Herausforderungen der Software-Architektur unter Einsatz von Blockchain-Technologie in Anwendungen

Die Blockchain-Technologie hat seit dem Erfolg von Kryptowährungen wie Bitcoin viel Aufmerksamkeit erregt. Das Konzept dieser Technologie besteht darin, Daten in Blöcken zu sichern, die dezentral auf miteinander verbundenen Knotenpunkten gespeichert werden. Ziel ist es, ein Konstrukt zu schaffen, das nicht verändert oder manipuliert werden kann. Um ein solches Netz zu betreiben und die Sicherheit im Netz herzustellen, ist eine enorme Rechenleistung erforderlich. Mit dieser Methode ist es möglich, Anwendungen zu programmieren, die nicht die Beteiligung einer dritten Vertrauensquelle, wie einer Bank, erfordern. Dies stellt jedoch Softwareentwickler*innen, die eine dezentrale Struktur in ihre Anwendungen implementieren wollen, vor einige Herausforderungen. Der folgende Text befasst sich mit der grundlegenden Struktur der Blockchain, ihren Vor- und Nachteilen und den Herausforderungen, die die Implementierung von Anwendungen mit Blockchain-Technologien mit sich bringt.

Die Blockchain

Die Blockchain ist eine dezentrale Softwarearchitektur, die aus verschiedenen Knotenpunkten zusammengesetzt ist. Ihr wesentlicher Bestandteil ist das Abrufen und Speichern von Informationen. Jeder Knoten besitzt den gesamten Datensatz und synchronisiert sich mit anderen Knoten in Form von Transaktionen, verteilt und bestätigt neue Blöcke mithilfe eines Konsensalgorithmus, um neue Informationen in der Kette zu speichern. Die Informationen werden in der Datenkette in Blöcken gespeichert. Der Inhalt der Blöcke kann variieren (zum Beispiel bei Kryptowährungen die Transaktionsdaten). [2] Darüber hinaus enthält jeder Block den Hash-Wert des vorherigen Blocks und berechnet daraus seinen eigenen Hash-Wert. Dies bindet die Blöcke aneinander und erschwert ihre nachträgliche Änderung. Durch diese und andere Konzepte soll die Blockchain zu einem Werkzeug werden, das wir in der Softwareentwicklung einsetzen können, um Anwendungen vertrauenswürdiger, transparenter, sicherer und zuverlässiger zu machen. [4]

Basic Konzepte der Blockchain

Hash (vertrauenswürdiger)

Der Hash ist ein „Fingerabdruck" und hat immer die gleiche Länge, unabhängig von der Eingabe. Er bildet die Eingabe ab, ohne jegliche Informationen über die tatsächliche Eingabe zu liefern. Anhand des Hash-Werts lässt sich daher überprüfen, ob die Eingabe nach der Berechnung des Werts geändert wurde oder nicht. Dieselbe Eingabe gibt immer denselben Hash-Wert zurück. Wird der zu hashende Text geändert, ändert sich auch der tatsächliche Hash-Wert. [4]

Konsens-Algorithmus (vertrauenswürdiger)

Mit dem Konsens-Algorithmus werden neue Blöcke zur Blockkette hinzugefügt beziehungsweise bestätigt und im Netz verteilt. Da alle Knotenpunkte gleichberechtigt sind und alle an einer Kette arbeiten, muss ein Konsens darüber gefunden werden, wie neue Blöcke hinzugefügt werden. Die gängigsten Konzepte, die im Text vorgestellt werden, sind Proof of Work und Proof of Stake. Beide zielen darauf ab, Datenfälschungen durch Veränderung der Blockchain zu verhindern. Um die Kette zu manipulieren, sind je nach Konsensalgorithmus sehr viel Rechenleistung oder sehr viel Geld erforderlich. [7]

Unveränderlichkeit

Durch die Verkettung der Blöcke und den Konsensalgorithmus kann sichergestellt werden, dass unter der Annahme, dass genügend Knoten vorhanden sind, ein Zustand der Kette erreicht wird, in dem die in der Kette gespeicherten Daten nicht mehr verändert werden können, ohne dass sie verworfen werden. [16]

