GENERATION BLOCKCHAIN

Master-Studiengang
Einführung in Blockchain-Technologie & Kryptowährungen

www.generationblockchain.eu

2022-2024
OERS

Von
Frankfurt School of Finance & Management

Co-funded by the European Union

Inhalt

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

01 | EINFÜHRUNG IN DEN KURS

Willkommen zum Kurs Blockchain-Technologie & Kryptowährungen

Bevor Sie sich mit dem Inhalt des Kurses befassen, empfehlen wir Ihnen dringend, den Lehrplan zu lesen. Im Lehrplan finden Sie die wichtigsten Informationen zum Kurs, darunter:

- Überblick über den Kurs
- Kursvoraussetzungen und Dauer
- Kurs-Lernziele und Lehrplanübersicht
- Zeitplan für den Kurs
- Benotung und Kursabschluss
- Informationen über das ERASMUS+ Projekt "Generation Blockchain"

Über das ERASMUS-Projekt "Generation Blockchain"

Das ERASMUS+ Projekt "Generation Blockchain" zielt darauf ab, zur Verbesserung des digitalen Lernens und Lehrens in Hochschuleinrichtungen und zur Entwicklung fortgeschrittener studentischer Fähigkeiten beizutragen, damit sie besser darauf vorbereitet sind, zur digitalen Transformation der Gesellschaft beizutragen. Dieses Projekt ist eine Zusammenarbeit zwischen der Universität Szczecin in Polen, dem Frankfurt School Blockchain Center in Deutschland, Momentum Educate+Innovate in Irland, der Amsterdam University of Applied Sciences in den Niederlanden, dem European E-Learning Institute in Dänemark und der Universität Porto in Portugal.

Dieser Kurs wurde mit Unterstützung der Europäischen Kommission im Rahmen des Programms Erasmus+ finanziert. Die Verantwortung für den Inhalt dieses Kurses tragen allein die Projektpartner; die Kommission und die Nationale Agentur für das Programm Erasmus+ haften nicht für die weitere Verwendung der darin enthaltenen Angaben.

01

MODUL 1

Einführung in Blockchain-Technologie und Kryptowährungen

Co-funded by the European Union

Finanziert von der Europäischen Union. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die des Autors/der Autoren und spiegeln nicht unbedingt die der Europäischen Union oder der Nationalen Agentur wider. Weder die Europäische Union noch die Nationale Agentur können für sie verantwortlich gemacht werden.

Inhalt Modul 1

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

01| MODUL 1 Einführung in die Blockchain-Technologie

Kapitel Überblick

In diesem Modul werden wir einen kurzen Überblick über die Geschichte der Distributed-Ledger-Technologien, insbesondere der Blockchain-Technologie, und deren Aufbau (d. h. Kryptografie, Blockstruktur, Mining und Konsens) geben. Diese Grundlage wird es Ihnen ermöglichen, die Blockchain-Technologie zu verstehen und sie erleichtert die Nutzung aktueller Internetprotokolle, während sie gleichzeitig verbessert und ergänzt wird. Darüber hinaus werden wir uns mit der Geschichte des Geldes und insbesondere mit Bitcoin als der ersten Anwendung der Blockchain-Technologie beschäftigen. Als Bezugspunkt werden wir uns die Merkmale der Bitcoin-Blockchain ansehen, insbesondere ihr Peer-to-Peer-Netzwerk, das die Speicherung von Transaktionen ermöglicht, Transparenz und Unveränderlichkeit sowie verschiedene Konsensmechanismen bietet.

Lernziele

Nach dem ersten Modul sollten Sie dazu in der Lage sein:

- Erklären Sie den Unterschied zwischen der Blockchain-Technologie und der Distributed-Ledger-Technologie (DLT).
- Diskutieren Sie über Blockchain-Technologien und Formen des Geldes.
- Erklären Sie den Unterschied zwischen Blockchain und der Kryptowährung Bitcoin.
- Erklären Sie, wie die Bitcoin-Blockchain funktioniert.
- Erörtern Sie die Merkmale der Blockchain.
- Erklären Sie Blockchain-Komponenten wie Mining und Konsens.
- Erklären Sie, woraus ein Block in einer Blockchain besteht.
- Erklären Sie, wie Transaktionen auf einer Blockchain funktionieren.
- Diskutieren Sie die Vor- und Nachteile der Konsensmechanismen Proof-of-Work und Proof-of-Stake.
- Erklären Sie die drei Hauptfunktionen von Geld.

01| EINFÜHRUNG IN DLTS & BLOCKCHAIN-TECHNOLOGIE

Einführung in Modul 1

Um die Grundlagen für diesen Kurs zu schaffen, werden wir Ihnen zunächst die Distributed Ledger Technology (DLT) und Blockchain als eine ihrer Unterkategorien vorstellen.

1.1 Was ist die Blockchain-Technologie?

Grundsätzlich ist die Blockchain-Technologie eine Datenbankstruktur, die auf dem Prinzip eines dezentralen, unveränderlichen und transparenten digitalen Transaktionsbuchs beruht. Mit ihr lassen sich Vermögenswerte und Informationen in verschiedenen Formen verwalten, speichern und übertragen. Das Wort Blockchain bezieht sich auf ihre Datenbankstruktur. Jede Transaktion wird in Form eines Datenblocks zusammen mit anderen für die Validierung der Transaktion erforderlichen Daten aufgezeichnet. Auf die Einzelheiten der Transaktionsdaten wird später in Modul 1 eingegangen. Jeder Block ist kryptografisch mit dem vorangehenden und nachfolgenden Block verbunden. Dementsprechend bestätigt jeder Block seinen Platz in der Abfolge der Transaktionen. Durch die Transaktionen und die Speicherung von Daten bilden diese Blöcke eine Kette von Daten - die Blockchain.

Eine Blockchain ist ein digitales Hauptbuch (auch Ledger genannt), das von einem verteilten öffentlichen Computernetz kontrolliert wird. Es wird zwischen öffentlichen und privaten Blockchains unterschieden. Im weiteren Sinne bezieht sich ein Hauptbuch auf einen Informationsspeicher, der Aufzeichnungen über Transaktionen enthält, die endgültig, endgültig und unveränderlich sein sollen. Ein verteiltes Ledger wird nicht zentral gespeichert, sondern das Ledger wird auf vielen verschiedenen Computern (sogenannten Nodes) gespeichert und aktualisiert. Ein verteiltes Hauptbuch (Distributed Ledger) als spezifische Kalibrierung eines Hauptbuchs ist ein Hauptbuch, das von einer Reihe von DLT-Knoten (Distributed Ledger Technology) gemeinsam genutzt und zwischen den DLT-Knoten mit Hilfe eines Konsensmechanismus synchronisiert wird, der so konzipiert ist, dass er fälschungssicher ist, nur Anhänge enthält und unveränderlich ist und bestätigte und validierte Transaktionen oder Informationen enthält.

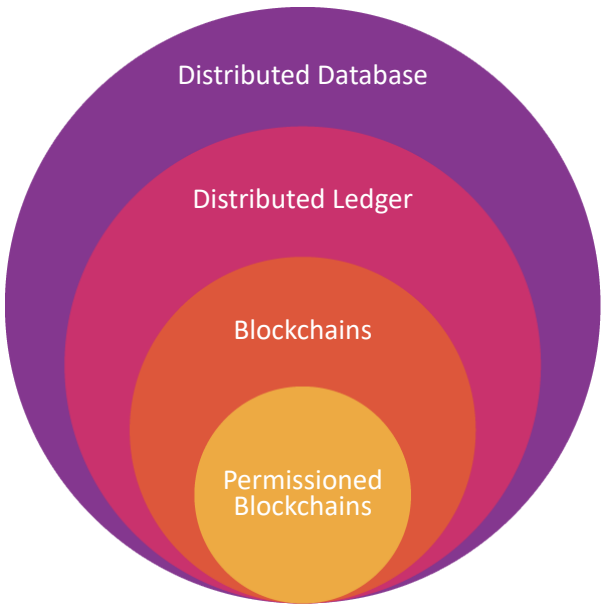
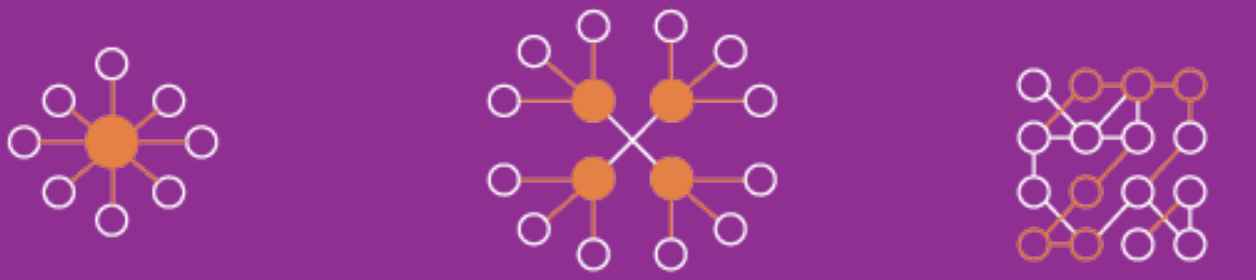


Abbildung 1: Beziehung zwischen verteilten Ledgern und Blockchains

1.2 Verschiedene Arten von Blockchain-Netzwerken

Blockchain-Systeme können zentralisierte, dezentralisierte oder verteilte Netzwerksysteme sein.



Zentralisiertes Netzwerk

Alle Knotenpunkte sind unter einer einzigen Autorität verbunden

Dezentrales Netzwerk

Keine einzige Autorität kontrolliert die Knotenpunkte

Verteiltes Netzwerk

Jeder Knoten ist unabhängig und miteinander verbunden

Abbildung 2: Blockchain-Netzwerkarchitektur

Im Rahmen dieser ersten Unterscheidung gibt es vier Haupttypen von dezentralen oder verteilten Netzwerken in der Blockchain: öffentliche Blockchain-Netzwerke, private Blockchain-Netzwerke, hybride Blockchain-Netzwerke und Konsortial-Blockchain-Netzwerke.

