BLOCKCHAIN FOR AGRIFOOD EDU

Modul 2

Die Bausteine der Blockchain und der Blockchain-Mechanismus

Co-funded by the European Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Beschreibung des Moduls

Das Modul "Die Bausteine der Blockchain und der Blockchain-Mechanismus" umfasst die Grundsätze der Blockchain-Erstellung (was ist ein Block und was ist eine Kette), die grundlegenden Merkmale des traditionellen, dezentralen und verteilten Konzepts der Datenbanken sowie die Eigenschaften und Anforderungen der Kryptographie und Hash-Funktionen und hat als Ergebnis. Es sind auch eine Erklärung des Unterschieds zwischen Proof of Work und Proof of State und die wichtigsten Vorteile von Blockchain im Modul enthalten.

Lernergebnisse

Die Absolventen des Moduls erwerben grundlegende theoretische Kenntnisse im Bereich der Blockchain-Erstellung und Anforderungen an kryptographische und Hash-Funktionen. Das Wissen wird anhand einer Fallstudie gefestigt und durch ein Quiz überprüft.

Die Ergebnisse sind:

- Modul mit Lernmaterial
- Fallstudie
- Interaktive Tätigkeit
- Quiz

Inhalt

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Inhalt

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Inhalt

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

01

EINLEITUNG ZU Modul 2

Die Bausteine der Blockchain und der Blockchain-Mechanismus

Einführung

Was ist die Blockchain-Technologie?

Die Blockchain-Technologie ist ein fortschrittlicher Datenbankmechanismus, der einen transparenten Informationsaustausch innerhalb eines Unternehmensnetzwerks ermöglicht. Eine Blockchain-Datenbank speichert Daten in Blöcken, die in einer Kette miteinander verbunden sind.

Die Daten sind chronologisch konsistent, da die Kette nicht ohne Zustimmung des Netzwerks gelöscht oder geändert werden kann. Folglich können Sie die Blockchain-Technologie nutzen, um ein unveränderliches oder unveränderbares Hauptbuch zur Verfolgung von Aufträgen, Zahlungen, Konten und anderen Transaktionen zu erstellen.

Das System verfügt über eingebaute Mechanismen, die unautorisierte Transaktionseinträge verhindern und die Konsistenz in der gemeinsamen Sicht auf diese Transaktionen herstellen.

Einführung

Die Bausteine der Blockchain und der Blockchain-Mechanismus

Blockchain-Bausteine und Blockchain-Mechanismus sind Schlüsselkonzepte im Bereich des digitalen Ökosystems und der Kryptowährungen.

Blockchain ist eine Technologie, mit der Transaktionen und Ereignisse in einem dezentralen und unveränderlichen System aufgezeichnet werden können.

Die Grundbausteine der Blockchain sind die folgenden Elemente:

- Blöcke
- Verteiltes Hauptbuch
- Kryptographie
- Konsens-Mechanismus
- Unveränderlichkeit

Einführung

Die Bausteine der Blockchain und der Blockchain-Mechanismus

BLOCKS

Die Blockchain besteht aus einer Kette von Blöcken, wobei jeder Block eine Liste von Transaktionen und eine eindeutige Kennung (Hash) des vorherigen Blocks enthält. Dadurch wird die Integrität der Daten gewährleistet.

VERTEILTER LEDGER

Die Blockchain wird auf Tausenden von Computern (Knoten) in der ganzen Welt gespeichert. Jeder Knoten hat eine Kopie der gesamten Blockchain, was ihre Widerstandsfähigkeit gegen Ausfälle und Angriffe erhöht.

Einführung

Die Bausteine der Blockchain und der Blockchain-Mechanismus

CRYPTOGRAPHIE

Die asymmetrische Kryptographie wird zur Sicherung von Transaktionen verwendet. Jeder Teilnehmer hat einen privaten und einen öffentlichen Schlüssel, die die Überprüfung und Unterzeichnung von Transaktionen ermöglichen.

KONSENSMECHANISMUS

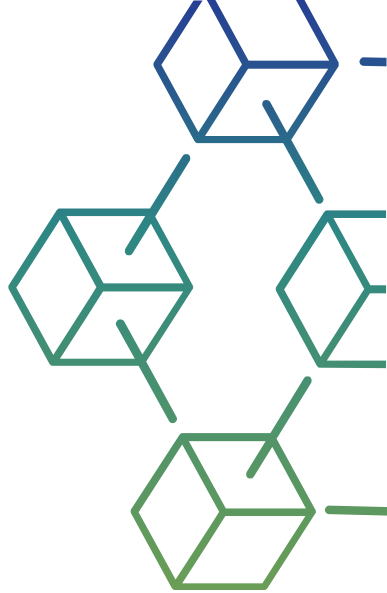
Bei der Blockchain müssen die Knoten einen Konsens über gültige Transaktionen erzielen. Dies wird in der Regel durch verschiedene Konsensalgorithmen wie Proof of Work (PoW) oder Proof of Stake (PoS) erreicht.

IMMUTABILITÄT

Sobald Daten in der Blockchain gespeichert sind, können sie nicht mehr ohne weiteres geändert werden. Das sorgt für Vertrauen und Transparenz.

Einführung

Die Bausteine der Blockchain und der Blockchain-Mechanismus



- Der Blockchain-Mechanismus gewährleistet die Integrität der Daten und stellt sicher, dass Transaktionen unanfechtbar sind.
- Blockchain findet nicht nur in der Kryptowährung Anwendung, sondern auch im Finanzwesen, in der Lieferkette, im Gesundheitswesen und in vielen anderen Branchen.
- Ihre Zukunft hängt von der Fähigkeit von Gemeinschaften und Unternehmen ab, innovativ zu sein und ihr Potenzial zu nutzen, um echte Probleme zu lösen und die digitale Welt zu verändern.

02

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung

Wie funktioniert eine Blockchain?

- Jede Transaktion oder Dateneingabe, die als "Block" bezeichnet wird, ist durch kryptografisches Hashing sicher mit der vorhergehenden verknüpft, wodurch eine kontinuierliche und fälschungssichere Informationskette entsteht.
- Da es keine Möglichkeit gibt, einen Block zu ändern, ist Vertrauen nur an dem Punkt erforderlich, an dem ein Benutzer oder ein Programm Daten eingibt. Dieser Aspekt reduziert den Bedarf an vertrauenswürdigen Dritten, bei denen es sich in der Regel um Prüfer oder andere Menschen handelt, die Kosten verursachen und Fehler machen.

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung

Eine Blockchain besteht aus Programmen, die Skripte genannt werden und die Aufgaben ausführen, die man normalerweise in einer Datenbank erledigen würde: Eingabe und Abruf von Informationen sowie deren Speicherung und Ablage an einem bestimmten Ort. Eine Blockchain ist verteilt, was bedeutet, dass mehrere Kopien auf vielen Rechnern gespeichert sind, die alle übereinstimmen müssen, damit sie gültig sind.

Die Blockchain sammelt Transaktionsinformationen und trägt sie in einen **Block** ein, wie eine Zelle in einer Tabellenkalkulation, die Informationen enthält. Sobald der Block voll ist, werden die Informationen durch einen **Verschlüsselungsalgorithmus** geleitet, der eine hexadezimale Zahl, den **Hash,** erzeugt