Dezentrales Netzwerk (transparenter & zuverlässiger)

Das Netz besteht aus verschiedenen Peer-to-Peer-Blöcken (Knoten), die ohne eine zentrale Stelle miteinander kommunizieren, um Daten auszutauschen und zu speichern. [6]

Trusted vs. Untrusted Networks

Wir unterscheiden hier zwischen „vertrauenswürdigen und nicht vertrauenswürdigen" Netzen. Bei „vertrauenswürdigen" Knoten wird davon ausgegangen, dass alle Teilnehmer ehrlich sind und dem Netzwerk nicht schaden wollen. Dieses Konzept wird auf die derzeit meist firmeninternen dezentralen Datenbanken angewandt. Bei Blockchains wird in der Regel die Theorie eines nicht vertrauenswürdigen Netzwerks verfolgt, bei dem sich einige Knoten (Nodes) willkürlich verhalten können, ohne das Netzwerk tatsächlich zu beeinflussen. In diesem Fall erhält jede Node die gesamte Blockchain, die sie benötigt, um entscheiden zu können, ob eine Transaktion gültig ist oder nicht. [5]

Chancen der Blockchain-Technologie

Die Blockchain-Technologie kann uns helfen, Softwareanwendungen zu entwickeln, die vertrauenswürdiger, transparenter, sicherer und zuverlässiger sind als zentralisierte Anwendungen, die das Vertrauen Dritter erfordern. Daraus resultiert der Vorteil, dass Anwendungen nicht mehr eine vertrauenswürdige dritte Partei als Quelle angewiesen benötigen, was zentrale Anwendungen, wie wir sie derzeit haben, erheblich verändern würde. Das populärste System, das diese Technologie nutzt, sind derzeit Kryptowährungen. Diese nutzen die Blockchain-Technologie, um eine digitale Währung ohne ein zentrales System wie eine traditionelle Bank zu implementieren. [4]

Die dezentrale Verteilung der Chain auf viele Knoten soll sicherstellen, dass ein Ausfall einzelner Knoten nicht zu einem Gesamtausfall führt, wodurch auch das Risiko eines Totalausfalls im Vergleich zu zentralisierten Anwendungen deutlich minimiert wird. Erwähnenswert ist auch, dass die Anzahl der Knoten einen Einfluss auf die Transparenz und Sicherheit des Systems hat. Je mehr Knoten das System hat, desto sicherer und transparenter wird es. Denn jeder Knoten erhält die gesamte Kopie der Blockchain, sodass keine Transaktion unbemerkt geändert oder hinzugefügt werden kann. Um dies zu erreichen, muss derzeit viel Rechenleistung aufgewendet werden, was sich auch im Stromverbrauch niederschlägt. [4]

Rechenaufwendige Challenges in der Blockchain-Entwicklung

Konsensmechanismus

Um die Sicherheit zu erhöhen, wird oft ein Proof-of-Work-Verfahren verwendet. Dieses dient bei vielen Blockchain-Varianten als Konsensalgorithmus. Dabei muss der Knoten Rechenleistung aufwenden, um eine vordefinierte Aufgabe lösen zu können. Im Falle des Bitcoin-Netzwerks muss der Knoten eine NONCE (number only used once) eingeben, um einen neuen Block zum Netzwerk hinzuzufügen. Die Aufgabe bezieht sich auf den Hash-Wert des hinzuzufügenden Blocks. Sobald eine Lösung gefunden wurde, ist es einfach, sie als korrekt zu verifizieren. Bei Bitcoin wäre ein Beispiel, einen Hash-Wert zu finden, der mit n Nullen beginnt. Die Miner müssen nun eine korrekte NONCE finden. Gelingt dies, können die anderen Knoten im Netz den Wert verifizieren und zu ihrer Kette hinzufügen. Der Nachteil dieser Technologie ist der erforderliche Rechenaufwand und die „verschwendeten" Ressourcen, wie Strom oder Rechenleistung, die für andere Anwendungen hätten genutzt werden können.