1

Öffentliche Blockchain-Netzwerke

Öffentliche Blockchain-Netze erfordern keine zentrale Behörde, die die Teilnahme genehmigt. Ein öffentliches Blockchain-Netzwerk schränkt standardmäßig den Zugang für keinen Nutzer ein. Diese Gleichheit ist auch im Recht aller Teilnehmer zum Lesen, Bearbeiten und Validieren der Blockchain gegeben. Beispiele für öffentliche Blockchain-Netzwerke sind Bitcoin, Ethereum und Litecoin.

2

Private Blockchain-Netzwerke

In einem privaten Blockchain-Netzwerk kontrolliert eine einzelne Organisation oder Institution private Blockchains, die auch als verwaltete Blockchains bezeichnet werden. Die Behörde, die die private Blockchain betreibt, legt fest, welche Teilnehmer Rechte wie Zugang und Abstimmung haben. Dezentralisierung ist bei privaten Blockchains nur bis zu einem gewissen Grad möglich, da sie Zugangsbeschränkungen haben. Ein Beispiel für ein privates Blockchain-Netzwerk ist Ripple, ein Netzwerk zum Austausch digitaler Währungen für Unternehmen.

3

Hybride Blockchain-Netzwerke

Hybride Blockchain-Netzwerke kombinieren Aspekte von privaten und öffentlichen Blockchain-Netzwerken. Ein Anwendungsfall für hybride Blockchains ist das Bankwesen, bei dem die zentrale Institution der Öffentlichkeit Zugang zu digitaler Währung gewähren kann, die bankeigene Währung aber gleichzeitig privat bleibt. Auf diese Weise ist ein Teil der in der Kette gespeicherten Daten öffentlich zugänglich, während ein Teil der Daten durch eine Zugangskontrolle eingeschränkt ist.

4

Konsortium Blockchain-Netzwerke

In einem Konsortial-Blockchain-Netzwerk gibt es eine Gruppe ausgewählter Organisationen, die Zugriffs-, Lese- und Bearbeitungsrechte festlegen können. Dieser Aufbau wird häufig in Branchen verwendet, in denen mehrere Organisationen gemeinsame Ziele haben und von der gemeinsamen Verantwortung für Waren, Daten oder Vermögenswerte profitieren. Das Global Shipping Business Network Consortium zum Beispiel digitalisiert die Schifffahrtsbranche und fördert die Zusammenarbeit zwischen den Akteuren der maritimen Industrie.

1.3 Merkmale der Blockchain-Technologie

Die Blockchain-Technologie hat in der Regel die Form einer dezentralen Datenbankstruktur oder eines digitalen Registers, das Transaktionen transparent aufzeichnet und als Grundlage für viele digitale Währungen dient. Die besonderen Merkmale der Blockchain-Technologie sind Dezentralisierung, Unveränderlichkeit und Transparenz. Es handelt sich letztlich um ein offen einsehbares Hauptbuch, das alle Transaktionen transparent dokumentiert. In der Regel wird ein solches Hauptbuch nicht zentral gespeichert, sondern auf vielen verschiedenen Computern oder Knotenpunkten abgelegt und aktualisiert. Durch die dezentrale Speicherung wird sichergestellt, dass eine Blockchain nicht von einer zentralen Behörde verwaltet werden muss, wodurch das Risiko eines einzelnen Ausfallpunkts eliminiert wird. Neben der Transparenz hat die Blockchain-Technologie die drei folgenden Hauptmerkmale:

Dezentralisierung

Dezentralisierung in der Blockchain bedeutet, dass die Kontrolle und Entscheidungsfindung von einer zentralisierten Einheit (d. h. einer Einzelperson, Organisation oder Gruppe) auf ein dezentrales Netzwerk übertragen wird. Dezentralisierte Blockchain-Netzwerke nutzen Transparenz, um die Notwendigkeit von Vertrauen zwischen den Teilnehmern zu verringern. Diese Netzwerke halten die Teilnehmer auch davon ab, übermäßige Autorität oder Kontrolle übereinander auszuüben, was die Funktionalität des Netzwerks beeinträchtigen würde.

Unveränderlichkeit

Unveränderlichkeit bedeutet, dass etwas nicht verändert oder umgestaltet werden kann. Kein Teilnehmer kann eine Transaktion verfälschen, sobald ein Knoten sie im gemeinsamen Hauptbuch aufgezeichnet hat. Wenn ein Transaktionsdatensatz einen Fehler enthält, muss man eine neue Transaktion hinzufügen, um den Fehler rückgängig zu machen, und beide Transaktionen sind für das Netzwerk sichtbar.

Konsens

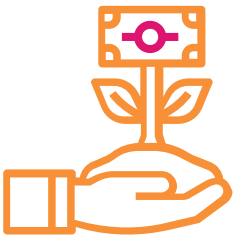
Ein Blockchain-System legt Regeln für die Zustimmung der Teilnehmer zur Aufzeichnung von Transaktionen fest. Sie können neue Transaktionen nur dann aufzeichnen, wenn die Mehrheit der Teilnehmer im Netzwerk ihre Zustimmung gibt. Bildlich gesprochen kann man sich die Blockchain als eine Kette von Blöcken vorstellen, von denen jeder einzelne Transaktionsdaten miteinander verknüpft. Die Transaktionen werden zu Blöcken zusammengefasst, auf ihre Gültigkeit geprüft und an die vorherige Kette von Blöcken angehängt - ein Prozess, der bei Bitcoin Proof of Work (PoW) genannt wird. Der PoW-Ansatz beinhaltet die Lösung von Rechenproblemen, die nur durch häufiges Ausprobieren gelöst werden können. Dadurch wird sichergestellt, dass ausreichend Arbeit in die Berechnung und Sicherung der Transaktionen investiert wird. Neben PoW gibt es eine Vielzahl anderer Konsensmechanismen, die für bestimmte Anwendungsfälle auf der Grundlage ihrer spezifischen Vor- und Nachteile ausgewählt werden können.

1.4 Was sind die wichtigsten Komponenten der Blockchain-Technologie?

Die Blockchain-Architektur besteht aus den folgenden Hauptkomponenten:

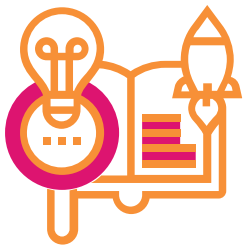
Verteiltes Hauptbuch

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 Bearbeitungsrechte hat, die gesamte Datei löschen. Nicht so bei DLT - hier gelten strenge Regeln darüber, wer die Datei bearbeiten darf und wie sie bearbeitet wird. Sie können Einträge nicht mehr löschen, sobald sie erfasst wurden.



Intelligente Verträge

Unternehmen nutzen Smart Contracts, um Geschäftsverträge selbst zu verwalten, ohne dass eine unterstützende Drittpartei erforderlich ist. Intelligente Verträge sind auf einem Blockchain-System gespeicherte Programme, die automatisch ausgelöst werden, wenn bestimmte Bedingungen erfüllt sind. Konkret führen intelligente Verträge Wenn-Dann-Anweisungen aus, sodass Transaktionen sicher abgeschlossen werden können. Beispielsweise kann eine Lotterie festlegen, dass das Preisgeld der Lotterie unter denjenigen Parteien verteilt wird, die die Lotterie durch richtiges Erraten der Zahlen gewinnen. Die Information über die richtige Zahl wäre Teil der Wenn-Dann-Anweisung.



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 zugänglich ist. 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, worauf in einem späteren Kapitel noch eingegangen wird.

Ein Beispiel: Bob und Alice sind zwei Mitglieder eines Netzwerks. Alice zeichnet eine Transaktion auf, die mit ihrem privaten Schlüssel verschlüsselt ist. Bob kann sie mit seinem öffentlichen Schlüssel entschlüsseln. Auf diese Weise kann Bob sicher sein, dass Alice die Transaktion durchgeführt hat. Der öffentliche Schlüssel von Alice hätte nicht funktioniert, wenn der private Schlüssel von Bob manipuliert worden wäre.

1.5 Der Unterschied zwischen Datenbanken und Blockchains

Blockchain ist eine bestimmte Art von Datenbankverwaltungssystem, das im Vergleich zu herkömmlichen Datenbanken mehr Funktionen aufweist. Einige der wesentlichen Unterschiede zwischen einer herkömmlichen Datenbank und einer Blockchain sind die folgenden:

- Die Kontrolle ist in Blockchains dezentralisiert, ohne das Vertrauen in die vorhandenen Daten zu beschädigen, was andere Datenbanksysteme in diesem Umfang nicht leisten können.
- Normalerweise sind die an einer Transaktion beteiligten Unternehmen nicht berechtigt, ihre gesamte Datenbank mit Dritten zu teilen. In Blockchain-Netzwerken verfügt jedes teilnehmende Unternehmen über eine (transparente) Kopie des aktuellen Stands des Hauptbuchs mit automatischen Aktualisierungen.
- Blockchains sind unveränderlich, d. h., Sie können nur Daten einfügen, aber nicht bearbeiten oder löschen.

1.6 Entwicklung der Blockchain-Technologie

Die Geschichte der Blockchain und die von Bitcoin sind miteinander verwoben. Im Jahr 2008 wurde das Bitcoin-Whitepaper veröffentlicht. In diesem Whitepaper wurde ein Konzept für ein dezentrales Geldsystem vorgestellt. Die Entwicklung der Blockchain-Technologie hat einen neuen Höhepunkt erreicht, seit Satoshi Nakamoto, der unbekannte Autor, das Bitcoin-Whitepaper veröffentlicht hat. Inzwischen gibt es Anwendungsmöglichkeiten für die Blockchain-Technologie, die weit über die Funktion eines Finanztransaktionsbuchs hinausgehen. So können beispielsweise mit intelligenten Verträgen eine Vielzahl von Verwaltungs- und Prozessanwendungen abgewickelt werden, zu denen eine normale Blockchain-Basisschicht nicht in der Lage ist. Die Ausführung dieser Smart Contracts kann in Echtzeit verfolgt werden - als logische Weiterentwicklung des Open-Source-Gedankens ermöglicht die Blockchain somit eine offene Ausführung.