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung

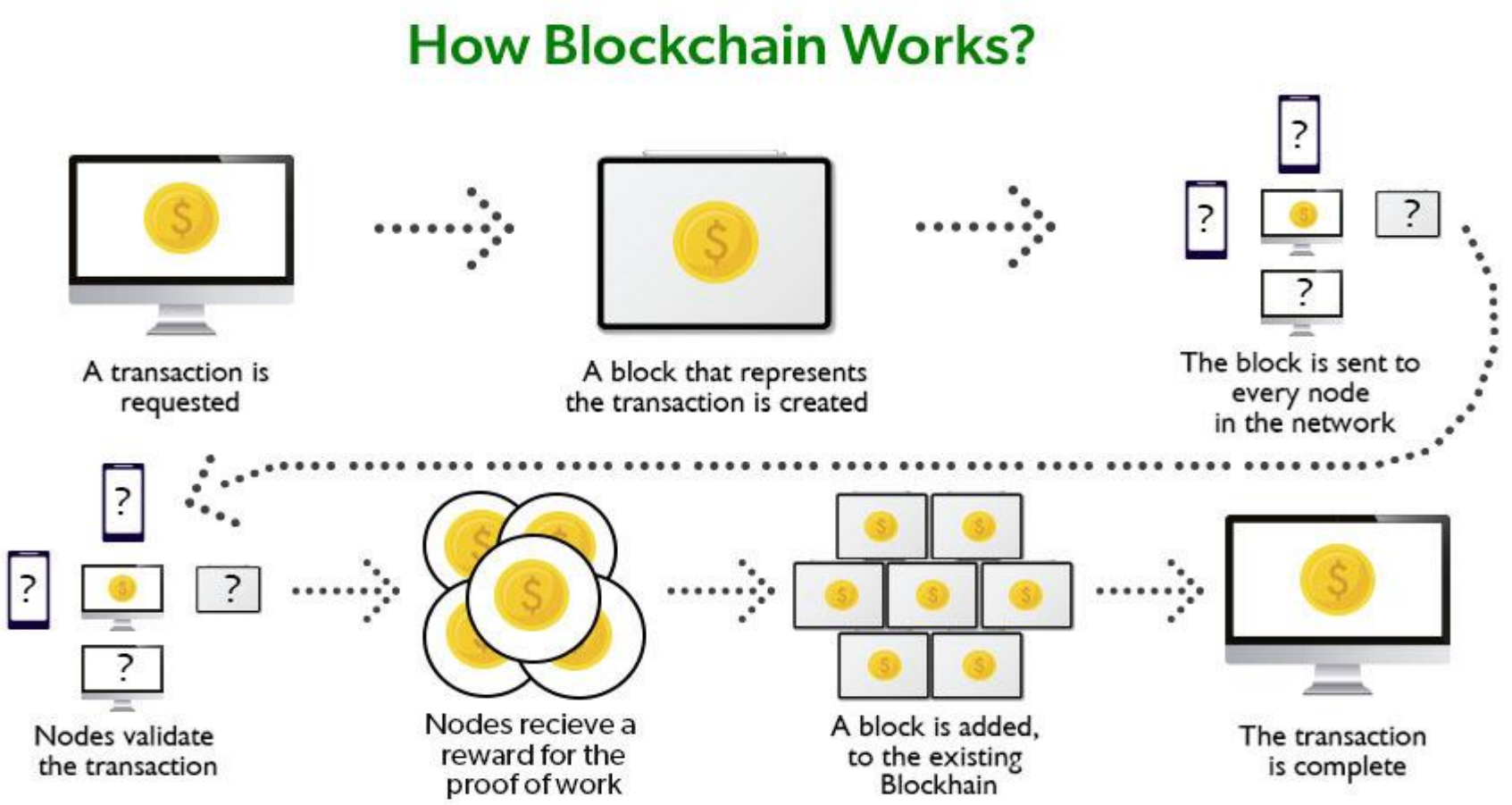


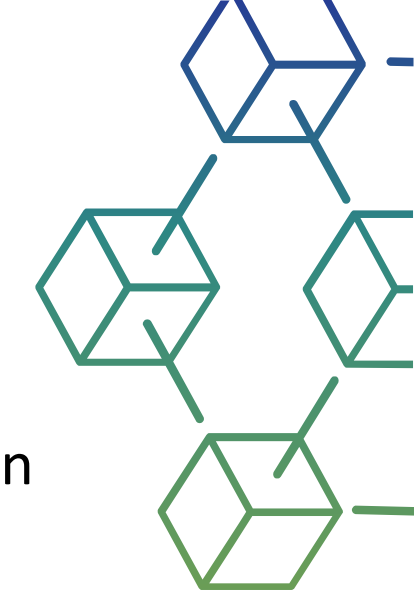
Abbildung 1: So funktioniert die Blockchain (Quelle: https://www.geeksforgeeks.org/how-does-the-blockchain-work/)

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung

Der Transaktionsprozess in einer Blockchain lässt sich wie folgt zusammenfassen:

1. Erleichterung einer Transaktion
2. Überprüfung der Transaktion
3. Bildung eines neuen Blocks
4. Konsens-Algorithmus
5. Hinzufügen des neuen Blocks zur Blockchain
6. Transaktion abgeschlossen

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung



Der Hashwert wird dann in den folgenden Blockkopf eingegeben und mit den anderen Informationen des Blocks verschlüsselt. So entsteht eine Reihe von Blöcken, die aneinandergereiht werden.

Transaktionen folgen einem bestimmten Prozess, je nachdem, auf welcher Blockchain sie stattfinden. Wenn Sie zum Beispiel auf der Bitcoin-Blockchain eine Transaktion mit Ihrer Kryptowährungs-Wallet - der Anwendung, die eine Schnittstelle für die Blockchain bereitstellt - initiieren, wird eine Reihe von Ereignissen ausgelöst.

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung

1. **Erleichterung einer Transaktion:** Eine neue Transaktion wird in das Blockchain-Netzwerk eingegeben. Alle Informationen, die übertragen werden müssen, werden mit öffentlichen und privaten Schlüsseln doppelt verschlüsselt.
2. **Überprüfung der Transaktion:** Die Transaktion wird dann an das Netz der weltweit verteilten Peer-to-Peer-Computer übermittelt. Alle Knoten im Netzwerk überprüfen die Gültigkeit der Transaktion, z. B. ob ein ausreichendes Guthaben für die Durchführung der Transaktion vorhanden ist.
3. **Bildung eines neuen Blocks:** In einem typischen Blockchain-Netzwerk gibt es viele Knoten und viele Transaktionen werden gleichzeitig überprüft. Sobald die Transaktion verifiziert und als rechtmäßige Transaktion deklariert wurde, wird sie dem Mempool hinzugefügt. Alle überprüften Transaktionen eines bestimmten Knotens bilden einen Mempool, und mehrere solcher Mempools bilden einen Block.

Grundlegende Komponenten: Blöcke, kryptografisches Hashing, Dezentralisierung

6. **Konsens-Algorithmus:** Die Knoten, die einen Block bilden, versuchen, den Block dem Blockchain-Netzwerk hinzuzufügen, um ihn dauerhaft zu machen. Wenn jedoch jeder Knoten auf diese Weise Blöcke hinzufügen darf, wird das Funktionieren des Blockchain-Netzwerks gestört.
7. **Hinzufügen des neuen Blocks zur Blockchain:** Nachdem der neu erstellte Block seinen Hash-Wert erhalten hat und authentifiziert wurde, kann er nun der Blockchain hinzugefügt werden. In jedem Block gibt es einen Hash-Wert des vorherigen Blocks, und so werden die Blöcke kryptografisch miteinander verbunden, um eine Blockchain zu bilden. Ein neuer Block wird dem offenen Ende der Blockchain hinzugefügt.
8. **Transaktion abgeschlossen:** Sobald der Block zur Blockchain hinzugefügt wird, ist die Transaktion abgeschlossen und die Details dieser Transaktion werden dauerhaft in der Blockchain gespeichert. Jeder kann die Details der Transaktion abrufen und die Transaktion bestätigen.

Vergleich mit herkömmlichen Datenbanken

Herkömmliche Datenbanken sind zentralisiert, veränderbar und für die Hochgeschwindigkeitsdatenverarbeitung optimiert, während Blockchains dezentralisiert und unveränderlich sind und sich darauf konzentrieren, durch Konsensmechanismen Vertrauen und Transparenz zu schaffen. Die Wahl zwischen den beiden hängt von den spezifischen Anforderungen einer bestimmten Anwendung ab.

- *Zentralisierung vs. Dezentralisierung*
- *Datenstruktur*
- *Zugangskontrolle*
- *Konsens-Mechanismus*
- *Unveränderliche vs. veränderliche Daten*
- *Transaktionsgeschwindigkeit und Skalierbarkeit*
- *Anwendungsfälle*