Eine Alternative zum weit verbreiteten Proof of Work ist der Proof of Stake, bei dem die Knoten einen Einsatz leisten, der als Sicherheitsmaßnahme für das Netz dient. Dann wird je nach Algorithmus ein Knoten ausgewählt, der einen neuen Block anhängt und von anderen Knoten überprüft wird. Versucht ein Angreifer, eine Transaktion zu manipulieren, wird er mit dem Verlust des Einsatzes bestraft. Mit Hilfe des Proof-of-Stake-Konzepts kann etwas Energie eingespart werden, was sich jedoch auf die Zuverlässigkeit der Blockgenerierung und die Leistung des Systems auswirkt. Eine Kombination der beiden Algorithmen würde mehr Zuverlässigkeit bieten. [3]

Skalierbarkeit des Systems

Darüber hinaus ergeben sich neue Probleme mit der Skalierbarkeit der Blockchain. In der derzeitigen Architektur der Blockchain erhält jeder Knoten eine Kopie aller Daten, um transparent, sicher und mit hoher Verfügbarkeit handeln zu können. Diese Struktur führt jedoch zu Leistungsproblemen, da jeder Knoten seinen Speicher erweitern müsste, um weiterhin am Netz teilnehmen zu können. Die Knoten können jedoch nicht unendlich viel Speicher verwalten.

Die Blockchain hinter der Kryptowährung Bitcoin benötigt derzeit 400,5 Gigabyte (blockchain.com, Stand: 12. April 2022), die jeder Knoten, der am Netzwerk teilnehmen will, herunterladen muss. Im Vergleich zum Vorjahr waren es 338,8 Gigabyte, die für die Speicherung der Kette verwendet wurden. Ethereum benötigt rund 620 Gigabyte für die Speicherung ihrer Blockchain.

Es gibt verschiedene Ansätze, um mit Hilfe der veränderten Struktur mehr Skalierbarkeit in die Blockchain zu bringen. So ermöglicht das Multi-Chain-Konzept die getrennte Speicherung von Transaktionen, die nicht miteinander verknüpft sind. Sofern dies erfüllt ist, können Transaktionen auch gleichzeitig ausgeführt werden. Ein weiteres Konzept wäre eine Sidechain, die neben der eigentlichen Blockchain existiert, aber mit dieser verankert ist. Mit Hilfe dieser Sidechain können Transaktionen ausgelagert werden, sie verfügt über einen eigenen Konsensmechanismus sowie ein eigenes „Ledger". Transaktionen können zwischen der Sidechain und der Blockchain (Hauptkette) hin und her transferiert werden. Die Geschwindigkeit der Transaktionen auf der Sidechain ist nicht direkt von der Geschwindigkeit der Transaktionen auf der Hauptchain abhängig. [6]

Sicherheit (Angriffe auf Blockchains)

Die Blockchain ist ein verteiltes System, das Informationen in Form von Blöcken speichert und diese an die Kette anhängt. Dies geschieht im ständigen Austausch mit den anderen Teilnehmern des Netzwerks. Versuchen nun Angreifer*innen, Daten in einem Block zu verändern und an die Kette anzuhängen, erkennt das Konsensprotokoll dies und die Kette wird als ungültig betrachtet, da die Mehrheit der anderen Knoten diesen manipulierten Block nicht enthält. Gelingt es dem*r Angreifer*in, mehr als 51 Prozent der Rechenleistung des Netzwerks zu erreichen, kann er*sie die Blockkette manipulieren und andere Knoten außer Kraft setzen. [6]

Challenges der Blockchain-Implementierung

Die Blockchain stellt auch die Anwendungsentwickler vor Herausforderungen, da sie sich anders verhält als eine klassische zentrale Datenbank. Im folgenden Abschnitt werden einige der Herausforderungen angeführt, die in der frühen Entwicklungsphase berücksichtigt werden sollten.