Dank der rasanten Blockchain-Entwicklung können auf diese Weise sensible Daten wie Gesundheitsdaten oder Eigentumsverhältnisse wie Grundbesitz über eine Blockchain organisiert und kontrolliert werden. Gleichzeitig ist jeder Eintrag, der jemals in einem Blockchain-Verzeichnis gemacht wurde, für immer nachvollziehbar und kann nicht gelöscht oder verändert werden. Entsprechend groß ist das Interesse von Unternehmen an der Erforschung dieser Technologie. Die Hauptmotivationen sind die Aspekte Sicherheit, Transparenz und Effizienzsteigerung (in Bezug auf Kosten, Zeit, Personal und Digitalisierung). Die Möglichkeit, Prozesse über eine sichere Infrastruktur zu automatisieren und gleichzeitig das Risiko der Datenmanipulation auszuschalten, erscheint für Institutionen und Unternehmen attraktiv.

Es ist zu beachten, dass es nicht "die eine Blockchain" gibt. Vielmehr kann eine Blockchain in sehr unterschiedlichen Kalibrierungen gestaltet sein. Eine Blockchain, die in der Verwaltung einer Behörde eingesetzt wird, ist anders konzipiert als beispielsweise die bekannteste Blockchain, die Bitcoin-Blockchain, auf der eine Vielzahl von Anwendungen basiert.

1.7 Vorteile der Blockchain-Technologie im Vergleich zu herkömmlichen Datenbanksystemen

Herkömmliche Datenbanktechnologien stellen bei der Erfassung von Finanztransaktionen eine Reihe von Herausforderungen dar. Nehmen wir zum Beispiel den Verkauf einer Immobilie. Sobald das Geld ausgetauscht ist, geht das Eigentum an der Immobilie auf den Käufer über. Sowohl der Käufer als auch der Verkäufer können die Geldtransaktionen einzeln aufzeichnen, aber keiner der beiden Quellen kann man trauen, wenn es um die vollständige Beseitigung von Zweifeln geht. Der Verkäufer könnte behaupten, er habe das Geld nicht erhalten, obwohl er es erhalten hat, und der Käufer könnte ebenso behaupten, er habe das Geld bezahlt, obwohl er es nicht erhalten hat.

Um mögliche rechtliche Probleme zu vermeiden, muss eine vertrauenswürdige dritte Partei die Transaktionen überwachen und validieren. Das Vorhandensein dieser zentralen Behörde verkompliziert nicht nur die Transaktion, sondern schafft auch einen potenziellen Single Point of Failure und erhöht die Anfälligkeit. Wenn die zentrale Datenbank kompromittiert würde, könnten beide Parteien darunter leiden. Die Blockchain könnte solche Probleme entschärfen, indem sie je ein Hauptbuch für den Käufer und den Verkäufer schafft. Alle Transaktionen müssen von beiden Parteien genehmigt werden und werden automatisch in beiden Ledgern in Echtzeit aktualisiert. Jede Verfälschung historischer Transaktionen führt zur Verfälschung des gesamten Hauptbuchs. Diese Eigenschaften der Blockchain-Technologie haben dazu geführt, dass sie in verschiedenen Sektoren eingesetzt wird, u. a. bei der Schaffung digitaler Währungen wie Bitcoin und anderen Anwendungsfällen, die Gegenstand des nächsten Kapitels sind.

02

MODUL 1

BLOCKCHAIN-NUTZUNG IN VERSCHIEDENEN BRANCHEN

2.1 Anwendungsfälle auf dem Finanzmarkt für Blockchain-Anwendungen

Internationaler Zahlungsverkehr

Blockchain kann sichere, effiziente und fälschungssichere Aufzeichnungen über sensible Aktivitäten erstellen. Dies ist im Zusammenhang mit internationalen Zahlungen und Geldtransfers von Vorteil, wo hohe Transaktionsgebühren, verschiedene Vermittler und lange Abwicklungszeiten immer noch die Norm sind. Die Geschäftsbank Banco Santander hat 2018 den weltweit ersten Blockchain-basierten Geldtransferdienst eingeführt. Mit dem sogenannten "Santander One Pay FX" können Kunden noch am selben oder nächsten Tag internationale Überweisungen tätigen. Durch den Einsatz von Blockchain konnte Santander die Anzahl der Vermittler, die normalerweise für diese Transaktionen erforderlich sind, reduzieren und die Kosten für Überweisungen durch weniger manuelle Arbeit senken, wodurch der Prozess effizienter wurde.

Kapitalmärkte

Auf den Kapitalmärkten kann die Blockchain-Technologie zu einem schnelleren Clearing und einer schnelleren Abwicklung, zur Konsolidierung von Prüfpfaden und zu operativen Verbesserungen beitragen (z. B. Tokenisierung von Aktien und weniger manuelle Arbeit, Überwachung umfangreicherer Datensätze, Marktüberwachung, Fondsportfolioverwaltung).

Handelsfinanzierung

Traditionell sind die üblichen Methoden der Handelsfinanzierung mit langsamen Prozessen verbunden, die die Geschäftstätigkeit unterbrechen und die Liquidität beeinträchtigen. Dies ist darauf zurückzuführen, dass der grenzüberschreitende Handel viele Daten umfasst (z. B. Ursprungsland, Produktdetails, Dokumentation von Transaktionen). Die Blockchain-Technologie kann diese Datenverfolgung und -überwachung automatisieren.

Einhaltung von Vorschriften und Audit

In der Buchführung und Rechnungsprüfung verringert sich die Möglichkeit menschlicher Fehler und die Korrektheit der Daten. Kontodaten können nicht mehr geändert werden, sobald sie in einer Kette erfasst sind.

Schutz vor Geldwäscherei

Durch die Aufzeichnung der Kette, unterstützt durch das "Know Your Customer (KYC)"-Verfahren, mit dem ein Unternehmen die Identität seiner Kunden identifiziert und überprüft, können Münzen, Token und Adressen, die Geld waschen oder im Verdacht stehen, dies zu tun, auf eine schwarze Liste gesetzt werden, was zur Aufdeckung betrügerischer Aktivitäten in Bezug auf Geld und Geschäfte führt.

Versicherung

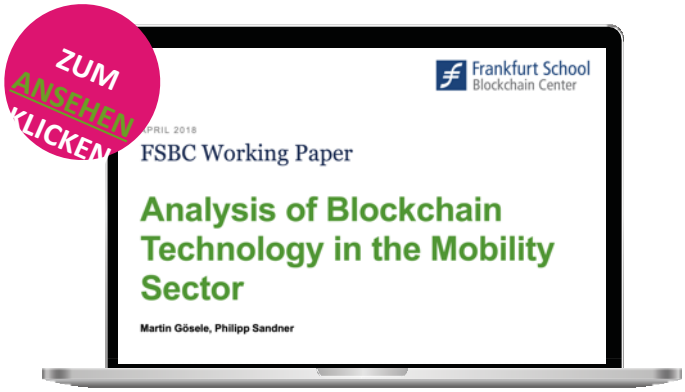
Blockchain in Verbindung mit intelligenten Verträgen in Versicherungssystemen hat verschiedene Anwendungsfälle. Die Verlagerung von Versicherungsansprüchen auf eine Blockchain kann dazu führen, dass häufige Betrugsquellen in der Branche reduziert werden (z. B. durch Ablehnung mehrerer Ansprüche bei einem Vorfall). Es besteht auch die Möglichkeit, Krankenakten (oder besser gesagt nur die relevanten Teile) kryptografisch zu sichern und zwischen Versicherungsgesellschaften, Ärzten und dem Patienten zu verteilen. Ein weiteres Beispiel wäre die Anmeldung eines Todesfalls, bei dem der manuelle Prozess der Antragstellung durch ein automatisiertes Blockchain-System ersetzt wird.

Peer-to-Peer-Transaktionen

P2P-Zahlungsdienste wie PayPal, Swish oder Venmo bieten in vielen Teilen der Welt schnelle und kostengünstige Transaktionen mit E-Geld an, obwohl einige Dienste die Transaktionen je nach Standort einschränken. Transaktionsgebühren, das Risiko von Hacks und Insolvenzen und die Notwendigkeit eines Vermittlers können durch die Einführung eines Blockchain-basierten Systems reduziert oder eliminiert werden.

2.2 Anwendungsfälle in der Industrie für Blockchain-Anwendungen

Um mehr über industrielle Anwendungsfälle für Blockchain im Mobilitätssektor zu erfahren, lesen Sie das Exkursionspapier "Analyse der Blockchain-Technologie im Mobilitätssektor" von Prof. Dr. Philipp Sandner und Martin Gösele.



03

MODUL 1

FUNKTIONSMECHANISMEN VON BLOCKCHAIN-TRANSAKTIONEN

3.1 Wie funktioniert eine Transaktion auf der Blockchain?

Blockchain-Mechanismen sind komplex. Im Folgenden wird ein kurzer Überblick über die Transaktionsverarbeitung auf Blockchains gegeben. Sehen Sie sich zunächst diese Blockchain-Demo an.

Sehen Sie sich zunächst diese Blockchain-Demo an.

Sie können das Blockchain-Demo-Tool auch selbst ausprobieren. Klicken Sie dazu hier.

Aufzeichnung der Transaktion

Eine Blockchain-Transaktion zeigt die Bewegung von physischen oder digitalen Vermögenswerten von einer Partei zu einer anderen im Blockchain-Netzwerk. Sie wird in einem Datenblock aufgezeichnet und enthält Details wie (z. B. Wer war an der Transaktion beteiligt? Wann hat die Transaktion stattgefunden? Wie viel des Vermögenswertes wurde ausgetauscht?).

Abbildung 3: Beispiel einer Bitcoin-Transaktion (Quelle: Mempool Space, abgerufen am 27.10.2022)

Wie in der Abbildung dargestellt, ist die Transaktions-ID die eindeutige Kennung, die zur Verfolgung der Transaktion verwendet wird; alle Transaktionen können über die Block-Explorer-Websites verfolgt werden. Die Eingangsadresse gibt an, wer die Absenderadresse(n) der Gelder ist/sind, die Ausgangsadresse ist die Empfängeradresse der Gelder. In diesem Fall gibt es eine externe Empfängeradresse, und die Eingangsadresse erhält die nicht ausgegebenen Bitcoin über die Eingangsadresse zurück. In den Transaktionsinformationen werden Details über die Transaktion aufgeführt, z. B. die Höhe der an den Miner gezahlten Gebühren und der Gesamtbetrag der eingegebenen Bitcoin. Die Differenz zwischen dem Gesamtbetrag der Bitcoin-Eingabe und -Ausgabe bestimmt die Transaktionsgebühr.