Vergleich mit herkömmlichen Datenbanken

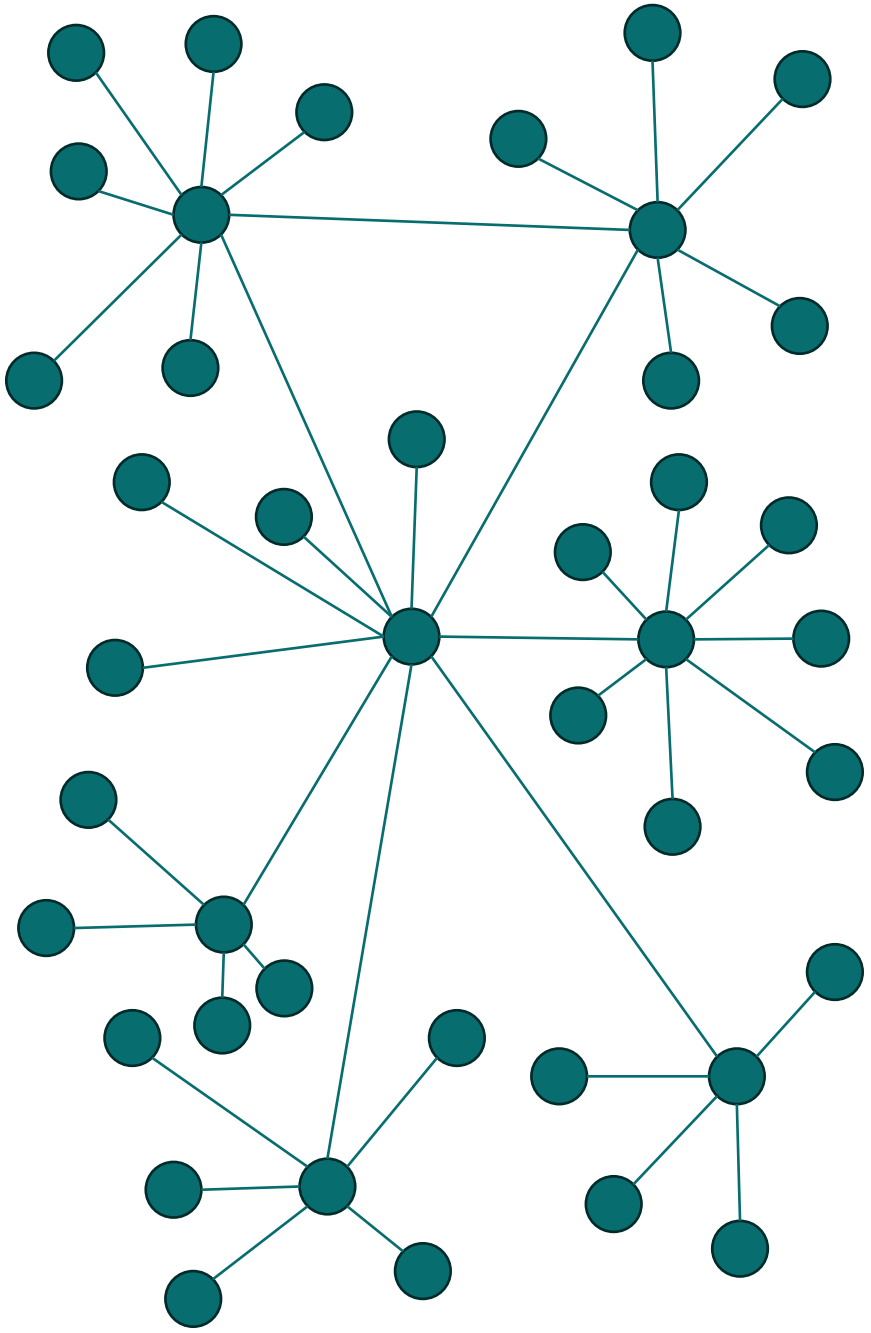
Zentralisierung vs. Dezentralisierung

Traditionelle Datenbanken: Bei herkömmlichen Datenbanken handelt es sich um zentralisierte Systeme, bei denen eine einzige Einheit (z. B. ein Unternehmen oder eine Organisation) die Kontrolle über die Datenbank hat. Sie stützen sich auf einen zentralen Server oder eine Gruppe von Servern zur Verwaltung und Speicherung von Daten.

Blockchain: Blockchains sind dezentrale Netzwerke, in denen Daten über mehrere Knoten (Computer) in einem Netzwerk verteilt sind. Es gibt keine zentrale Behörde oder einen einzigen Kontrollpunkt, was sie resistent gegen Zensur und Manipulationen macht.

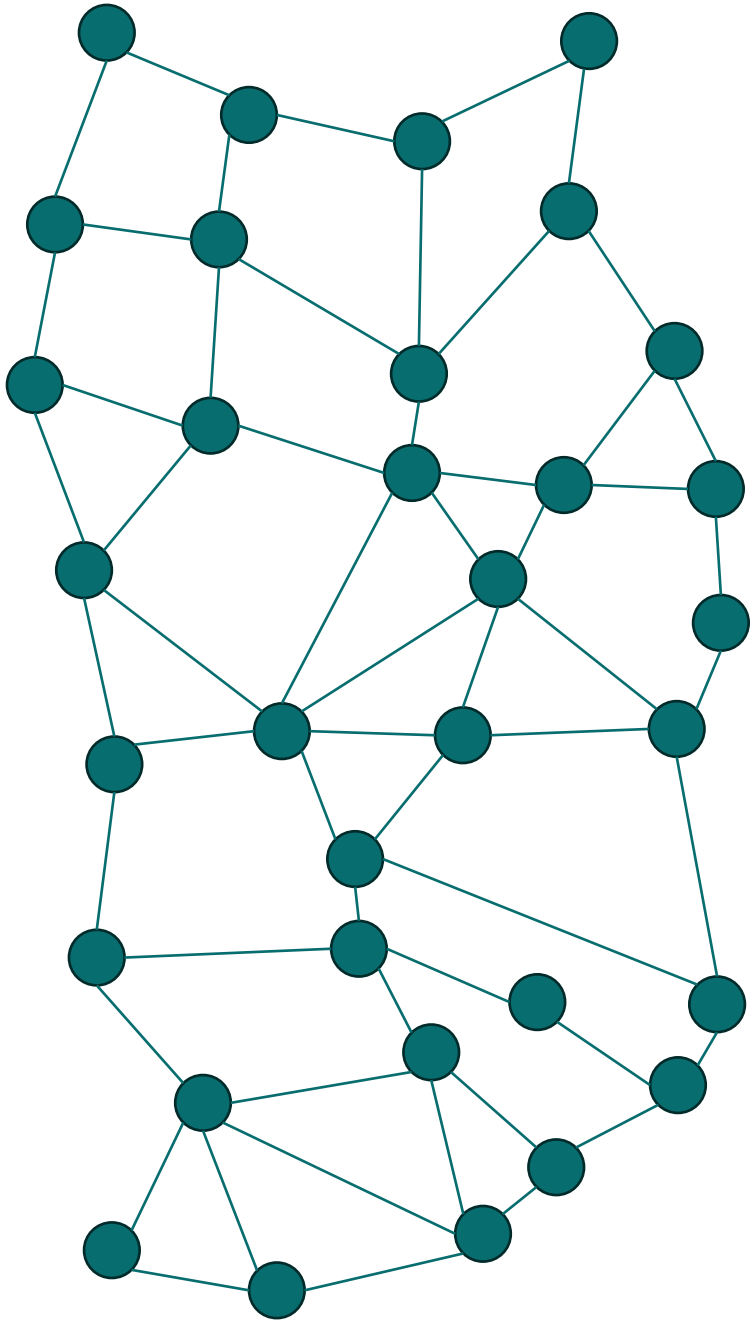
Zentralisiert

Alle Knoten sind über eine einzige Behörde verbunden.



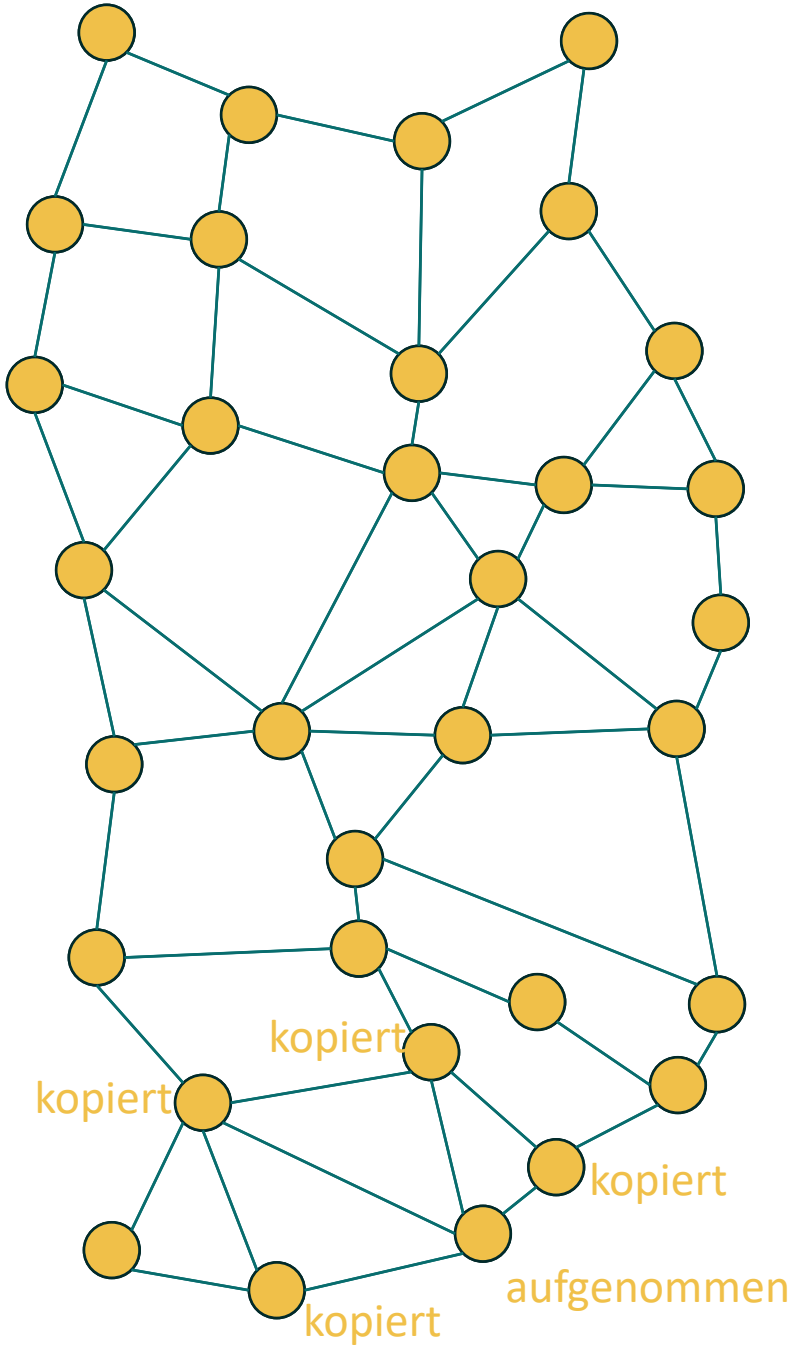
Dezentralisiert

Die Knoten werden nicht von einem einzigen Behördenserver kontrolliert, sondern haben alle eine eigene Entität.



Verteilt

Jeder Knoten ist unabhängig und untereinander vernetzt.



Transaktion im verteilten Netz

Die Transaktion wird in einem Knoten aufgezeichnet und ineinander kopiert.