Dezentralisierungsproblem

Dabei wird zwischen vollständig dezentralen Anwendungen, sogenannten DApps, unterschieden. Hier wird nur die Blockchain als Backend genutzt. Das Backend könnte in einen sogenannten Smart Contract umgewandelt werden, der auf der Blockchain gespeichert wird und somit nicht mehr verändert werden kann. Die Vorteile dieser komplett dezentralen Struktur sind unter anderem, dass die Nutzer*innen mehr Vertrauen haben können, da die Smart Contracts im Nachhinein nur schwer zu ändern sind. Eine zentrale Behörde hat somit keine Kontrolle mehr, was auch die Zensur erschwert.

Eine dezentrale Architektur hat zudem den Vorteil, dass einzelne Knotenpunkte ausfallen können, ohne dass die Anwendung offline ist. Dennoch ist eine solche Architektur nicht für jede Anwendung geeignet. Diese Struktur führt zu einer geringen Transaktionsrate, sodass diese Architektur nicht so viele Daten verarbeiten kann wie eine zentralisierte Anwendung, zumal Transaktionskosten anfallen, die von der Nutzerin bzw. vom Nutzer bezahlt werden müssen, während hybride Apps die Blockchain-Technologie nur für spezielle Aufgaben nutzen. [1]

Transaction-Flow-Problem

Aufgrund der völlig dezentralen Struktur der Blockchain und des Konsensprotokolls kommt es, wie oben erwähnt, zu erheblichen Wartezeiten für Transaktionen auf der Blockchain. Wie lange eine Transaktion genau dauert, lässt sich nur schwer vorhersagen, da es von mehreren Variablen abhängt, beispielsweise davon, wann die Transaktion zu einem Block hinzugefügt wurde und wie lange es dauert, bis die richtige NONCE gefunden und von den anderen Knoten bestätigt wird. Im Durchschnitt kann das Bitcoin-Netzwerk 7 Transaktionen pro Sekunde verarbeiten. Im Jahr 2021 gab es Transaktionszeiten bis zu einem Maximum von rund 3.340 Minuten (blockchain.com Stand 12. April 2022) Dieses Verhalten muss bei der Entwicklung und Planung der Software-Architektur berücksichtigt werden. Die Forscher*innen nennen zwei Möglichkeiten, wie dies in den Anwendungen umgesetzt werden kann:

Synchron

Die Transaktion wirkt sich so auf das Verhalten der Software aus, dass Benutzer*innen im aktuellen Zustand bleiben, bis die Transaktion vollständig verarbeitet und bestätigt ist.

Asynchron

Bei dieser Art der Implementierung geht die Anwendung in einen vorausschauenden Zustand über, sodass die Anwendung nicht mehr mit der Blockchain synchron ist. Dabei wird davon ausgegangen, dass jede Transaktion ausgeführt wird.

Eine synchrone Anwendung ist konsistenter, sie befindet sich im gleichen Zustand wie der Knoten im Blockchain-Netzwerk, beeinträchtigt aber den Benutzer*innenfluss, da es zu erheblichen Wartezeiten kommen kann. Die asynchrone Anwendung hingegen bietet einen schnelleren Benutzer*innenstrom, muss aber auch mit verschiedenen Rollback-Szenarien umgehen. [1]

Oracle-Problem (offchain content)

Das Oracle-Problem tritt auf, wenn die Blockchain oder der Smart Contract Daten aus der Realität benötigt. Wenn auf der Blockchain Transaktionen stattfinden, beispielsweise eine Überweisung von Kryptowährungen auf verschiedene Wallets, geschieht dies ohne externe Einflüsse. Dies nennt man Onchain-Inhalt, da die Blockchain keine Daten aus anderen Quellen benötigt, um die Übertragung durchzuführen. Problematisch wird es jedoch, wenn ein dezentrales System wie die Blockchain auf eine externe Quelle angewiesen ist, die nicht dezentralisiert sind ("offchain content").