Die Blockinformationen geben Auskunft über die Blockgröße (in diesem Beispiel 1,12 MB), die durchschnittliche Mining-Gebühr, die an die Miner gezahlt werden muss, damit Ihre Transaktion in den Block aufgenommen wird, welcher Miner bzw. welche Mining-Farm den Block geschürft hat, und andere wichtige Informationen. Alle Transaktionsdaten (siehe Abbildung 3) werden für jede einzelne Transaktion im Block selbst aufgeführt. Die Blockinformationen (siehe Abbildung 4) sind sozusagen nur die Zusammenfassung der Transaktionsdaten innerhalb des Blocks. Im Allgemeinen beträgt die Bitcoin-Blockgröße etwa 1 MB, obwohl es Vorschläge und Diskussionen über eine Vergrößerung der Blockgröße gibt, um mehr Skalierbarkeit für Bitcoin als Transaktionsnetzwerk zu erreichen.

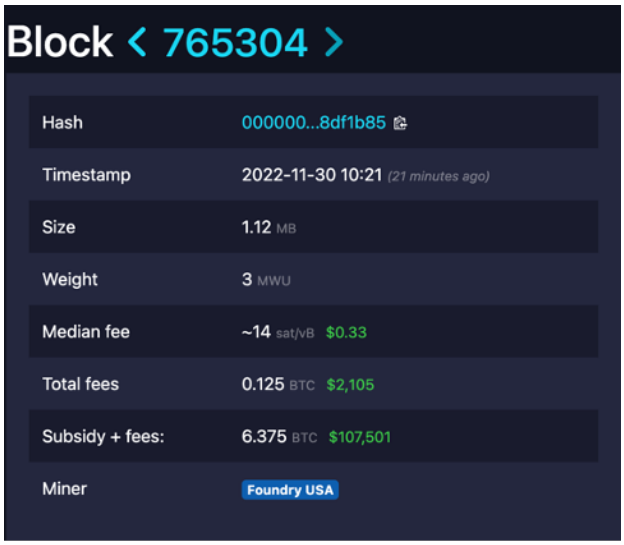


Abbildung 4: Beispielhafte Bitcoin-Transaktionen (Quelle: Mempool Space, abgerufen am 30.11.2022)

Einen Konsens finden

Die meisten Teilnehmer des verteilten Blockchain-Netzes müssen sich über den aktuellen Zustand des Netzes und die Gültigkeit von Transaktionen einigen, indem sie Konsensmechanismen nutzen. Konsens bedeutet, dass ein allgemeines Einvernehmen über den aktuellen Zustand des Netzes besteht. Je nach Art des Netzwerks können die Regeln für die Einigung variieren, werden aber in der Regel zu Beginn des Netzwerks festgelegt. Stellen Sie sich eine Gruppe von Leuten vor, die ins Kino gehen. Wenn es keine Meinungsverschiedenheiten über eine vorgeschlagene Filmauswahl gibt, wird ein Konsens erzielt. Kann kein Konsens gefunden werden, könnte sich die Gruppe aufteilen und getrennte Wege gehen. In Bezug auf die Blockchain ist der Prozess formalisiert, und das Erreichen eines Konsenses bedeutet, dass mindestens 51 % der Knoten im Netzwerk über den nächsten globalen Zustand des Netzwerks einig sind.

Verbinden Sie die Blöcke

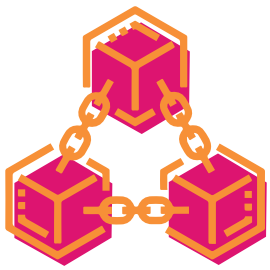
Sobald ein Konsens erreicht ist, werden die Transaktionen auf der Blockchain in Blöcke geschrieben. Dann wird ein kryptografischer Hash an jeden neuen Block angehängt, wie im Video zuvor gezeigt wurde. Der Hashwert bildet dann die Kette, die die Blöcke miteinander verbindet. Wenn die Daten im Block bearbeitet werden, ändert sich der Hash-Wert, was auf eine Manipulation hinweist. Mit jedem weiteren Block wird der vorherige Block erneut verifiziert.

Das Hauptbuch teilen

Das System sendet dann die neueste Kopie des zentralen Hauptbuchs an alle Teilnehmer des Netzwerks, wodurch der Status der gespeicherten Kopie der Blockchain für alle Teilnehmer aktualisiert wird. Das Mining erfordert erhebliche Rechenressourcen und nimmt aufgrund der Komplexität des Softwareprozesses viel Zeit in Anspruch. Im Gegenzug verdienen die Miner einen kleinen Betrag an Krypto. Die Miner fungieren als moderne Angestellte, die

3.2 Was sind die Vorteile der Blockchain-Technologie?

Die Blockchain-Technologie bietet viele Vorteile für die Verwaltung von Vermögenstransaktionen:



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.

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 sowie kosten- und zeiteffizienter.

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.

3.3 Was ist der Unterschied Zwischen Bitcoin und Blockchain?

Bitcoin und Blockchain können austauschbar verwendet werden, sind aber zwei verschiedene Dinge. Da Bitcoin eine frühe Anwendung der Blockchain-Technologie war, begannen die Menschen versehentlich, Bitcoin für Blockchain zu verwenden, was zu dieser falschen Bezeichnung führte. Wie in einem früheren Kapitel gezeigt wurde, hat die Blockchain-Technologie viele Anwendungsfälle außerhalb von Bitcoin. Bitcoin ist eine digitale Währung, die ohne zentrale Kontrolle funktioniert und die Blockchain-Technologie als zugrunde liegende Infrastruktur nutzt.

04

MODUL 1

DIE GESCHICHTE DES GELDES

4.1 Geschichte des Geldes

Geld selbst ist so alt wie die Zivilisation, selbst in den primitivsten Gesellschaften wurden nützliche und wertvolle Gegenstände als Zahlungsmittel verwendet. Natürliches Geld oder Warengeld sind Oberbegriffe für diese frühen Formen von Geld. Im Laufe der Geschichte wurde eine Vielzahl von Dingen als Geld verwendet. Dazu gehören Lebensmittel, Nutztiere, Waffen, Schmuck, Kleidung und auch Schneckenhäuser. So ist das räumlich und zeitlich am weitesten verbreitete Zahlungsmittel die Kaurischnecke, die oft fälschlicherweise als "Kaurimuschel" bezeichnet wird. Die Kaurischnecke, das bis heute erfolgreichste Zahlungsmittel der Weltgeschichte, wurde in weiten Teilen Afrikas und Asiens verwendet. Funde in China legen sogar nahe, dass die Kaurimuschel dort bereits im 2. Jahrtausend v. Chr. als Geld verwendet wurde. Normalerweise wurden diese Arten von Geld getauscht, d. h. man musste eine Ware, die man besaß, gegen eine andere Ware, die man haben wollte, eintauschen, was die Tauschfähigkeit zu einem groben Schätzspiel machte.

Dieses Naturalgeld oder Warengeld wurde mit zunehmendem Handel durch Münzen ersetzt, die ausschließlich Geldfunktion hatten. Die ersten Münzen wurden im 7. Jahrhundert v. Chr. im Königreich Lykien geprägt. Es handelte sich um formlose Klumpen aus Elektronen, einer natürlich vorkommenden Gold-Silber-Legierung. Die Münzprägung erleichterte den Handel, und so verbreitete sich die neue Kulturtechnik des Bezahlens in der Antike von Kleinasien nach Europa. Nach und nach wurden auch in Griechenland und Rom Münzen geprägt. Die antiken Herrscher begannen, ihre Porträts auf die Münzen zu prägen, die somit nicht nur Zahlungsmittel, sondern auch Bildträger waren. Mit dem Ende des Römischen Reiches im 5. Jahrhundert n. Chr. endete auch die antike Ära des Münzwesens, und in der Spätantike und im frühen Mittelalter ging der Münzumlauf in ganz Europa stark zurück. Erst im Hochmittelalter, im 12. Jahrhundert, vollzog sich in Italien wieder der Übergang von einer Natural- zu einer Geldwirtschaft, und damit kamen auch die Münzen wieder zum Einsatz. Allerdings gab es kein einheitliches Münzsystem mehr wie im Römischen Reich. So zirkulierten im Heiligen Römischen Reich Deutscher Nation, das von Kleinstaaten geprägt war, viele verschiedene Währungen. Im Spätmittelalter setzte sich schließlich der rheinische Gulden als eine Art Reserve durch.

Papiergeld, wie wir es heute kennen, hat sich erst relativ spät durchgesetzt. Dennoch ist Papiergeld im Laufe der Geschichte immer wieder als Zahlungsmittel aufgetaucht, zum Beispiel in China im 10. In Europa wurde es erst viel später eingeführt. Erst die Bank of England in Großbritannien schaffte es, ein dauerhaftes öffentliches Vertrauen in Papiergeld zu schaffen. Im Jahr 1833 erklärte die englische Regierung Banknoten zum gesetzlichen Zahlungsmittel und wurde damit zum Vorreiter. Aufgrund der rasch wachsenden Wirtschaft im Zeitalter der Industrialisierung war die Geldversorgung von wesentlicher Bedeutung. Dies führte zu einer allmählichen Abkehr von Edelmetallwährungen. Das Münzgeld wurde zum Kleingeld.

Geld, unabhängig von seiner Form, wird häufig anhand von drei Funktionen oder Dienstleistungen definiert:

1 **Wertaufbewahrung:**
Wert über einen langen Zeitraum aufrechterhalten oder gesteigert wird.

2 **Einheit der Rechnung:**
die ein gemeinsames Maß für den Wert der ausgetauschten Waren und Dienstleistungen darstellen und fungibel, teilbar und abzählbar sein müssen.

3 **Tauschmittel:**
ist ein zwischengeschaltetes Instrument oder System, das zur Erleichterung des Warenverkehrs zwischen Parteien eingesetzt wird.

