BLOCKCHAIN REVOLUTION ITALIAN SUMMIT

www.blockchainrevolution.it

Blue Chain

www.bluechain.it

Glossary - blockchain and new tech

BLOCKCHAIN

Die Blockkette (Blockchain) ist ein virtuelles Transaktionsbuch in einem Netzwerk aus Rechnern. Jede Veränderung wird dabei erfasst und dezentral auf mehreren Rechnern verteilt und gespeichert. Dadurch bedarf es keiner zentralen Instanz mehr, wie einer Bank oder Behörde.

BLOCK

Ein Block ist eine Sammlung von Transaktionen die von einem sogenannten Miner veröffentlicht wurden. Das Ziel jeden Miners ist es, einen gültigen Block zu publizieren um so Rewards oder Fees zu erhalten.

KONSENS

Einigung der Mehrheit der Teilnehmer eines Netzwerks über die Gültigkeit einer historischen Abfolge von Transaktionen.

VALIDATOR-KNOTEN

Knoten in einem Netz, der zu der Gruppe von Validierern gehört, die für die Erstellung von Blöcken und die Übermittlung dieser Blöcke an das Netz verantwortlich sind. Um einen neuen Block zu erstellen, müssen die Prüfer die vom Konsensalgorithmus vorgegebenen Regeln befolgen.

PRIVATSCHLÜSSEL

In asymmetrischen kryptografischen Systemen verwendete Information, die es u n t e r anderem ermöglichen, ein Dokument auf nachprüfbare und nicht widerlegbare Weise zu "bestätigen". Bei Kryptowährungen wird sie in der Regel verwendet, um Überweisungen von einem Konto auf ein anderes zu tätigen. Die sichere Aufbewahrung des privaten Schlüssels ist eines der heikelsten Elemente bei der Verwendung von Kryptowährungen.

PROOF OF WORK

Konsensalgorithmus, bei dem der Benutzer ein komplexes mathematisches Problem lösen muss, um eine Transaktion zu verifizieren. Derjenige, der das Problem löst und damit zeigt, dass er oder sie eine Aufgabe erfüllt hat, erhält in der Regel eine Belohnung.

FORK

Die Bezeichnung aus dem Englischen lässt sich am besten als „Gabelung“ übersetzen. Aber was ist ein Fork? In der Praxis wird der Code einer bestehenden Blockchain derart modifiziert, dass eine vollkommen neue Blockchain ins Leben gerufen wird.

DISTRIBUTET-LEDGER-TECHNOLOGIE (DLT)

Tist eine spezielle Form der Datenverarbeitung und –speicherung. Als Distributed Ledger versteht man eine dezentrale Datenbank, die Teilnehmern eines Netzwerks eine gemeinsame Lese- und Schreibberechtigung erlaubt. Neue Datensätze können im Rahmen des Konsens-Mechanismus von jedem Nutzer (permissionless) oder nur von bestimmen Nutzern (persmissioned) hinzugefügt werden. Sie werden von allen Nodes (Nutzer) überprüft und dezentral gespeichert. Eine Form der DLT ist z.B. die Blockchain.

KRYPTOGRAPHIE

Kryptographie ist eine Methode zum Schutz von Informationen und Kommunikation durch die Verwendung von Computercodes. Eine Blockchain verwendet zwei verschiedene Arten von kryptografischen Algorithmen, die asymmetrischen Schlüsselalgorithmen und Hash-Funktionen.

PEER-TO-PEER

ist eine verteilte Rechnerarchitektur, d.h. eine Rechnerstruktur, in der mehrere Einzelrechner miteinander interagieren. Die Knotenpunkte (d. h. jedes Gerät, das mit den anderen im gleichen Netz kommunizieren kann) werden als "gleichwertig" bezeichnet, weil sie gleichzeitig Server und Client sind, die gleiche hierarchische Ebene haben und sich ohne zentrale Instanzen koordinieren.

