rechenintensiv als das Überprüfen einzelner Transaktionen.
Serverless Blockchain	In Serverless Blockchains werden die Nodes von Clouddienstanbietern gehostet. So lassen sich die Rechenressourcen flexibel an den aktuellen Transaktionsdurchsatz anpassen, statt sie beständig an der Spitzenkapazität auszurichten. Zudem kann dank der hohen Zuverlässigkeit und Verfügbarkeit der Clouddienste die Anzahl der erforderlichen Nodes möglicherweise reduziert werden.
Sharding	Ein Verfahren, mit dem das Blockchain-Netzwerk in kleinere Partitionen („Shards“) unterteilt werden kann, um seine Effizienz zu erhöhen. Sharding lässt sich in die Kategorien Data Sharding (Partitionieren der Daten) und Execution Sharding (Aufteilen der Transaktionsverarbeitung) unterteilen. Hierdurch können der Durchsatz und die Effizienz des Netzwerks wesentlich gesteigert werden.
Smart Contract	Sich selbst ausführende Verträge mit vordefinierten Regeln und Bedingungen, die als Code geschrieben und in einer Blockchain bereitgestellt werden. Sie erzwingen und vereinfachen automatisch die Erfüllung der vertraglichen Vereinbarungen, ohne dass Vermittlungsinstanzen erforderlich sind.
Sybil Attack	Ein Angriff auf ein Permissionless-Blockchain-Netzwerk, bei dem eine einzelne Entität zahlreiche falsche Identitäten erstellt, um die Funktionalität und Integrität des Netzwerks zu beschädigen. Diese Bedrohung kann durch einen Sybil-resistenten Konsensalgorithmus gemindert werden.

Begriff	Definition
Transaktion	Eine Dateneinheit, die eine Aktion oder einen Wertaustausch in einer Blockchain darstellt. Dies kann die Übertragung von Kryptowährung, die Erfüllung eines Smart Contract oder das Aufzeichnen sonstiger relevanter Informationen beinhalten.
Transaktions-komplexität	Der Umfang der Rechenressourcen, die zum Verarbeiten und Überprüfen einer Transaktion in einer Blockchain erforderlich sind. Die Komplexität hängt vom Typ und von der Zusammensetzung der Transaktion ab, einschließlich zugehöriger Smart Contracts oder zugehöriger Datenvorgänge.
Trusted Third Party (TTP)	Eine Vermittlungsinstanz, der mehrere Parteien vertrauen, um Transaktionen zu erleichtern und ihre Vertrauenswürdigkeit sicherzustellen. Dieses Vertrauen auf eine zentrale Instanz kann zu Schwachstellen oder zentralen Fehlerstellen in einem System führen.
Umweltbelastung	Die Belastung der Umwelt durch die digitale Infrastruktur, insbesondere durch Stromverbrauch, CO_2-Emissionen und Elektronikschrott.
Verfügbarkeit	Die Zusicherung des Zugriffs auf Daten und Dienste, wenn sie benötigt werden.
Vertraulichkeit	Die Gewissheit, dass der Zugriff auf und die Offenlegung von Daten auf autorisierte Benutzer und Systeme beschränkt sind.
Zero-Knowledge Proof (ZKP)	Eine kryptografische Methode, mit der eine Partei gegenüber einer anderen Partei die Gültigkeit einer Aussage nachweisen kann, ohne zusätzliche Informationen preiszugeben.

www.dena.de

future-energy-lab.de

dena
Deutsche Energie-Agentur