Geld kann jedes Gut sein, das bei Transaktionen, die den Transfer von Waren und Dienstleistungen von einer Person zur anderen beinhalten, allgemein verwendet und akzeptiert wird. In der heutigen Welt gibt es zwei traditionelle Formen von Geld: Fiatgeld und Geschäftsbankgeld. Fiat-Geld in Form von Banknoten und Münzen erhält seinen Wert dadurch, dass die Regierung Fiat-Geld zum gesetzlichen Zahlungsmittel erklärt, so dass es von allen Händlern und Gewerbetreibenden im Land als Mittel zur Begleichung von Schulden akzeptiert werden muss. Fiat-Geld hat per Definition einen wesentlich geringeren inneren Wert. Sein Wert ergibt sich aus den Kräften von Angebot und Nachfrage. Dies ist die Form der Währung, mit der wir am meisten vertraut sind.

Eine weitere Form des Geldes ist das Geschäftsbankengeld, das als Forderungen gegenüber Finanzinstituten bezeichnet werden kann, die zum Kauf von Waren oder Dienstleistungen verwendet werden können. Was alle diese Geldarten gemeinsam haben, sind die grundlegenden Eigenschaften des Geldes:

1 Dauerhaftigkeit

2 Tragbarkeit

3 Liquidität

4 Eine Rechnungseinheit

5 Status als gesetzliches Zahlungsmittel

6 Widerstandsfähigkeit gegen Fälschungen

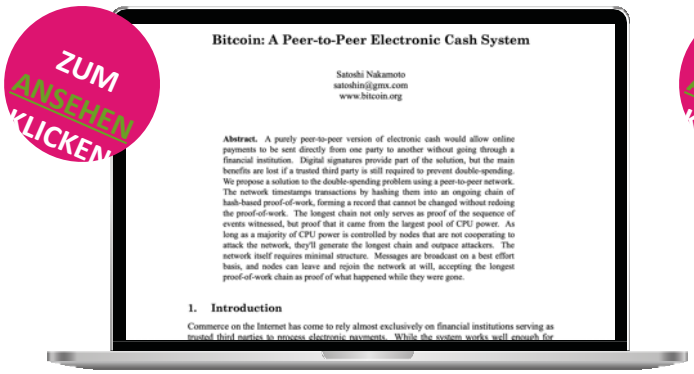
4.2 Einführung in Bitcoin und die Bitcoin-Blockchain

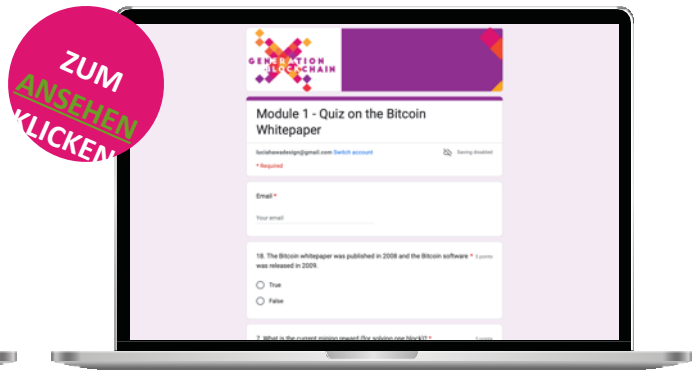
Bitcoin

Um Bitcoin zu verstehen, ist es wichtig, das Bitcoin-Whitepaper zu lesen, da Bitcoin gemessen an der Marktkapitalisierung der wichtigste Kryptowährungswert ist. Beachten Sie, dass Sie die technologischen Aspekte in diesem Stadium nicht im Detail verstehen müssen. Die Lektüre der Whitepaper soll einen Überblick über die Absichten von Bitcoin und die Mechanik der Technologie geben.

Hier finden Sie das Whitepaper.

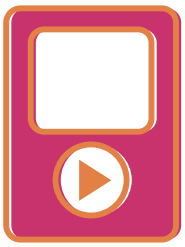
Testen Sie nach dem Durchlesen Ihr Verständnis mit diesem Quiz.





Bitcoin-Geldbörsen

Was sind Bitcoin-Wallets und welche Arten von Wallets gibt es? Um einen Überblick über dieses Thema zu bekommen, hören Sie sich die Generation Blockchain Podcast Episode "Bitcoin Wallets" an.



Generation Blockchain Podcast Episode "Bitcoin-Geldbörsen"

Beispiel für einen öffentlichen Bitcoin-Schlüssel:
Bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

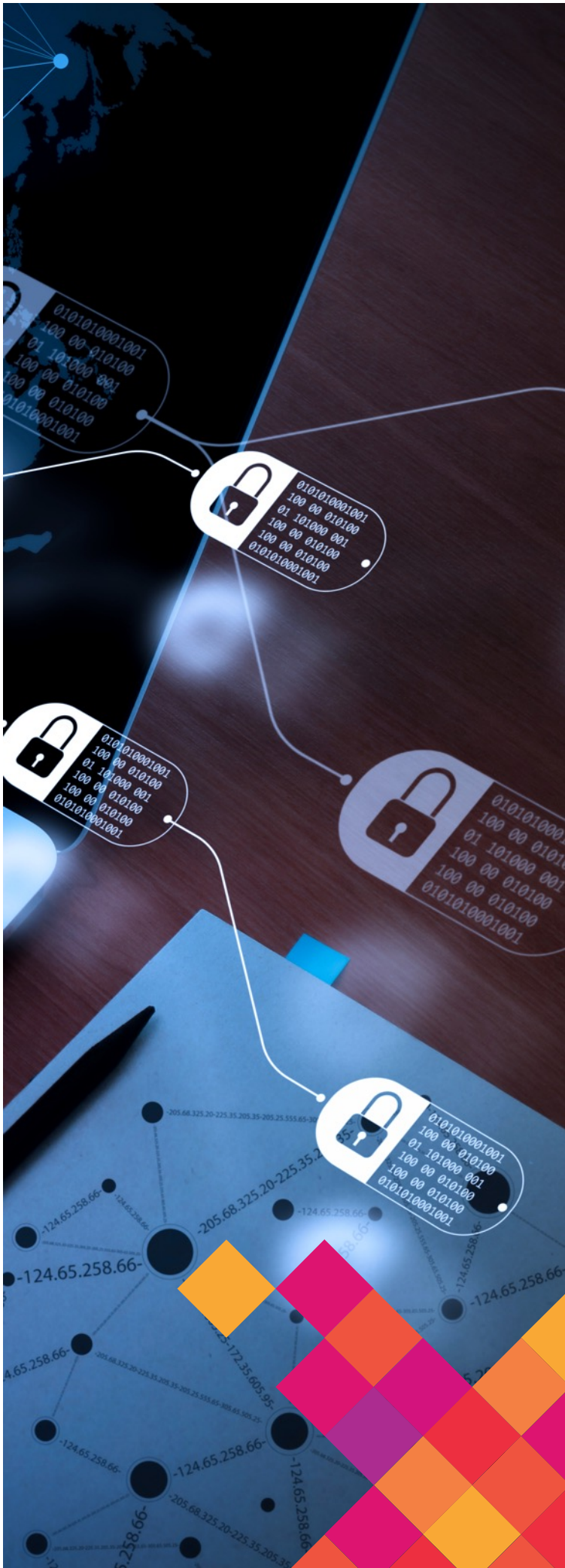
! SENDEN SIE KEINE BITCOINS AN DIESE ADRESSE. BITCOINS, DIE AN DIESE ADRESSE GESENDET WERDEN, SIND UNWIDERRUFLICH VERLOREN!

Bitcoin-Netzwerk

Ein öffentliches Hauptbuch zeichnet alle Bitcoin-Transaktionen auf, und Server auf der ganzen Welt halten Kopien dieses Hauptbuchs. Die Server sind wie Banken. Während jede Bank nur das Geld kennt, das ihre Kunden umtauschen, wissen die Bitcoin-Server über jede einzelne Bitcoin-Transaktion auf der Welt Bescheid. Jeder Computer kann einen Knotenpunkt einrichten. Das ist so, als würden Sie Ihre eigene Bitcoin-Bank anstelle eines Bankkontos eröffnen. Beachten Sie, dass die Einrichtung eines Knotens nicht gleichbedeutend damit ist, ein Miner zu sein.

Bitcoin-Schürfen

Rund um die Uhr und ohne Ausfallzeiten übertragen Menschen Bitcoins über das Bitcoin-Netzwerk. Im öffentlichen Bitcoin-Netzwerk schürfen die Mitglieder Kryptowährung, indem sie komplexe mathematische Krypto-Berechnungen lösen, um neue Blöcke zu erzeugen. Bitcoin-Mining ist der Prozess der Bereitstellung von Rechenleistung für die Transaktionsverarbeitung, die Sicherung und Synchronisierung des aktuellen Blockchain-Status für alle Nutzer im Netzwerk. Mining ist eine Art dezentrales Bitcoin-Rechenzentrum mit Minern auf der ganzen Welt. Dieser Prozess wird Mining genannt und erinnert an das Goldschürfen. Anders als beim Goldschürfen gibt es beim Bitcoin-Mining eine Belohnung für nützliche Dienste. Die Auszahlung der jeweiligen Bitcoin-Anteile richtet sich nach der erbrachten Rechenleistung. Im Jahr 2022 beträgt die Blockbelohnung für Miner 6,25 BTC pro neuem Block. Miner konkurrieren miteinander, um die Berechnung für den nächsten Block am schnellsten zu lösen. Der Block desjenigen Miners, der die kryptografische Berechnung als erster löst, wird schließlich im nächsten Block in der Blockchain gespeichert. Die Blöcke der anderen Schürfer sind ungültig und können nicht an die Kette angehängt werden. Die Blockzeit, die angibt, wie lange es dauert, einen Block für Bitcoin zu schürfen, beträgt im Durchschnitt 10 Minuten. Alle Miner beginnen gleichzeitig mit der Lösung des Rätsels. Die Zeit zum Lösen des Rätsels hängt von der aktuellen Schwierigkeitsrate ab. Wenn relativ viele Miner gleichzeitig versuchen, das Rätsel zu lösen, wird es für eine kurze Zeit im Durchschnitt schneller gelöst, bis sich der Schwierigkeitsgrad an die Gesamtzahl der Miner anpasst und die Blockzeit von 10 Minuten ausgeglichen wird. Neue Bitcoins werden nicht auf der Grundlage der Nachfrage geschürft, die Gesamtmenge an Bitcoin ist von Anfang an festgelegt (auf 21 Millionen) und kann nicht durch monetäre Instrumente aufgebläht werden. In herkömmlichen Fiat-Währungssystemen drucken Regierungen oder Zentralbanken mehr Geld, wenn ein Bedarf besteht. Vielmehr wird Bitcoin selbst oder in der Cloud (Cloud Mining) geschürft. Das System sendet jede neue Transaktion öffentlich an das Netzwerk, was bedeutet, dass die Knoten des Netzwerks Transaktionen mit anderen Knoten teilen. Ein neuer Block wirkt wie das endgültige Kontobuch von Bitcoin.