MINING

Prozess, bei dem Bitcoin-Transaktionen verifiziert, in Blöcken gruppiert, validiert und der Blockchain hinzugefügt werden. Dies geschieht durch die Lösung kryptographischer Aufgaben, die einen gewissen Zeit- und Energieaufwand erfordern, der durch Gebühren und die Ausgabe neuer Werte belohnt wird.

HASHING - HASH

Ergebnis einer Funktion, die Daten in eine einseitige Hash-Zeichenkette fester Länge umwandelt, aus der sich nicht auf die Eingabedaten zurückschließen lässt. Ein Hash kann als die elektronische Version eines Fingerabdrucks für jede Art von Daten angesehen werden.

PROOF OF STAKE

Konsensalgorithmus, bei dem Registerentwicklungen nicht mit Rechenaufwand validiert werden, sondern bei dem die Nutzer die Gültigkeit von Transaktionen garantieren, indem sie einen Teil ihrer Kryptowährungen einsetzen, d.h. verpfänden. Für die Prüfer besteht somit ein Anreiz, sich ehrlich zu verhalten, um das, was sie zugesagt haben, nicht zu verlieren.

INTERNET DER WERTE

Digitales Netzwerk von Knotenpunkten, die Werte übertragen durch ein System von Algorithmen und Regeln kryptographische Regeln. Dieses Netz ermöglicht es, die Konsens, auch bei fehlendem Vertrauen, über die Änderungen, die an einem verteilten Hauptbuch vorgenommen werden sollen das die Übertragungen von einzigartigen einzigartige digitale Werte.

DEZENTRALISIERUNG

Dezentralisierung bedeutet die Übertragung der Kontrolle über eine Aktivität oder Organisation auf mehrere Standorte oder Autoritäten und nicht auf eine einzelne. Im Blockchain-Glossar bezieht sich Dezentralisierung auf die Übertragung von Kontrolle und Entscheidungsfindung von einer Entität auf ein verteiltes Netzwerk. Dezentrale Blockchains sind unveränderlich und eliminieren eine Reihe von Risiken

KONSENSVERFAHREN

Das Konsensverfahren ist der entscheidende Baustein, um die Blockchain vor Manipulationen zu schützen. Es verhindert, dass ein Teilnehmer einen Wert mehrfach nutzt – also beispielsweise einen Betrag mehrfach transferiert, obwohl er nur einmal vorhanden ist. Das Konsensverfahren löst dieses „Double-Spending-Problem": Erst wenn die Mehrheit der angeschlossenen Nodes sich über die Schaffung eines bestimmten neuen Blocks einig ist, wird dieser validiert und an die zuvor erstellten Blöcke angehängt.

NODE

Computer im Netzwerk, der eine Kopie des Blockchain-Ledgers verwaltet.

PUBLIC KEY

Der private Schlüssel ist geheim und entspricht in etwa dem Passwort – er sollte also den Computer, auf dem er generiert wurde, niemals verlassen und mit Sorgfalt behandelt werden. Der öffentliche Schlüssel wiederum ist öffentlich und kann frei weitergegeben werden

ELEMENTE DIE EINEN BLOCK BILDEN:

- Index, die absolute Nummer des Blocks, d.h. seine Position innerhalb der Kette
- Zeitstempel, die Uhrzeit, zu der der Block erzeugt wurde
- der HASHWERT des vorherigen Blocks
- Alle Informationen, die sich auf den Wert des Blocks beziehen
- HASH des Blocks selbst, d. h. sein Identifizierungscode, der von allen oben beschriebenen Daten abhängt
- NONCE ist die Zahl, die, wenn sie zu den anderen Daten addiert wird, einen Hash mit einer bestimmten Anzahl von Nullen erzeugt, der zum Schließen und Validieren des Blocks verwendet wird. Die Aufgabe der Miner ist es, die Nonce zu finden.

SMART CONTRACT

Smart Contracts sind Computerprotokolle, die Verträge abbilden oder überprüfen oder die Verhandlung oder Abwicklung eines Vertrags technisch unterstützen können. Eine schriftliche Fixierung des Vertrages wird damit unter Umständen überflüssig.