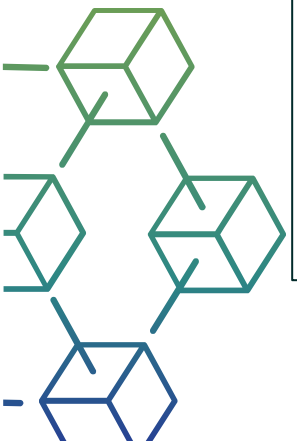
Hash-Funktion

Eine Hash-Funktion ist eine mathematische Funktion, die einen Eingabewert in einen anderen komprimierten Wert umwandelt. Die Eingabe in die Hash-Funktion kann eine beliebige Länge haben, die Ausgabe hat jedoch immer eine feste Länge.

Hash-Funktionen sind äußerst nützlich und kommen in fast allen Anwendungen der Informationssicherheit vor.

Eindeutige Ausgabe der Hash-Funktion

DATEN	HASH-FUNKTION	HASH
Die Bausteine der Blockchain.	Hash-Funktion SHA1	d355724c886c15a6272e5a8e6f416438535ca0be
Die Bausteine der Blockchain.	Hash-Funktion SHA1	54b05cb173b979447e87e3d4af19a41a774f631c
Eine Hash-Funktion ist eine mathematische Funktion, die einen Eingabewert in einen anderen komprimierten Wert umwandelt. Die Eingabe in die Hash-Funktion kann eine beliebige Länge haben, die Ausgabe hat jedoch immer eine feste Länge.	Hash-Funktion SHA1	63dd04188931586e47c899271ccdcd681b0cc357

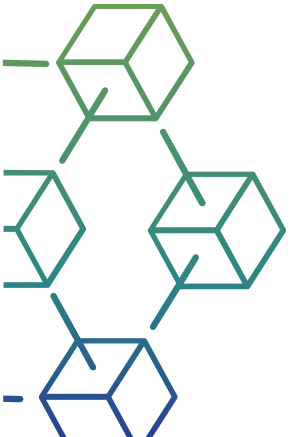


SHA1 ist in dieser Zeit nicht ausreichend

Die Bausteine der Blockchain.

Hash-Funktion
SHA3-512

33322d615333e9faa2109c35997cf144876cc75ba76059454b28c81d2fa1c286a68679a00afb
baa71e9170ffc3bdaf6fbef5035a31b4f40a354502dd985368d4

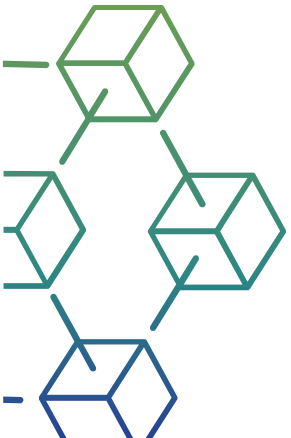


Pre-Image-Widerstand

Diese Eigenschaft bedeutet, dass es rechnerisch schwierig sein sollte, eine Hash-Funktion umzukehren.

Mit anderen Worten: Wenn eine Hash-Funktion h einen Hash-Wert z erzeugt, dann sollte es schwierig sein, einen beliebigen Eingabewert x zu finden, der zu z hasht.

Diese Eigenschaft schützt vor einem Angreifer, der nur einen Hash-Wert hat und versucht, die Eingabe zu finden.



Kollisionswiderstand

Diese Eigenschaft bedeutet, dass es schwer sein sollte, zwei verschiedene Eingaben beliebiger Länge zu finden, die denselben Hash ergeben. Diese Eigenschaft wird auch als kollisionsfreie Hash-Funktion bezeichnet.

Mit anderen Worten: Für eine Hash-Funktion h ist es schwer, zwei verschiedene Eingaben x und y zu finden, bei denen h(x) = h(y) ist.

Da eine Hash-Funktion eine komprimierende Funktion mit fester Hash-Länge ist, ist es unmöglich, dass eine Hash-Funktion keine Kollisionen hat. Diese Eigenschaft der Kollisionsfreiheit bestätigt nur, dass diese Kollisionen schwer zu finden sein sollten.

Diese Eigenschaft macht es für einen Angreifer sehr schwierig, zwei Eingabewerte mit demselben Hash zu finden.

Wenn eine Hash-Funktion kollisionssicher ist, dann ist sie auch sekundär abbildsicher.

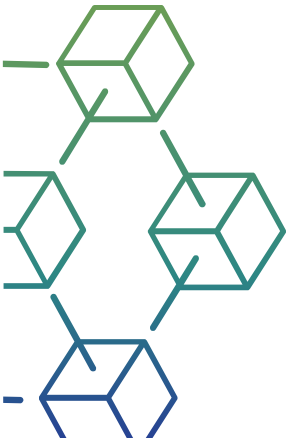
Quelle: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

Zweite Vorabbildung Widerstand

Diese Eigenschaft bedeutet, dass es bei einer Eingabe und ihrem Hashwert schwer sein sollte, eine andere Eingabe mit demselben Hashwert zu finden.

Mit anderen Worten: Wenn eine Hash-Funktion h für eine Eingabe x den Hash-Wert h(x) erzeugt, dann sollte es schwierig sein, einen anderen Eingabewert y zu finden, bei dem h(y) = h(x) ist.

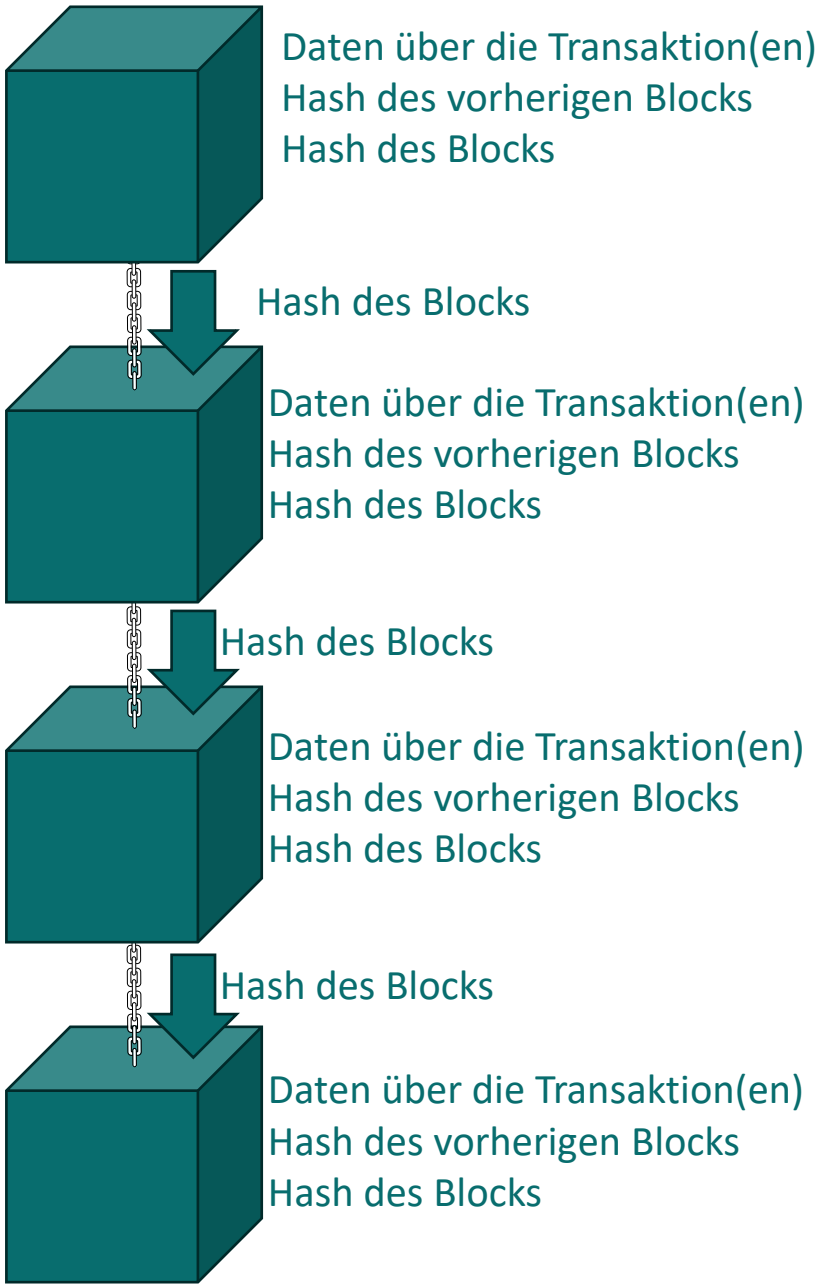
Diese Eigenschaft der Hashfunktion schützt vor einem Angreifer, der einen Eingabewert und dessen Hash hat und einen anderen Wert als legitimen Wert anstelle des ursprünglichen Eingabewertes ersetzen will.