05

MODUL 1
INFRASTRUKTUR DER BLOCKCHAIN-TECHNOLOGIE

Ihr erster Kontakt mit der Infrastruktur der Blockchain-Technologie besteht darin, die Elemente und Teilnehmer dieser Technologie (d. h. Miner, Knoten, Hash-Funktionen, Public-Key-Kryptografie, digitale Signaturen und Adressen) eingehend kennenzulernen.

5.1 Blockchain-Technologie

Die Blockchain dokumentiert jeden Geldtransfer, der innerhalb eines bestimmten Netzwerks (z. B. des Bitcoin-Netzwerks) stattfindet. Dadurch wird sichergestellt, dass niemand denselben Geldbetrag zweimal ausgeben kann. Auf diese Weise konnten Blockchains das so genannte Problem der doppelten Ausgaben in der digitalen Welt lösen. Anstatt Kopien eines Originalgegenstands oder -vermögenswertes zu versenden, ermöglichen Blockchains, dass digitale Dinge zu einem bestimmten Zeitpunkt nur an einem Ort existieren. Digitales Geld und Vermögenswerte wären nicht funktionsfähig, wenn eine Kopie dieses Geldes oder Vermögenswerts zweimal versendet werden könnte.

5.2 Knotenpunkte

Die Knotenpunkte, die ein Netzwerk von Computern sind, betreiben eine Blockchain und bilden deren Kerninfrastruktur. Die Knoten im Netzwerk tauschen Informationen über neu eingehende Transaktionen und die Bildung von Blöcken aus. Es ist wichtig zu wissen, dass es verschiedene Arten von Knoten gibt. Ein Full Node ist ein Knoten, der eine vollständige Kopie der Blockchain unterhält und über Offline-Fähigkeiten verfügt, während ein Light Node keine Kopie der Blockchain unterhält und in seinen Funktionen eingeschränkter ist (d. h. er lädt nur den Block-Header und nicht den vollständigen Block herunter). Bevor ein Light-Node Teil eines Blockchain-Netzwerks sein kann (d. h. um Transaktionen zu senden oder zu validieren), muss er mit einem Full-Node verbunden sein. In diesem Sinne ist das Blockchain-Netzwerk mit der Infrastruktur Ihres Telefons vergleichbar.

Vollknoten können mit dem Mobilfunkmast verglichen werden, mit dem Ihr Telefon (d. h. der leichte Knoten) verbunden ist. Alle Antennenstationen (d. h. die Vollknoten) sind miteinander verbunden und bilden die Infrastruktur des Kommunikationsnetzes. Wenn Sie mit Ihrem Telefon einen Anruf tätigen wollen, müssen Sie zuerst eine Verbindung zu einem Mobilfunkmast herstellen, bevor Sie mit einem anderen Mobiltelefon kommunizieren können. Ähnlich verhält es sich im verteilten Netzwerk einer Blockchain: Die vollständigen Knoten sind die meiste Zeit über in Betrieb und bilden das verteilte Netzwerk. Sie verwalten auch eine Kopie der gesamten Blockchain. Wenn Sie eine Brieftasche auf Ihrem Telefon oder Computer verwenden, werden Sie wahrscheinlich einen Light-Knoten benutzen. In diesem Fall müssen Sie sich zuerst mit einem Full Node verbinden, bevor Sie mit der Blockchain interagieren können. Die Teilnehmer eines Netzwerks entscheiden sich für einen Full Node, wenn sie zur Stabilität und Sicherheit des Netzwerks beitragen wollen, aber für die Verwendung von Kryptowährungen ist dies nicht unbedingt erforderlich.

5.3 Miner und Validierer

Jeder Miner ist ein Knoten im Blockchain-Netzwerk, aber man muss kein Miner sein, um einen Knoten zu betreiben. Miner unterstützen das Netzwerk, indem sie Informationen weiterleiten und eine Kopie der Blockchain aufbewahren, genau wie alle anderen Knotenpunkte. Im Gegensatz zu Nicht-Miner-Knoten sind Miner für die Erstellung neuer Blöcke in der Blockkette verantwortlich. Jeder Block in einer Blockchain ist eine kollektive Entscheidung über die Geschichte eines bestimmten Zeitpunkts. Um eine kollektive Entscheidung zu treffen, findet das Netzwerk einen Konsens darüber, welche Transaktionen in welcher Reihenfolge in den nächsten Block aufgenommen werden. Nicht alle von den Minern vorgeschlagenen Blöcke sind gleich. Ein Grund dafür ist, dass es unterschiedlich lange dauert, bis sich neue Transaktionen im gesamten Netzwerk verbreiten, wodurch sich unterschiedliche Transaktionspools mit ungeprüften Transaktionen bilden.

In Ethereum werden die Miner als Validatoren bezeichnet, seit Ethereum von seinem Proof-of-Work- auf den Proof-of-Stake-Algorithmus umgestellt hat. Ein Validator ist im Wesentlichen ein Wähler für einen neuen Block. Je mehr Stimmen ein Block erhält, desto größer ist die Wahrscheinlichkeit, dass er ausgewählt wird.

Der Grund, warum Miner ein Interesse daran haben, ehrlich und im Interesse des Netzwerks zu handeln, ist, dass sie einen Anreiz haben, sich nach den Regeln der Blockchain zu verhalten. Wenn eine ungültige Transaktion in einen Block eingefügt wird, hat dieser Block aufgrund seiner fehlerhaften Dateneingabe keine Chance, der Gewinnerblock zu sein. Der Miner, der das Rätsel zuerst löst, wird mit der Blockbelohnung und/oder der Transaktionsgebühr belohnt, die jeder, der eine Transaktion über die Bitcoin- und Ethereum-Blockchain sendet, zahlen muss, damit die Transaktion in einen der nächsten Blöcke aufgenommen wird. Die wahrscheinliche Chance, die Blockbelohnung und die Transaktionsgebühren zu erhalten, schafft den Anreiz für Einzelpersonen, die teure Hardware zu kaufen und zu betreiben, die zur Lösung des kryptografischen Puzzles benötigt wird. Der erste Schürfer, der einen Block löst, erhält eine Belohnung in der Währung, die er gerade schürft. Der siegreiche Schürfer darf sich selbst eine Transaktion mit einigen Münzen (je nach Blockchain und Kryptowährung) schicken, die es vorher nicht gab.

Die Miner erhalten den letzten Stapel von Transaktionsdaten, der dann durch einen kryptografischen Algorithmus geordnet wird. Dabei wird ein Hash, eine Zahlen- und Buchstabenfolge, die keine Transaktionsdaten preisgibt, erzeugt und zur Überprüfung der Gültigkeit verwendet. Der Hash stellt sicher, dass der entsprechende Block nicht verändert wurde. Wenn auch nur eine Zahl nicht stimmt oder nicht an der richtigen Stelle steht, wird für die entsprechenden Daten ein anderer Hashwert erzeugt. Der Hashwert des vorherigen Blocks wird in den nächsten Block integriert, so dass sich der generierte Hashwert ändert, wenn im vorherigen Block etwas geändert wurde. Der Hash-Wert muss außerdem unter einem vom Hash-Algorithmus festgelegten Zielwert liegen. Ist der generierte Hash-Wert zu groß, wird er erneut generiert, bis er unter dem angegebenen Zielwert liegt.

5.4 Hash-Funktionen

Die Datenüberprüfung ist eine wichtige Komponente beim Aufbau einer Datenstruktur in einem dezentralen Netzwerk. Nur durch die Verifizierung können die Teilnehmer zwischen gültigen Daten und ungültigen Informationen unterscheiden. In Blockchain-Systemen sind Hash-Funktionen die mathematischen Einwegfunktionen, die als Mittel zur Überprüfung von Daten in Blockchains in verschiedenen Phasen der Datenüberprüfung (d. h. bei der Erstellung einer Adresse, dem Nachweis des Eigentums, dem Nachweis der Integrität der Blockchain selbst) verwendet werden.

Alle Hash-Funktionen nehmen Eingaben variabler Länge entgegen und erzeugen eine Ausgabe fester Länge, den Hash-Wert. Hash-Funktionen sind unumkehrbare Einwegfunktionen. Sie können Ihren Hashwert nicht in die Daten zurückübersetzen, die Sie eingegeben haben, um den Hashwert zu erhalten, wie im Blockchain-Demovideo gezeigt wurde. Hash-Funktionen sind pseudozufällig (d. h., sie erzeugen scheinbar zufällige Ausgaben aus zwei ähnlichen Eingaben). Die Wahrscheinlichkeit, dass eine Hash-Funktion für zwei oder mehr verschiedene Eingaben die gleiche Ausgabe erzeugt, ist höchst unwahrscheinlich. Sie sind jedoch deterministisch, d. h. sie erzeugen für eine bestimmte Eingabe immer die gleiche Ausgabe. In diesem Sinne ist ein Hash-Wert vergleichbar mit einem Fingerabdruck von Daten. Man kann die Integrität von Dateien überprüfen und Änderungen feststellen, indem man ihre Hashwerte vergleicht. Die Eingabe kann jede Art von Daten sein (d. h. Audio, Video, Bild) und ist nicht auf Zahlen beschränkt.