Smart Contracts sind selbst ausführbarer Code, der sich auf der Blockchain befindet. Wenn man mit ihnen beispielsweise eine Wette auf ein Fußballspiel abbilden möchte, muss man Daten von diesem Spiel abrufen, um zu entscheiden, wer der Gewinner der Wette ist. Dies geschieht über eine Schnittstelle, eine zentrale Schnittstelle, das Oracle. Sie stellt der Blockchain Daten aus der realen Welt zur Verfügung und regelt damit die Bedingungen im Smart Contract. Alle Vorteile der Blockchain könnten durch einen einzigen Fehler zunichtegemacht werden. Denn wenn das Oracle unter der Kontrolle der Angreifer*innen ist, können diese den Smart Contract kontrollieren. [7]

Datenschutzproblem

Die DSGVO gilt auch für diesen Bereich der Informationsverarbeitung, die EU sieht in der Blockchain eine potenzielle Gefahr für die Rechte und Pflichten der Bürger*innen, wenn es um personenbezogene Daten geht. [8] Dies liegt daran, dass die derzeitige Struktur der Blockchain dazu dient, eine unveränderliche Historie z. B. von Transaktionen zu speichern, was wiederum im Widerspruch zu Artikel 17 der DSGVO steht. Dieser gibt den Nutzern*innen das Recht auf Vergessenwerden, was wiederum bedeutet, dass die entsprechenden personenbezogenen Daten wie der Kontostand oder die Transaktionen bei Kryptowährungen aus der Blockchain gelöscht werden müssen.

Einsatz der Blockchain in der Praxis

Neben dem Bankwesen gibt es viele andere Bereiche, in denen Blockchain-Technologien eingesetzt werden können, wie zum Beispiel beim elektronischen Wahlsystem. Damit soll die Einrichtung eines modernen Wahlsystems ermöglicht werden, das Wahlbetrug ausschließt und die Wahlbeteiligung erhöht. Das System wurde im Jahr 2018 in West Virginia getestet. Für dieses digitale Wahlsystem wurde die Blochain verwendet, es soll verhindert werden, dass Wählerstimmen gefälscht werden, außerdem soll durch das System ein transparenterer Wahlprozess entstehen. Ein weiterer Aspekt ist die zeitnahe Auswertung der digital erfassten Ergebnisse. Ein System verwendet beispielsweise einen von der Regierung ausgestellten Ausweis und eine Webcam, um die Stimmabgabe der Bürger*innen zu verifizieren, sodass diese ihre Stimmen abgeben und anschließend verfolgen können, ob diese korrekt abgegeben wurde. Bevor das System jedoch in großem Maßstab eingesetzt werden kann, müssen die Entwickler dieses Systems noch einige der oben genannten Probleme lösen, beispielsweise in Bezug auf Skalierbarkeit und Energieeffizienz. Außerdem muss trotz der Transparenz die Geheimhaltung des Stimmzettels gewahrt bleiben. [10]

Die Blockchain kann auch bei der Pandemiebekämpfung nützlich sein, wenn es darum geht, die Sicherheit zu gewährleisten, etwa bei der Verteilung von Impfstoffen, um die Lieferkette zu verfolgen und Missbrauch zu verhindern, gefälschte Impfstoffe aufzuspüren und Aufzeichnungen über Impfungen zu führen. Für ein solches Projekt entscheiden sich die Forscher*innen für eine private Blockchain-Architektur, bei der die einzelnen Teilnehmer erst zugelassen werden müssen, bevor sie am Netz teilnehmen dürfen. Ein Grund dafür ist, dass jedem Knoten im System eine Rolle zugewiesen werden muss. Einzelne Knoten im Netzwerk können Rohdaten hinzufügen

und sie kryptografisch in den Blöcken speichern. Dies sind Onchain-Inhalte, die mit Offchain-Inhalten von Gesundheitsbehörden verknüpft werden können. Diese wiederum können dann über eine Schnittstelle Anwendungen wie den Grünen Pass zur Verfügung gestellt werden. [9]