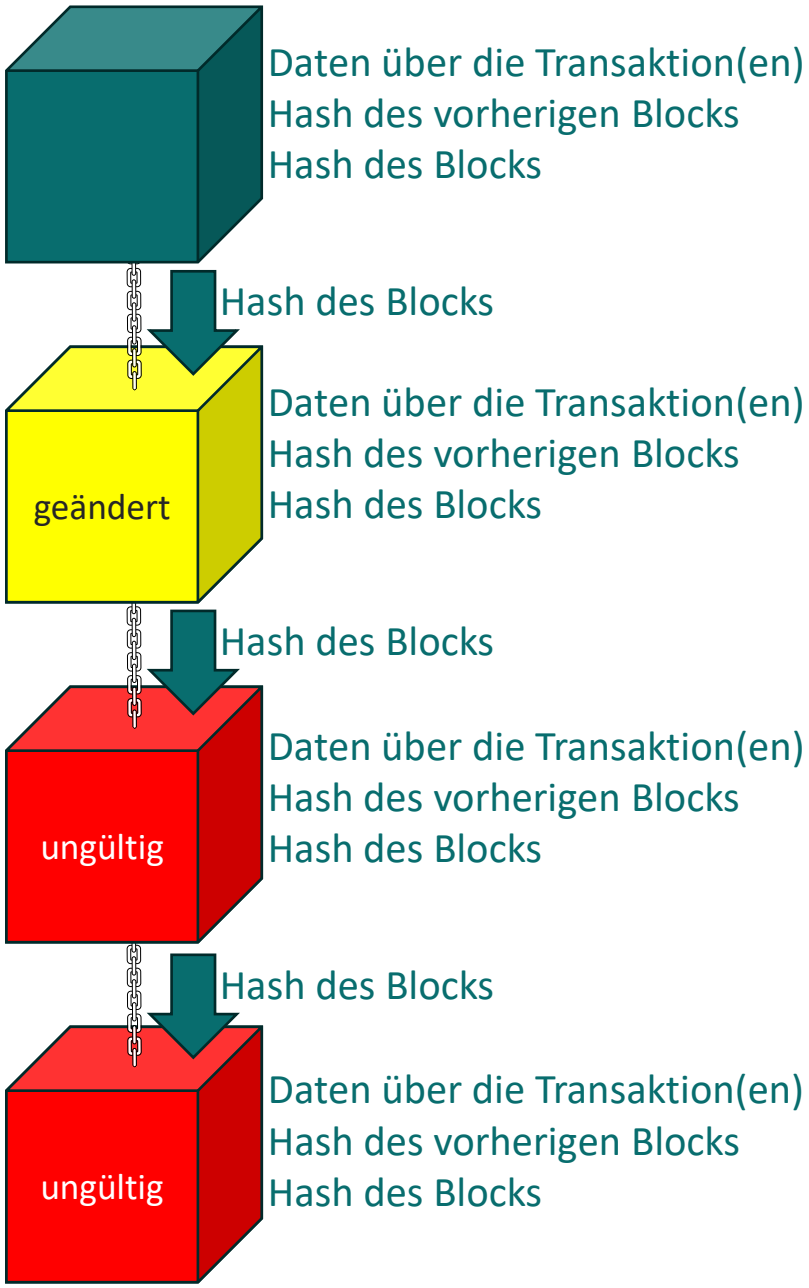
Blockchain

Block = Daten + Hash des vorherigen Blocks + Hash

Kette = Kette zwischen Blöcken

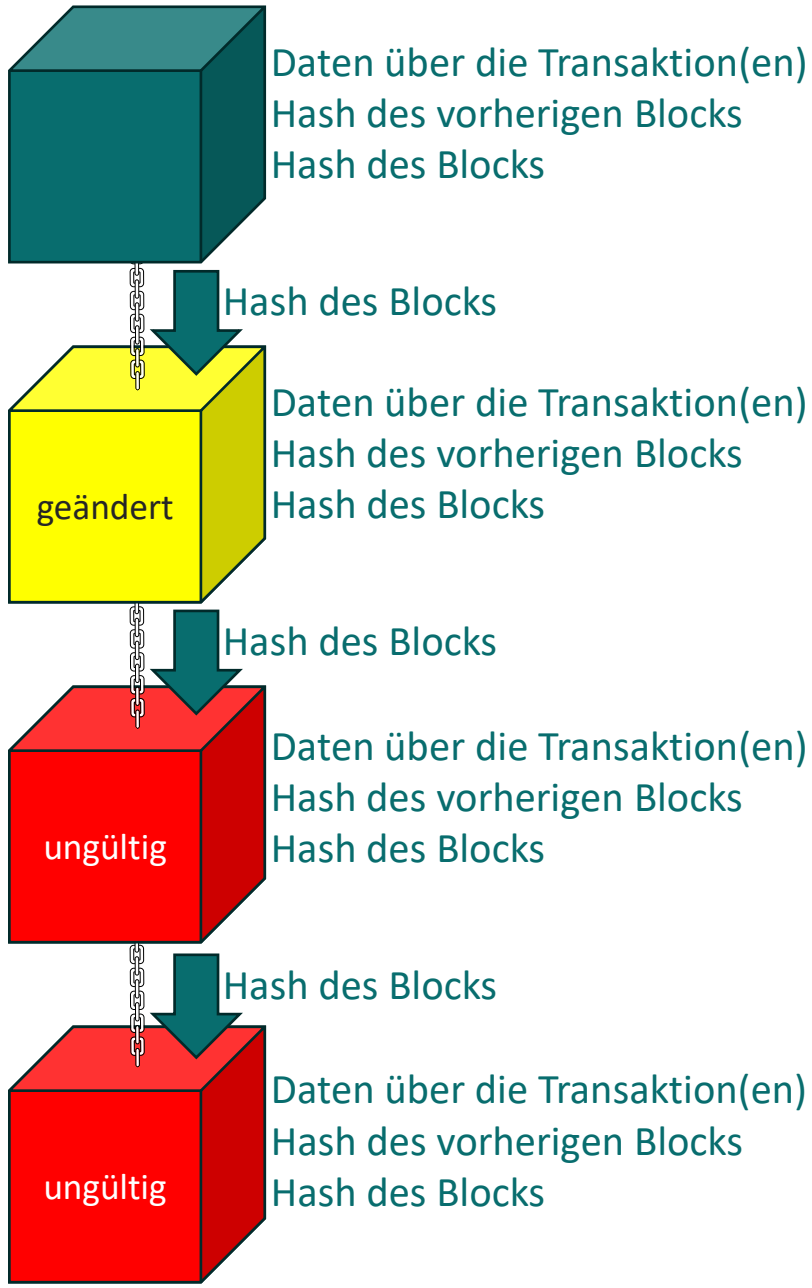


Alle Transaktionen werden in "Blöcken" aufgezeichnet.



Wenn ein Block (eine Transaktion in einem Block) geändert wird

Wert der Hash-Funktion ist unterschiedlich



Wenn ein Hacker einen Block (Daten in einem Block) ändern möchte, muss er alle folgenden Blöcke und alle Kopien von Blöcken im verteilten Netzwerk ändern

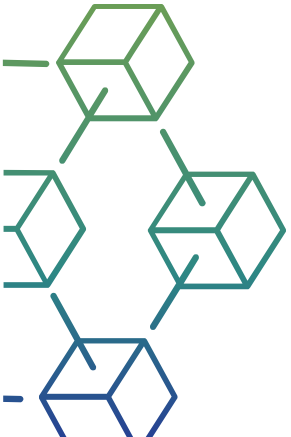
Fast unmöglich

(benötigt gigantische Rechenleistung, Strom usw.)