Hash-Mode	Hash-Name	Example
0	MD5	8743b52063cd84097a65d1633f5c74f5
10	md5($pass.$salt)	01dfae6e5d4d90d9892622325959afbe:7050461
20	md5($salt.$pass)	f0fda58630310a6dd91a7d8f0a4ceda2:4225637426
30	md5(utf16le($pass).$salt)	b31d032cfdcf47a399990a71e43c5d2a:144816
40	md5($salt.utf16le($pass))	d63d0e21fdc05f618d55ef306c54af82:13288442151473
50	HMAC-MD5 (key = $pass)	fc741db0a2968c39d9c2a5cc75b05370:1234
60	HMAC-MD5 (key = $salt)	bfd280436f45fa38eaacac3b00518f29:1234
70	md5(utf16le($pass))	2303b15bfa48c74a74758135a0df1201
100	SHA1	b89eaac7e61417341b710b727768294d0e6a277b
110	sha1($pass.$salt)	2fc5a684737ce1bf7b3b239df432416e0dd07357:2014
120	sha1($salt.$pass)	cac35ec206d868b7d7cb0b55f31d9425b075082b:5363620024
130	sha1(utf16le($pass).$salt)	c57f6ac1b71f45a07dbd91a59fa47c23abcd87c2:631225
140	sha1($salt.utf16le($pass))	5db61e4cd8776c7969cfd62456da639a4c87683a:8763434884872
150	HMAC-SHA1 (key = $pass)	c898896f3f70f61bc3fb19bef222aa860e5ea717:1234
160	HMAC-SHA1 (key = $salt)	d89c92b4400b15c39e462a8caa939ab40c3aeeea:1234
170	sha1(utf16le($pass))	b9798556b741befdbddcbf640d1dd59d19b1e193
200	MySQL323	7196759210defdc0
300	MySQL4.1/MySQL5	fcf7c1b8749cf99d88e5f34271d636178fb5d130

Abbildung 5: Allgemeine Hash-Typen (Quelle: Hashcat, abgerufen am 15.11.2022)

Wie die Abbildung zeigt, gibt es verschiedene Hash-Funktionen, die unterschiedliche Ergebnisse mit fester Länge haben und von verschiedenen Blockchains verwendet werden. Eine der am häufigsten verwendeten Hash-Funktionen ist der sogenannte SHA256 (Secure Hash Algorithm 256 bit). Die 256 steht für die feste Länge des Hashwerts. Es gibt viele Hash-Funktionen, von denen die meisten ihre feste Länge in ihrem Namen angeben.

5.5 Kryptographie mit öffentlichen Schlüsseln

Die Public-Key-Kryptographie (auch als asymmetrische Kryptographie bekannt) gewährt den Inhabern von Kryptowährungen Zugang zu ihrem Geld. Sie bietet eine Möglichkeit zum Nachweis des Eigentums. Bei der symmetrischen Kryptografie verschlüsseln und entschlüsseln Sie eine Nachricht mit demselben Schlüssel von beiden Seiten. Dies funktioniert ähnlich wie bei einem Vorhängeschloss, bei dem derselbe Schlüssel zum Öffnen (Entschlüsseln) und Schließen (Verschlüsseln) des Vorhängeschlosses verwendet wird. Die asymmetrische Verschlüsselung beruht auf der Eigenschaft, dass Schlüssel immer paarweise vorkommen und komplementär verwendet werden. Einer der Schlüssel verschlüsselt etwas und der andere entschlüsselt es. Die Schlüssel werden öffentlicher und privater Schlüssel genannt, auch Ausgabeschlüssel oder geheimer Schlüssel. Ihre Schlüssel übersetzen Ihre Identität auf der Blockchain. Sie erhalten Gelder mit Ihrem öffentlichen Schlüssel und senden Gelder mit Ihrem privaten Schlüssel.

Schlüssel und Identität

Die Idee bei Kryptowährungen ist, dass Sie mit Ihrem öffentlichen Schlüssel Geld erhalten und es mit Ihrem privaten Schlüssel ausgeben. Die Schlüssel werden absichtlich öffentlich und privat genannt, da Sie Ihren öffentlichen Schlüssel mit jedem teilen können. Sie brauchen Ihren privaten Schlüssel, um Ihr Geld auszugeben. Wer Zugang zu Ihren Schlüsseln hat, kann auch auf Ihr Geld zugreifen. Ein öffentlicher Schlüssel ist vergleichbar mit Ihrer Adresse. Sie können ihn an Personen weitergeben, die Ihnen einen Brief oder ein Paket schicken wollen. Ihr privater Schlüssel ist wie der Schlüssel zu Ihrem Briefkasten. Nur mit diesem Schlüssel können Sie auf Ihre Post zugreifen, und in der Regel haben nur Sie selbst Zugang zu ihm. Ihre Schlüssel werden sowohl für das Senden als auch für das Empfangen von Transaktionen benötigt. Eine Transaktion ist auf technischer Ebene eine Nachricht an alle Knoten im Netz. Die Informationen in der Nachricht werden dann mit den privaten Schlüsseln verschlüsselt, was als digitales Signieren einer Transaktion bezeichnet wird. Dieser Prozess wird nicht manuell durchgeführt, sondern es gibt Wallets, die diese Schritte für den Nutzer übernehmen. Wallets sind in der Lage, Schlüssel zu generieren und zu verwalten sowie zu ver- und entschlüsseln.

Generierung von Schlüsseln und Adressen

Auf Gelder oder Daten, die an einen öffentlichen Schlüssel gesendet werden, kann nur zugreifen, wer im Besitz des entsprechenden privaten Schlüssels ist. Der öffentliche Schlüssel wird mittels Elliptic Curve Cryptography (ECC) aus dem privaten Schlüssel abgeleitet. ECC ist das am weitesten verbreitetere Kryptographieverfahren bei Kryptowährungen mit öffentlichem Schlüssel, obwohl es auch andere Kryptographieverfahren gibt. Die Kryptografie verwendet Einwegfunktionen, und die Multiplikation auf einer elliptischen Kurve ist eine weitere erwähnenswerte Einwegfunktion. Daher kann die Ableitung eines öffentlichen Schlüssels aus einem privaten Schlüssel nicht rückgängig gemacht werden.

Digitale Signaturen

Eine Transaktion kann nur validiert werden, wenn sie mit einer gültigen digitalen Signatur versehen ist. Der private Schlüssel, der mit der Adresse verbunden ist, die das Geld speichert, muss eine Transaktion signieren. Wenn eine Transaktion an das Netzwerk gesendet wird, wird sie von allen vollständigen Knoten und Minern anhand der Nachricht, des öffentlichen Schlüssels oder der Adresse und der Signatur überprüft. Eine Signatur kann erst am Ende der Überprüfung gültig oder ungültig sein.

Peer-to-Peer-Netzwerk

In einem P2P-Netzwerk haben alle Teilnehmer die gleiche Rolle. Jeder von ihnen fungiert als Client (d. h., er fordert Daten an) und als Server (d. h., er stellt Daten bereit). Der Vorteil eines P2P-Netzwerks besteht darin, dass bei einem Ausfall eines Rechners die noch mit dem Netzwerk verbundenen Rechner weiterhin ihre Dienste anbieten. Diese Systemarchitektur macht Blockchain-Netzwerke widerstandsfähig gegenüber Einzelausfällen.

5.6 Konsensmechanismen

Bergbau & Konsens

Jede Blockchain muss einen Mechanismus wählen, der sicherstellt, dass sich alle Teilnehmer auf eine einzige Wahrheit bezüglich der Daten einigen. Stellen Sie sich das wie eine standardisierte Methode vor, um alle Politiker in einem Parlament dazu zu bringen, sich so schnell wie möglich auf eine Meinung zu einigen. Da die Politiker wahrscheinlich darüber diskutieren müssen, tun dies auch alle Teilnehmer eines Blockchain-Netzwerks, indem sie über das Netzwerk miteinander kommunizieren. Die Kommunikationsprotokolle sind in der Software implementiert, die auf allen beteiligten Geräten ausgeführt wird. Allerdings geht es bei der Kommunikation nicht um eine politische Meinung, sondern um den Datenstand der Blockchain, etwa den Transaktionsverlauf einer Währung wie Bitcoin. Um dieses Problem in Blockchain-Netzwerken zu lösen, wird ein Konsensmechanismus verwendet.

Das Problem der byzantinischen Generäle

Die verschiedenen Konsensmechanismen lösen ein uraltes Problem, das als Problem der byzantinischen Generäle bezeichnet wird. Das ursprüngliche Dilemma ist das folgende:

Eine Königin ist mit ihren 500 Soldaten in ihrem Schloss gefangen, weil das Schloss von fünf Armeen belagert wird, die jeweils 100 Mann stark sind. Jedes Heer hat sein Lager in der Nähe des Schlosses aufgeschlagen und steht unter dem unabhängigen Kommando eines Generals aus jedem Heer. Die Generäle müssen miteinander kommunizieren, um sich auf eine Angriffsstrategie zu einigen. Ihr Vertrauen ineinander ist jedoch begrenzt, da sie vermuten, dass einige von ihnen Verräter sind. Würden die Generäle eine Nachricht mit der Taktik und dem Zeitplan des Angriffs durch einen Boten von Lager zu Lager schicken, könnten die der Königin treuen Generäle leicht Änderungen an der Nachricht vornehmen und so falsche Informationen an das nächste Lager weitergeben.

Folglich ist die Veränderung schriftlicher Nachrichten kein sicheres Kommunikationsmittel. Die Verbreitung von Fehlinformationen könnte zum Sieg der böswilligen Generäle führen, da die verschiedenen Lager nicht gleichzeitig oder gar nicht angreifen würden. Auch im 21. Jahrhundert bleibt das Grundproblem bestehen: Wie kann man sicher sein, dass eine Nachricht authentisch ist und nicht verändert oder bösartig verändert wurde?

Authentizität bezieht sich auf die Gewissheit, dass die Gegenparteien Anrufe und E-Mails nicht gefälscht oder sich als jemand anderes ausgegeben haben. Manipulation bedeutet die Verfälschung, Löschung oder Einsichtnahme in die Nachricht durch böswillige Parteien.

Um das Problem der byzantinischen Generäle zu lösen, basieren die Konsensmechanismen auf zwei Konzepten:

1. Alle Generäle müssen zunächst einen Beitrag zum Netzwerk leisten, den sie nicht zurückbekommen, wenn sie sich nicht an die Regeln halten. Stellen Sie sich zum Beispiel zwei Geschäftsleute vor, die ein Joint Venture gründen wollen, aber einer von ihnen weigert sich, Zeit oder Kapital zu investieren. Der andere Geschäftsmann, der an der Sache beteiligt ist, würde die Loyalität des anderen in Frage stellen. Dies lässt sich auch auf dezentrale Netze anwenden.