IoT

Das Internet der Dinge ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.

AI
Künstliche Intelligenz ist der Versuch, menschliches Lernen und Denken auf den Computer zu übertragen und ihm damit Intelligenz zu verleihen. Statt für jeden Zweck programmiert zu werden, kann eine KI eigenständig Antworten finden und selbstständig Probleme lösen.

TOKEN
Eine bestimmte Art von digitalen Vermögenswerten, die über eine Blockchain gehandelt werden können. Token werden häufig als Repräsentation anderer digitaler oder fester Vermögenswerte oder eines Rechts verwendet, z. B. des Eigentums an einem Vermögenswert oder des Zugangs zu einer Dienstleistung.

METAVERSUM
Ein Metaversum oder Metaverse ist ein digitaler Raum, der durch das Zusammenwirken von virtueller, erweiterter und physischer Realität entsteht. Hauptaspekt ist es dabei die verschiedenen Handlungsräume des Internets zu einer Wirklichkeit zu vereinigen.

CYBER-SICHERHEIT
ist die Praxis des Schutzes von Systemen, Netzen und Programmen vor digitalen Angriffen. Cybersicherheit, auch bekannt als digitale Sicherheit, ist die Praxis des Schutzes digitaler Informationen, Geräte und persönlicher Werte. Dazu gehören persönliche Daten, Konten, Briefe, Fotos und sogar Geld.

CLOUD
Eine Cloud ist eine IT-Ressource, die via Internet verfügbar gemacht wird. Bei diesen Ressourcen kann es sich um Speicherplatz, Rechenleistung, Software (Web-Anwendungen) oder komplette IT-Infrastrukturen handeln.

BIG DATA
Big Data ist ein Synonym für große Datenmengen und zeichnet sich vor allem durch folgende Hauptmerkmale aus: Größe, Komplexität, Schnelllebigkeit und schwache Strukturierung. Bei der Auswertung von Big Data stoßen manuelle und herkömmliche Methoden der Datenverarbeitung schnell an ihre Grenzen.

ROBOTIK
Das Themengebiet der Robotik befasst sich mit dem Versuch, das Konzept der Interaktion mit der physischen Welt auf Prinzipien der Informationstechnik sowie auf eine technisch machbare Kinetik zu reduzieren.

NFT (Nicht-fungibler Token)
Ein Non-Fungible Token ist ein „kryptografisch eindeutiges, unteilbares, unersetzbares und überprüfbares Token, das einen bestimmten Gegenstand, sei er digital oder physisch, in einer Blockchain repräsentiert“

ON CHAIN
Ein Ausdruck, der herkömmliche Blockchain-Transaktionen qualifiziert, vom Netzwerk validiert und in einem Block im Hauptnetzwerk aufgezeichnet wird.

OFF CHAIN
Dieser Ausdruck bezieht sich auf Transaktionen, die nicht in der Blockchain aufgezeichnet werden, sondern separat validiert werden.
Diese Systeme werden im Allgemeinen eingesetzt, um die Geschwindigkeit oder die Vertraulichkeit von Transaktionen zu erhöhen.

SIDE CHAIN
Eine Sidechain ist eine Blockchain, die von einer übergeordneten Blockchain abgespalten wurde und seither in gewissen Grenzen eigenständig arbeiten kann. Sie ist jedoch weiterhin mit ihrer ursprünglichen Blockchain verbunden, sodass z. B. Assets zwischen beiden Blockketten ausgetauscht werden können. Eine Blockchain kann mehrere Sidechains zugleich besitzen.

MINER
Miner sind Computerbesitzer, die dem Netzwerk einer Kryptowährung, die auf einem “Proof-of-Work” Protokoll basiert, die Rechenleistung ihrer Computer zur Verfügung stellen. Wer als erster einen neuen Block überprüft, wird mit neu generierten Einheiten der Kryptowährungen belohnt.