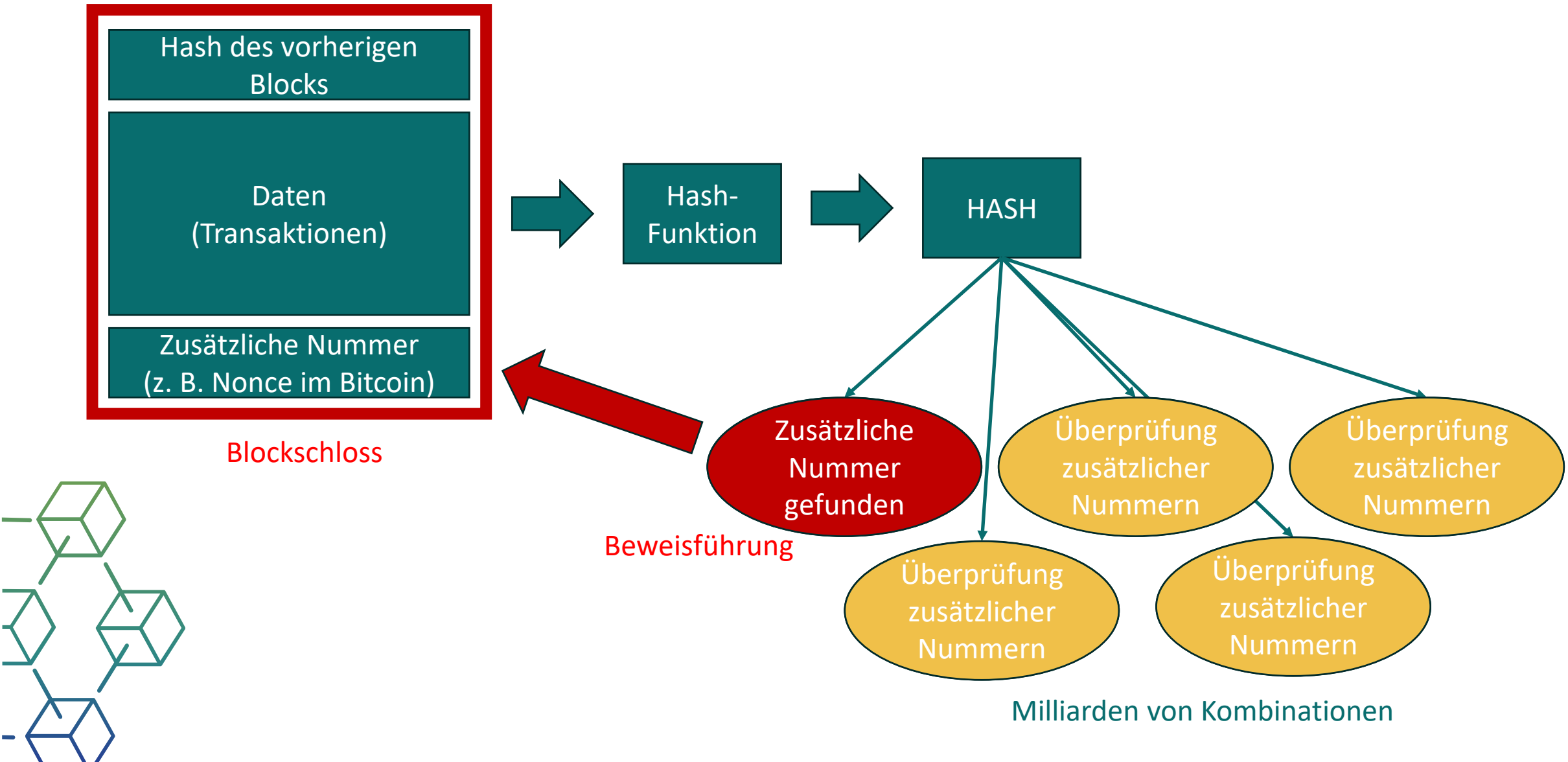
Nachweis der Arbeit

Proof of Work (PoW) ist eine Form des kryptographischen Beweises, bei dem eine Partei (der Prover) anderen (den Verifizierern) beweist, dass ein bestimmter Betrag eines bestimmten Rechenaufwands aufgewendet wurde.

Die Überprüfer können diese Ausgaben anschließend mit minimalem Aufwand bestätigen.



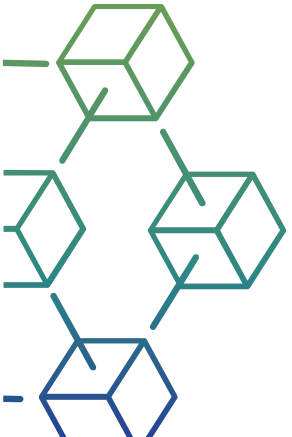
Nachweis der Arbeit



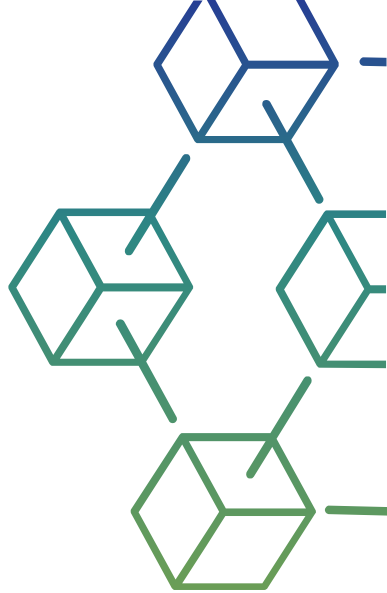
Nachweis des Einsatzes

Proof-of-Stake-Protokolle (PoS) sind eine Klasse von Konsensmechanismen für Blockchains, die durch die Auswahl von Validierern im Verhältnis zu ihrem Anteil an der zugehörigen Kryptowährung funktionieren.

Dies geschieht, um die Rechenkosten von Proof-of-Work (POW)-Systemen zu vermeiden.



Die 3 Ebenen der Blockchain



1. Blockchain 1.0: Der Ursprung der modernen Blockchain
2. Blockchain 2.0: Intelligente Verträge
3. Blockchain 3:0: Dezentralisierte Anwendung auf Unternehmensebene

Vergleich mit herkömmlichen Datenbanken

Datenstruktur

Traditionelle Datenbanken: Herkömmliche Datenbanken verwenden Tabellen, um Daten in einer strukturierten Weise zu organisieren, die normalerweise einem vordefinierten Schema folgt.

Blockchain: Blockchains verwenden eine Hauptbuchstruktur, bei der die Daten in Blöcken organisiert sind, wobei jeder Block eine Liste von Transaktionen oder Dateneinträgen enthält. Die Struktur ist in der Regel weniger starr und ermöglicht eine größere Flexibilität bei Datentypen und -formaten.

Vergleich mit herkömmlichen Datenbanken

Zugangskontrolle

Traditionelle Datenbanken: Die Zugriffskontrolle wird von einer zentralen Behörde verwaltet, und die Berechtigungen können für verschiedene Benutzer oder Rollen erteilt oder entzogen werden.

Blockchain: Die Zugangskontrolle wird häufig über kryptografische Schlüssel verwaltet. Die Nutzer haben die Kontrolle über ihre privaten Schlüssel, so dass sie mit der Blockchain interagieren können, ohne sich auf eine zentrale Behörde verlassen zu müssen. Öffentliche Blockchains sind in der Regel genehmigungsfrei, während private Blockchains unterschiedliche Stufen der Zugangskontrolle aufweisen können.

Vergleich mit herkömmlichen Datenbanken

Konsens-Mechanismus

Traditionelle Datenbanken: Herkömmliche Datenbanken stützen sich nicht auf einen Konsensmechanismus zwischen mehreren Parteien. Sie gehen davon aus, dass die in der Datenbank gespeicherten Daten korrekt sind.

Blockchain: Blockchains verwenden Konsensmechanismen (z. B. Proof of Work, Proof of Stake), um den Zustand des Ledgers zu validieren und zu vereinbaren. Dadurch wird sichergestellt, dass alle Teilnehmer des Netzwerks eine gemeinsame und vereinbarte Sicht auf die Daten haben.

Vergleich mit herkömmlichen Datenbanken

Unveränderliche vs. veränderliche Daten

Traditionelle Datenbanken: Daten in herkömmlichen Datenbanken können von autorisierten Benutzern mit den erforderlichen Berechtigungen geändert oder gelöscht werden.

Blockchain: Sobald Daten in der Blockchain gespeichert sind, sind sie in der Regel unveränderlich und resistent gegen Änderungen. Diese Unveränderlichkeit ist ein Kernmerkmal der Blockchain-Technologie.

Vergleich mit herkömmlichen Datenbanken

Transaktionsgeschwindigkeit und Skalierbarkeit

Traditionelle Datenbanken: Herkömmliche Datenbanken sind oft für hohe Transaktionsgeschwindigkeiten optimiert und können durch Hinzufügen weiterer Server oder Ressourcen leicht skaliert werden.

Blockchain: Öffentliche Blockchains, insbesondere solche, die Proof of Work verwenden, können langsamere Transaktionsverarbeitungsgeschwindigkeiten und Skalierbarkeitsprobleme aufweisen. Es werden jedoch verschiedene Lösungen und Technologien entwickelt, um die Skalierbarkeit von Blockchains zu verbessern.

Vergleich mit herkömmlichen Datenbanken

Anwendungsfälle

Herkömmliche Datenbanken: Herkömmliche Datenbanken eignen sich gut für Anwendungen, die einen hohen Durchsatz, eine geringe Latenzzeit und eine zentrale Steuerung erfordern, wie z. B. Banksysteme und E-Commerce-Plattformen.

Blockchain: Blockchains eignen sich am besten für Anwendungen, die Dezentralisierung, Vertrauen, Transparenz und Sicherheit erfordern, wie z. B. Kryptowährungen, Lieferkettenverfolgung, Wahlsysteme und intelligente Verträge.

03

Was sind die wichtigsten Komponenten der Blockchain-Technologie?

Was sind die wichtigsten Komponenten der Blockchain-Technologie?

Die Blockchain-Architektur besteht aus den folgenden Hauptkomponenten:

1. **Ein verteiltes Hauptbuch**
2. **Intelligente Verträge**
3. **Kryptographie mit öffentlichem Schlüssel**

Was sind die wichtigsten Komponenten der Blockchain-Technologie?

1. Ein verteiltes Hauptbuch

Ein verteiltes Hauptbuch ist die gemeinsame Datenbank im Blockchain-Netzwerk, in der die Transaktionen gespeichert werden, z. B. eine gemeinsame Datei, die jeder im Team bearbeiten kann. In den meisten gemeinsam genutzten Texteditoren kann jeder, der über Bearbeitungsrechte verfügt, die gesamte Datei löschen. Bei Distributed-Ledger-Technologien gibt es jedoch strenge Regeln dafür, wer die Datei bearbeiten darf und wie sie bearbeitet wird. Einmal aufgezeichnete Einträge können nicht mehr gelöscht werden.

Was sind die wichtigsten Komponenten der Blockchain-Technologie?

2. Intelligente Verträge

Unternehmen nutzen Smart Contracts, um Geschäftsverträge selbst zu verwalten, ohne dass eine unterstützende Drittpartei erforderlich ist. Dabei handelt es sich um Programme, die auf dem Blockchain-System gespeichert sind und automatisch ausgeführt werden, wenn bestimmte Bedingungen erfüllt sind. Sie führen Wenn-Dann-Prüfungen durch, damit Transaktionen sicher abgeschlossen werden können. Ein Logistikunternehmen kann zum Beispiel einen intelligenten Vertrag haben, der automatisch die Zahlung vornimmt, sobald die Waren im Hafen angekommen sind.