2. Zweitens muss das Hauptbuch manipulationsfrei sein (in Bezug auf vergangene und aktuelle Transaktionen). Ein System ist manipulationssicher, wenn die Knoten im Netzwerk jede Änderung oder Löschung früherer Transaktionen und Daten sofort erkennen. Alle Nutzertransaktionen werden aufgezeichnet, überprüft und in einer Blockchain gespeichert.

Im Falle der byzantinischen Generäle könnte eine Lösung darin bestehen, dass die Generäle im Voraus eine hohe Summe als Zeichen ihrer Loyalität zahlen. Bevor ein General eine Nachricht weitergeben kann, müsste seine Identität durch eine kryptografisch gesicherte und eindeutige Signatur nachgewiesen werden. Wenn ein General den Angriff sabotiert, kann die Transaktionshistorie Aufschluss über die Identität der Person geben, die die Unterschrift leistet. Die Strafe für Böswilligkeit ist ein finanzieller Verlust für den General, da er die im Voraus geleistete Einlage nicht zurückerstattet bekommt. Das Erreichen eines Konsenses auf diese Weise wird als "Proof-of-Stake" bezeichnet. Alle Generäle haben im Vorfeld einen Anteil an der Aufrechterhaltung des Netzwerks investiert, um sich zu beteiligen. Eine andere Alternative wäre, dass jeder General ein komplexes mathematisches Problem lösen muss, bevor er eine Nachricht unterschreiben und versenden darf. Der General müsste eine Menge Geld an Arbeiter zahlen, die die mathematischen Probleme für ihn lösen. Diese Methode wird als Proof of work (PoW) bezeichnet. Jeder General beweist seine Loyalität gegenüber dem Netzwerk, indem er kostspielige und zeitaufwändige Ressourcen verbraucht.

Konsens in verteilten Systemen

Die Geschichte der Kryptowährungen und die Reihenfolge, in der Transaktionen validiert wurden, müssen unbedingt im Auge behalten werden. Wenn ein Netzwerkteilnehmer eine Transaktion erstellt, wird diese an das gesamte Netzwerk gesendet. Jeder Knoten zeichnet die neuen Transaktionen auf und fügt sie zu seiner Version des Hauptbuchs hinzu. Die Versionen des Ledgers unterscheiden sich geringfügig von einem zum anderen. Wenn ein in der EU ansässiger Knotenpunkt eine Transaktion sendet, erhalten die ihm am nächsten gelegenen Knotenpunkte diese früher als ein in den USA ansässiger Knotenpunkt. Dies führt zu leicht unterschiedlichen Versionen desselben Transaktionsverlaufs. Letztendlich müssen sich alle Netzwerkknoten auf eine bestimmte Reihenfolge einigen, und genau das erreicht der Konsensmechanismus einer Blockchain. Es gibt viele Ansätze, um einen Konsens in einem verteilten Netzwerk zu erreichen, die beiden bekanntesten sind der PoW- und der PoS-Algorithmus (Proof of Stake).

Nachweis der Arbeit

Der Begriff "Mining" ist z.B. aus Bitcoin bekannt. Das Ethereum-Netzwerk lief früher auf PoW als Konsensmechanismus, bei dem Transaktionen durch Mining in Blöcke verpackt und damit bestätigt werden müssen. PoW beschreibt die Bedingung, dass ein Teilnehmer des Netzwerks ehrliche und nachweisbare Arbeit geleistet haben muss, um eine Anzahl von Transaktionen zu bestätigen. Der Block Reward, den Miner erhalten, soll die aufgewendete elektrische Energie und den Einsatz spezieller Hardware (z.B. ASIC-Miner oder GPU) kompensieren und darüber hinaus einen Gewinn aus dem aktuellen Block Reward und den in den Transaktionen genehmigten Transaktionsgebühren erzielen. PoW ist die bisher am weitesten verbreitete Methode bei Kryptowährungen. Die hohen Einsätze beim Mining sorgen auch dafür, dass die dadurch erzeugten Coins einen realen Gegenwert in Form von Fiatgeld haben.

So robust und bewährt das Verfahren auch sein mag, es wird auch stark kritisiert. Der Nachteil von PoW ist der Verbrauch von elektrischer Energie und die manchmal speziell hergestellte Hardware wird auf Kosten der Umwelt verbraucht. Der Vergleich (basierend auf groben Zahlenschätzungen) mit häufig genutzten Diensten und Branchen (z.B. Netflix, YouTube) und dem Energieverbrauch von Bitcoin und Ethereum relativiert den Energieverbrauch von PoW und PoS.

	Annualized energy consumption (TWh)	Comparison to PoS Ethereum
Gold mining	240	92,000x
Gold mining	130	50,000x
Bitcoin	130	50,000x
Bitcoin	100	38,000x
YouTube	244	94,000 x
Global data centers	200	78,000x
Netflix	0.45	175x
Netflix	94	36,000x
PayPal	0.26	100x
Gaming in USA	34	13,000x
PoW Ethereum	78	30,000x
PoS Ethereum	0.0026	1x

Abbildung 6: Vergleich des jährlichen Energieverbrauchs von Dienstleistungen und Industrie (Quelle: Energieaufwand von Ethereum, Ethereum Foundation, 2022)

> Die Schätzungen des Energieverbrauchs von YouTube wurden auch nach Kanälen und einzelnen Videos aufgeschlüsselt. Diesen Schätzungen zufolge verbrauchte YouTube beim Anschauen von Gangnam Style im Jahr 2019 mehr als 175-mal so viel Energie wie Ethereum pro Jahr verbraucht.
>
> Ethereum-Stiftung, 2022

Während die Verringerung des Kohlenstoff-Fußabdrucks der Kryptowährung (durch die Nutzung erneuerbarer Energiequellen) wünschenswert ist, muss man die folgende Frage für sich selbst beantworten:

Sind die Funktionen, die Bitcoin und andere Kryptowährungen erfüllen, den Energieaufwand wert, den sie verursachen?

Ein weiterer Nachteil ist die Spaltung der Gemeinschaft bei diesen Projekten. Es gibt immer zwei Gruppen. Die Nutzer, die die Transaktionsgebühren aufbringen und auf die Bestätigungen warten müssen, und die Miner, die den Profit im Auge haben und vor allem für sich selbst einen politischen Gewinn aus dem Projekt ziehen wollen. Vorschläge zur Verbesserung des Projekts und seiner Quellcode-Implementierung lösen in der Regel Diskussionen aus, in denen beide Lager ihre eigenen Interessen vehement verteidigen.

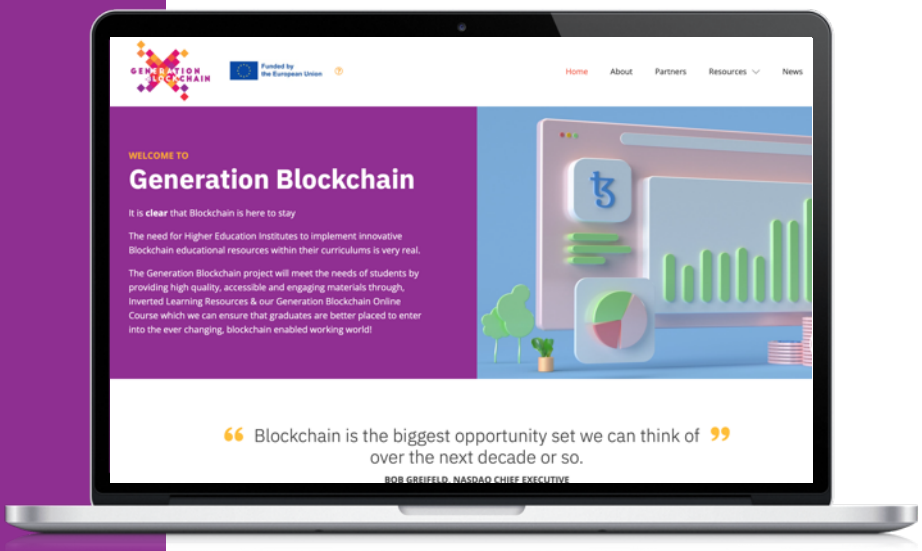
Proof of Stake

Wie beispielsweise in einer Aktiengesellschaft haben beim PoS alle Aktionäre das Recht, beim Konsens mitzureden. Diese Berechtigung, einen Block neuer Transaktionen zu validieren, wird jedes Mal deterministisch (durch Pseudozufall) zugewiesen. Bei diesem Prozess haben Aktionäre mit mehr Vermögen in ihren Wallets eine etwas höhere Chance, ausgewählt zu werden. Einerseits haben sie ein höheres Interesse an der Funktionalität des Netzwerks und sollten daher relativ mehr beitragen. Andererseits besteht bei einer zu heterogenen Auswahl der Anteilseigner die Gefahr, dass Blockbestätigungen zentralisiert werden und Parteien mit großen Anteilen an den Vermögenswerten gestärkt werden, was zu einer ungerechten Umverteilung des Reichtums führt. In den meisten Fällen werden bei PoS-basierten Blockchains die entsprechenden Token bereits "vorgebaut" (d. h. erstellt), anstatt wie bei PoW langsam durch Blockentdeckung in den Markt gespült zu werden, bis das festgelegte Maximum erreicht ist. PoS-Blockchains haben daher in der Regel bereits alle Anteile im Umlauf und können nur Aktionäre, die Blöcke gewinnen, mit Transaktionsgebühren bezahlen. Der Energieverbrauch beschränkt sich auf die einfache Nutzung durch die Teilnehmer und wird nicht durch komplexe Berechnungen in die Höhe getrieben, wie es bei PoW-Konsensmechanismen der Fall ist.

06

LERNKONTROLLE FÜR MODUL 1

Um Ihr Wissen zu testen, schließen Sie diese Lernkontrolle als Teil Ihrer Gesamtnote für den Kurs ab.
Klicken Sie hier.



Folgen Sie Ihrer Lernreise

www.generationblockchain.eu

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Co-funded by the European Union

Frankfurt School Blockchain Center · momentum [educate + innovate] · European E-Learning Institute · Amsterdam University of Applied Sciences · U.PORTO