Zusammengefasst

Die Blockchain-Technologie ist eine Möglichkeit, eine sichere, vertrauenswürdige und transparente Methode zur dezentralen Speicherung von Daten zu schaffen. Dadurch können Entwickler*innen vertrauenswürdige Instanzen, wie die Bank, im Beispiel der Kryptowährungen ersetzen. [4, 5, 6, 7] Damit diese Technologie zu einem Teil unseres Alltags wird, stehen die Blockchain-Entwickler*innen und die Programmierer*innen, die diese Technologie nutzen, noch vor einigen Herausforderungen. Die Blockchain muss skalierbarer werden, damit sie für transaktionsintensivere Anwendungen genutzt werden kann. Dabei müssen auch die Transaktionszeiten minimiert werden, um das Problem des Transaktionsflusses zu lösen. [6] Entwickler*innen sollten abwägen, inwieweit sie die Blockchain in ihre Anwendungen implementieren und sie so früh wie möglich einbinden. Sie müssen sich darüber im Klaren sein, dass das Oracle-Problem bei hybriden Lösungen eine große Rolle spielen wird, da es die Vorteile der Blockchain-Technologie zunichte machen könnte. Trotz dieser Herausforderung ist sie jedoch ein Weg, um Anwendungen dezentraler zu gestalten und Dienste ohne Dritte zu schaffen.

Quellenverzeichnis

[1] M. Wöhrer and U. Zdun, "Architectural Design Decisions for Blockchain-Based Applications," 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021, pp. 1-5, doi: 10.1109/ICBC51069.2021.9461109.
(https://ieeexplore.ieee.org/document/9461109)

[2] F. Wessling, C. Ehmke, O. Meyer and V. Gruhn, "Towards Blockchain Tactics: Building Hybrid Decentralized Software Architectures," 2019 IEEE International Conference on Software Architecture Companion (ICSA-C), 2019, pp. 234-237, doi: 10.1109/ICSA-C.2019.00048.
(https://ieeexplore.ieee.org/document/8712151)

[3] P. R. Nair and D. R. Dorai, "Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 279-283, doi: 10.1109/ICICV50876.2021.9388487.
(https://ieeexplore.ieee.org/document/9388487)

[4] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018, pp. 1-6, doi: 10.1109/AIEEE.2018.8592253.
(https://ieeexplore.ieee.org/document/8592253)

[5] F. Schuhknecht, "Talking Blockchains: The Perspective of a Database Researcher," 2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW), 2021, pp. 72-75, doi: 10.1109/ICDEW53142.2021.00020.
(https://ieeexplore.ieee.org/document/9438723)

[6] Yang Lu, “The blockchain: State-of-the-art and research challenges”, Journal of Industrial Information Integration, Volume 15, 2019, Pages 80-90,ISSN 2452-414X, https://doi.org/10.1016/j.jii.2019.04.002.
(https://www.sciencedirect.com/science/article/pii/S2452414X19300019)

[7] G. Caldarelli, "Real-world blockchain applications under the lens of the oracle problem. A systematic literature review," 2020 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), 2020, pp. 1-6, doi: 10.1109/ICTMOD49425.2020.9380598.
(https://ieeexplore.ieee.org/document/9380598)

[8] D. A. Hamdi and O. Alfandi, "Pros and cons of Blockchain-based approaches in Education," 2021 IEEE Global Engineering Education Conference (EDUCON), 2021, pp. 1558-1564, doi: 10.1109/EDUCON46332.2021.9454118.
(https://ieeexplore.ieee.org/document/9454118)

[9] L. Rosyidi, Warsono and M. S. Romadhon, "Design of Blockchain Implementation for Supervision of Vaccine Distribution: Indonesia Case," 2021 Sixth International Conference on Informatics and Computing (ICIC), 2021, pp. 1-6, doi: 10.1109/ICIC54025.2021.9632990.
(https://ieeexplore.ieee.org/document/9632990)

[10] **Z**. Khudoykulov, U. Tojiakbarova, S. Bozorov and D. Ourbonalieva, "Blockchain Based E-Voting System: Open Issues and Challenges," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-5, doi: 10.1109/ICISCT52966.2021.9670245.
(https://ieeexplore.ieee.org/document/9670245)