Was sind die wichtigsten Komponenten der Blockchain-Technologie?

3. Kryptographie mit öffentlichem Schlüssel

Die Public-Key-Kryptografie ist ein Sicherheitsmerkmal zur eindeutigen Identifizierung der Teilnehmer im Blockchain-Netzwerk. Dieser Mechanismus generiert zwei Sätze von Schlüsseln für Netzwerkmitglieder. Ein Schlüssel ist ein öffentlicher Schlüssel, der für alle Mitglieder des Netzwerks gilt. Der andere ist ein privater Schlüssel, der für jedes Mitglied einzigartig ist. Der private und der öffentliche Schlüssel arbeiten zusammen, um die Daten im Hauptbuch zu entsperren.

Was sind die wichtigsten Komponenten der Blockchain-Technologie?

3. Kryptographie mit öffentlichem Schlüssel

Ein Beispiel: John und Jill sind zwei Mitglieder des Netzes. John zeichnet eine Transaktion auf, die mit seinem privaten Schlüssel verschlüsselt ist. Jill kann sie mit ihrem öffentlichen Schlüssel entschlüsseln. Auf diese Weise ist Jill sicher, dass John die Transaktion durchgeführt hat. Jills öffentlicher Schlüssel hätte nicht funktioniert, wenn Johns privater Schlüssel verfälscht worden wäre.

04

Was sind die Vorteile der Blockchain-Technologie?

Was sind die Vorteile der Blockchain-Technologie?

Die Blockchain-Technologie bietet viele Vorteile für die Verwaltung von Vermögenstransaktionen. In den folgenden Unterabschnitten führen wir einige davon auf:

1. **Erweiterte Sicherheit**
2. **Verbesserte Effizienz**
3. **Schnelleres Auditing**

Was sind die Vorteile der Blockchain-Technologie?

1. Erweiterte Sicherheit

Blockchain-Systeme bieten das hohe Maß an Sicherheit und Vertrauen, das moderne digitale Transaktionen erfordern. Es besteht immer die Befürchtung, dass jemand die zugrunde liegende Software manipuliert, um für sich selbst Falschgeld zu erzeugen. Blockchain nutzt jedoch die drei Prinzipien Kryptografie, Dezentralisierung und Konsens, um ein hochsicheres zugrunde liegendes Softwaresystem zu schaffen, das nahezu unmöglich zu manipulieren ist. Es gibt keinen einzigen Fehlerpunkt und ein einzelner Benutzer kann die Transaktionsaufzeichnungen nicht ändern.

Was sind die Vorteile der Blockchain-Technologie?

2. Verbesserte Effizienz

Business-to-Business-Transaktionen können viel Zeit in Anspruch nehmen und zu betrieblichen Engpässen führen, vor allem, wenn die Einhaltung von Vorschriften und die Regulierungsbehörden Dritter beteiligt sind. Transparenz und intelligente Verträge in der Blockchain machen solche Geschäftstransaktionen schneller und effizienter.

05

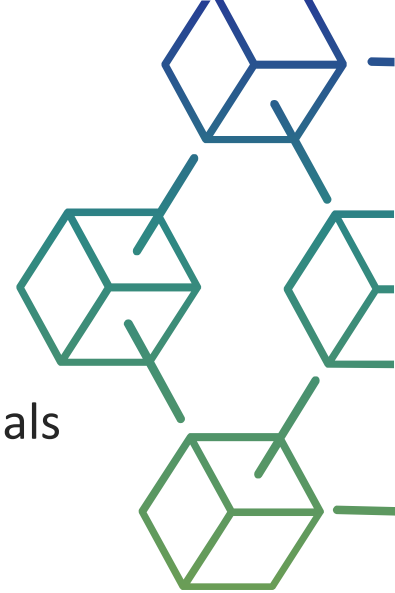
Was ist der Unterschied zwischen einer Datenbank und einer Blockchain?

Was sind die Vorteile der Blockchain-Technologie?

3. Schnelleres Auditing

Unternehmen müssen in der Lage sein, elektronische Transaktionen sicher zu erzeugen, auszutauschen, zu archivieren und nachprüfbar zu rekonstruieren. Blockchain-Datensätze sind chronologisch unveränderlich, was bedeutet, dass alle Datensätze immer zeitlich geordnet sind. Diese Datentransparenz beschleunigt die Audit-Verarbeitung erheblich.

Was ist der Unterschied zwischen einer Datenbank und einer Blockchain?



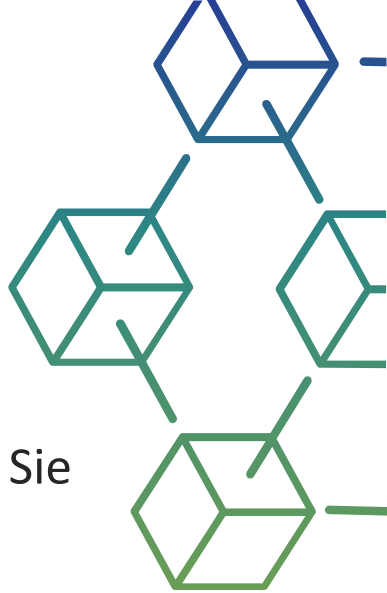
Blockchain ist eine besondere Art von Datenbankmanagementsystem, das mehr Funktionen als eine normale Datenbank hat. In der folgenden Liste beschreiben wir einige wesentliche Unterschiede zwischen einer herkömmlichen Datenbank und einer Blockchain:

- Blockchains dezentralisieren die Kontrolle, ohne das Vertrauen in die vorhandenen Daten zu beschädigen. Dies ist bei anderen Datenbanksystemen nicht möglich.
- Die an einer Transaktion beteiligten Unternehmen können nicht ihre gesamte Datenbank gemeinsam nutzen. In Blockchain-Netzwerken hat jedoch jedes Unternehmen seine Kopie des Hauptbuchs, und das System sorgt automatisch für die Konsistenz zwischen den beiden Hauptbüchern.
- Während man in den meisten Datenbanksystemen Daten bearbeiten oder löschen kann, kann man in der Blockchain nur Daten einfügen.

06

Wie unterscheidet sich die Blockchain von der Cloud?

Wie unterscheidet sich die Blockchain von der Cloud?



Der Begriff Cloud bezieht sich auf Computerdienste, auf die online zugegriffen werden kann. Sie können über die Cloud auf Software as a Service (SaaS), Product as a Service (PaaS) und Infrastructure as a Service (IaaS) zugreifen.

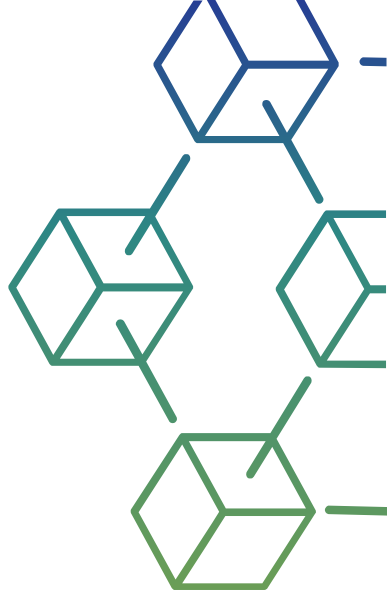
Cloud-Anbieter verwalten ihre Hardware und Infrastruktur und bieten Ihnen über das Internet Zugang zu diesen Datenverarbeitungsressourcen. Sie bieten viel mehr Ressourcen als nur Datenbankmanagement.

Wenn Sie einem öffentlichen Blockchain-Netzwerk beitreten möchten, müssen Sie Ihre Hardware-Ressourcen zur Verfügung stellen, um Ihre Ledger-Kopie zu speichern. Sie können zu diesem Zweck auch einen Server aus der Cloud verwenden. Einige Cloud-Anbieter bieten auch komplette Blockchain-as-a-Service (BaaS) aus der Cloud an.

07

Was ist Blockchain als Dienstleistung?

Was ist Blockchain als Dienstleistung?



Blockchain as a Service (BaaS) ist ein verwalteter Blockchain-Dienst, der von einem Drittanbieter in der Cloud bereitgestellt wird. Sie können Blockchain-Anwendungen und digitale Dienste entwickeln, während der Cloud-Anbieter die Infrastruktur und die Blockchain-Aufbauwerkzeuge bereitstellt.

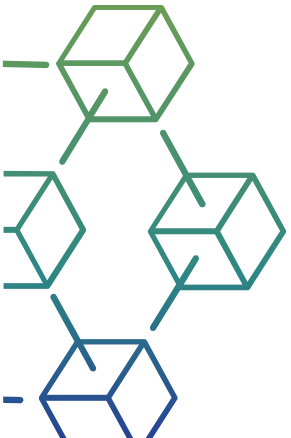
Alles, was Sie tun müssen, ist, die bestehende Blockchain-Technologie anzupassen, was die Einführung der Blockchain schneller und effizienter macht.