CRYPTOVALUE
Eine dezentralisierte digitale Währung, die kryptographische Techniken und Systeme zur Angleichung von Anreizen verwendet, um die Sicherheit des Austauschs zwischen den Nutzern zu gewährleisten. Anders als bei herkömmlichen Währungen gibt es keine zentralen Stellen, die Transaktionen vermitteln, und die Regeln, nach denen der Austausch erfolgt, sind in einer öffentlich überprüfbaren Open-Source-Software geschrieben.

WALLET
Ein privates Schlüsselspeichersystem, an das Kryptowährungen angeschlossen sind und das mit der jeweiligen Blockchain kommunizieren kann. Die „Brieftasche“ kann online, online oder auf einem festen Gerät sein.

STABLECOINS
Digitale Vermögenswerte, die die für Kryptowährungen typischen Garantien und Eigenschaften aufweisen, deren Preis jedoch gegenüber einem Referenzwert stabilisiert wird, bei dem es sich um eine Fiat-Währung wie den Dollar oder den Euro, einen Vermögenswert wie Gold oder einen Preisindex handeln kann.

BITCOIN
Die erste Kryptowährung, die die Blockchain-Technologie verwendet. Bitcoin, wurde 2008 geboren und 2009 von einer Person oder einer Gruppe von Personen eingeführt, die sich unter dem Pseudonym SatoshiNakamoto identifizierten.

ETHEREUM
Ethereum ist ein quelloffenes verteiltes System, welches das Anlegen, Verwalten und Ausführen von Programmen bzw. Kontrakten in einer eigenen Blockchain anbietet. Es stellt damit einen Gegenentwurf zur klassischen Client-Server-Architektur dar.

ZERO KNOWLEDGE PROOF
Ein Null-Wissen-Beweis kann mit hoher Wahrscheinlichkeit nachweisen, dass man ein Geheimnis weiß, ohne das Geheimnis zu verraten. Dieser Nachweis passiert meist nach einem Frage-Antwort-Protokoll und hat viele Anwendungen in der Kryptografie. Eine Partei versucht zu beweisen, die andere Partei verifiziert.

DOUBLE SPENDING
Situation, in der ein Nutzer versucht, dieselbe digitale Währung mehrmals auszugeben, z. B. indem er dieselbe Zahlung an zwei verschiedene Empfänger schickt.

DAPP
DApp steht für „dezentrale Applikation“ bzw. „decentralized Application“. Bei diesem Konzept werden die elementaren Werte und Zustände, anders als bei üblichen Applikationen, nicht auf einer einzigen Maschine, sondern in einem Netzwerk von Maschinen, wie einem Peer-to-Peer-Netzwerk, gespeichert und verifiziert.

GOVERNANCE
Eine Reihe von Regeln und Verfahren, die die Verwaltung einer Blockchain-Plattform und die Art und Weise regeln, in der Änderungen vorgeschlagen und möglicherweise an ihrem Betrieb vorgenommen werden können.

ICO
Initial Coin Offering oder auch Initial Public Coin Offering ist eine oftmals unregulierte Methode des Crowdinvestings, die von Unternehmen verwendet wird, deren Geschäftsmodell auf Kryptowährungen basiert.

ORACLE
Ein Blockchain-Orakel ist ein Dienst von Drittanbietern, der Smart Contracts mit der Außenwelt verbindet, in erster Linie um Informationen aus der Welt einzuspeisen, aber auch umgekehrt. Informationen aus der Welt kapseln mehrere Quellen, so dass dezentrales Wissen gewonnen wird.

BLOCKCHAIN ADRESSE
Jedes Bitcoin Wallet besitzt eine individuelle öffentliche Adresse, mit der das digitale Portemonnaie in der Bitcoin-Blockchain eindeutig identifizierbar ist. Gekaufte Bitcoins oder andere Zahlungen werden an diese Adresse überwiesen und landen kurze Zeit später im Wallet.

OPEN SOURCE
Als Open Source wird Software bezeichnet, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann. Open-Source-Software kann meistens kostenlos genutzt werden.