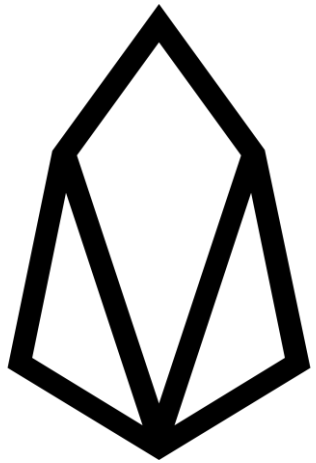
08

Anwendungsfall

Kryptowährung - die erste weit verbreitete Blockchain

- Moderne Kryptowährungen nutzen Blockchain
  - Bitcoin
  - Litecoin
  - Ethereum
  - XRP
  - EOS
  - NEO
  - Stellar
  - Monero
  - Gedankenstrich



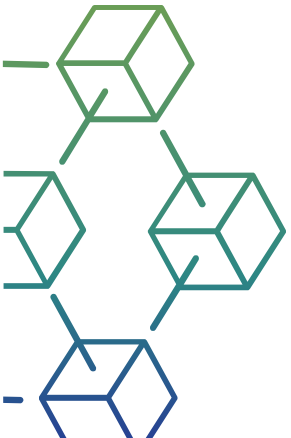


09

Schlussfolgerung

Schlussfolgerung

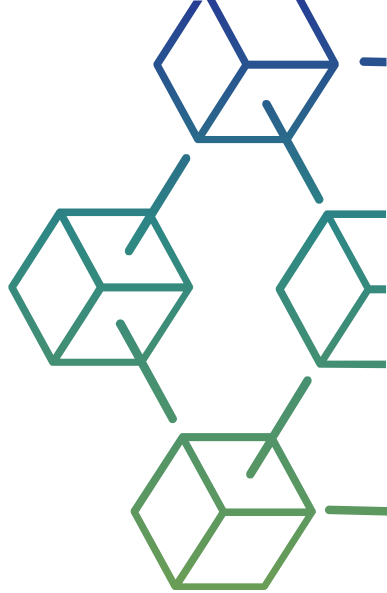
Die Blockchain-Technologie ist ein fortschrittlicher Datenbankmechanismus, der einen transparenten Informationsaustausch innerhalb eines Unternehmensnetzes ermöglicht. Die Blockchain besteht aus einer Kette von Blöcken, wobei jeder Block eine Liste von Transaktionen und eine eindeutige Kennung (Hash) des vorherigen Blocks enthält. Dadurch wird die Integrität der Daten gewährleistet. Blockchains sind dezentralisierte Netzwerke, bei denen die Daten über mehrere Knoten (Computer) in einem Netzwerk verteilt sind. Es gibt keine zentrale Behörde oder einen einzigen Kontrollpunkt, was sie resistent gegen Zensur und Manipulationen macht. Die Blockchain ist auf Tausenden von Computern (Knoten) auf der ganzen Welt gespeichert. Jeder Knoten hat eine Kopie der gesamten Blockchain, was ihre Widerstandsfähigkeit gegen Ausfälle und Angriffe erhöht.



Video

- Wie funktioniert eine Blockchain - einfach erklärt [6:00]
- Blockchain in 7 Minuten [7:03]
- Blockchain Erklärt [10:23]
- Was ist eine Blockchain? (Animiert + Beispiele) [8:27]
- Blockchain-Technologie erklärt (2-Stunden-Kurs) [1:54:53]
- Blockchain-Grundlagen & Kryptographie [1:17:37]

Links



- BlockChain-Prinzipien, Typ & Anwendung & Warum sollten Sie sich dafür interessieren?
- Gestaltungsprinzipien für Blockchain
- Grundsätze von Blockchains
- Grundsätze erfolgreicher Blockchain-Implementierungen
- Grundlegende Sicherheit der Blockchain
- Blockchain-Design - Entdecken Sie die Blockchain-Prinzipien
- Blockchain-Technologie: Prinzipien und Anwendung in der medizinischen Bildgebung

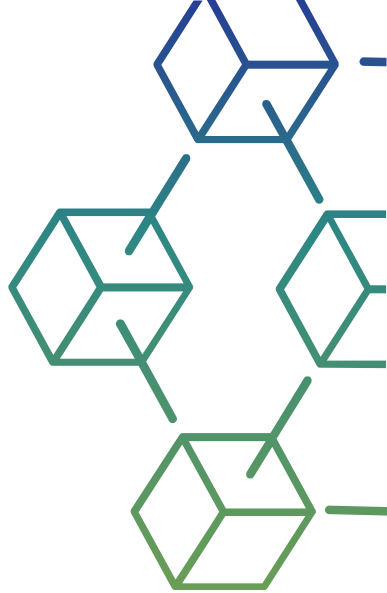
10

Interaktive Lernaktivität

5 Blöcke unter Blockchain erstellen

1. Online-Tool für Rauten verwenden
   https://emn178.github.io/online-tools/sha256.html
2. SHA256 verwenden und Hashes von 5 Blöcken erstellen - Inhalt auf der nächsten Folie

5 Blöcke unter Blockchain erstellen



1. 1st Blockinhalt:
   2023-01-01T10:34:12+1,Jonh Newman,Jane Newman,236.23,EUR
   e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

2. 2nd Blockinhalt:
   2023-01-01T10:35:28+1,Steve Johnson,Richard McCay,100.00,EUR
   Hash von der Hash-Funktion des Blocks 1st verwenden

3. 3rd Blockinhalt:
   2023-01-01T10:35:33+1,Charles Tann,Elisabeth Bronson,100.00,EUR
   Hash von der Hash-Funktion des Blocks 3rd verwenden

4. 4th Blockinhalt:
   2023-01-01T10:35:59+1,Roger Blackburn,Lisa Tann,50.00,EUR
   Hash von der Hash-Funktion des Blocks 3rd verwenden

5. 5th Blockinhalt:
   2023-01-01T10:36:01+1,Richard Moss,Edward Morris,85.00,EUR
   Hash von der Hash-Funktion des Blocks 4th verwenden

Versuchen Sie es:

1. Nehmen Sie dieselben kleinen Änderungen im Block 2nd vor und vergleichen Sie die neuen Hashes
2. Andere Hash-Funktion verwenden - Menü oben - Hash
    1. SHA1
    2. SHA2-512
    3. SHA3
    4. ...
3. Verwenden Sie den Inhalt Ihres Blocks für die Funktion hat

11

Quiz

Quiz

1. Was ist eine der wichtigsten Anforderungen an eine sichere Hash-Funktion?
   a) Kollisionssicherheit
   b) Redundanz
   c) Vorhersehbarkeit
   d) Linearität

Quiz

2. Was ist ein Merkmal einer zentralisierten Datenbankarchitektur?

   a) Eine einzige Kontroll- und Autoritätsstelle

   b) Verteilte Datenspeicherung über mehrere Knotenpunkte

   c) Autonome Entscheidungsfindung durch jeden Knoten

   d) Hohe Widerstandsfähigkeit gegen Zensur und Manipulationen

Quiz

3. Was ist ein Hauptmerkmal einer dezentralen Datenbankarchitektur?

   a) Mehr "zentrale" Knotenpunkte

   b) Eine einzige Kontroll- und Autoritätsstelle

   c) Zentralisierte Entscheidungsfindung durch einen bestimmten Knotenpunkt

   d) Geringe Redundanz und Fehlertoleranz

Quiz

4. Was ist ein charakteristisches Merkmal eines verteilten Datenbanksystems?

   a) Daten werden über mehrere Knotenpunkte in einem Netzwerk gespeichert

   b) Zentralisierte Kontrolle und Autorität über die gesamte Datenbank

   c) Fehlende Redundanz für mehr Leistung

   d) Begrenzte Skalierbarkeit aufgrund einer Single-Node-Architektur

Quiz

5. Was beschreibt einen Hash im Kontext der Informatik und Kryptographie am besten?

   a) Eine von einer Hash-Funktion erzeugte Ausgabe fester Größe, die die eindeutige digitale Signatur von Eingabedaten darstellt

   b) Eine Zeichenkette mit variabler Länge, die für die Datenspeicherung in Datenbanken verwendet wird

   c) Ein Programmierkonstrukt zur Optimierung des Datenabrufs in Algorithmen

   d) Ein Echtzeit-Verschlüsselungsverfahren zur Sicherung von Kommunikationskanälen

Quiz

6. Welche Komponente ist für die chronologische und unveränderliche Aufzeichnung von Transaktionen in einer Blockchain verantwortlich?

   a) Block

   b) Knotenpunkt

   c) Intelligenter Vertrag

   d) Konsens-Algorithmus

Quiz

7. Was ist der Hauptunterschied zwischen einer Blockchain und einer herkömmlichen Datenbank?

   a) Blockchain bietet eine dezentralisierte und verteilte Kontrolle, während herkömmliche Datenbanken in der Regel zentralisiert sind

   b) Herkömmliche Datenbanken bieten eine schnellere Transaktionsverarbeitung im Vergleich zur langsameren Natur der Blockchain

   c) Blockchain beruht auf einem einzigen Kontrollpunkt, während herkömmliche Datenbanken ein verteiltes Netzwerk für die Kontrolle nutzen

   d) Herkömmliche Datenbanken sind von Natur aus resistent gegen Manipulationen, während die Blockchain anfälliger für Datenmanipulationen ist.

Quiz

8. Wo wurde die Blockchain-Technologie zuerst eingeführt?

   a) Finanzen und Kryptowährungen

   b) Gesundheitswesen und medizinische Aufzeichnungen

   c) Soziale Medien und Networking

   d) E-Commerce und Online-Handel

https://blockchainforagrifood.eu/

Dankeschön

Haben Sie Fragen?

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.