

GLOBAL BLOCKCHAIN GLOSSARY OF TERMS

- English
- Español
- Deutsche
- عربي
- 中国



Please enjoy this resource of Global Blockchain Terms 2.0; now released in 5 languages. We hope this will continue our mission of providing value to the blockchain community.

Thank you to our contributors: Ulla Gomez, Thomas Wiesner, Aladin Abdelkawi, Wilbert Salinas, Rosa Santos, NGN



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH



51% Attack

A situation in which a majority of miners in the blockchain launch an attack on the rest of the nodes (or users). This kind of attack allows for double spending or stealing assets.



Agreement Ledger

A distributed ledger used by two or more users to negotiate and reach agreement



Block Height

Number of blocks connected together in the block chain



Byzantine Fault Tolerance (BFT)

Byzantine fault tolerance (BFT) is the property of a system that is able to resist the class of failures derived from the Byzantine Generals' Problem. This means that a BFT system is able to continue operating even if some of the nodes fail or act maliciously.



Chaincode

A program that initializes and manages a ledgers state through submitted applications



Coinbase

The largest exchange for buying and selling Bitcoin & converting Bitcoin into dollars or other currencies.



Consensus

The agreement of all participants of a network on the validity of a transaction



Cryptocurrency

A digital currency based on mathematics, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Cryptocurrencies operate independently of a central bank.



Dagger Hashimoto

The proposed spec for the mining algorithm in Ethereum 1.0



ABI (Application Binary Interface)

An interface between two binary program modules, often one program is a library and the other is being run by a user



Alt-coin

Any cryptocurrency that exists as an alternative to bitcoin



Blockchain (Public)

A mathematical structure for storing digital transactions (or data) in an immutable, peer-to-peer ledger that is incredibly difficult to fake and yet remains accessible to anyone.



Casper

Consensus algorithm that combines proof of work and proof of stake. Ethereum is going to use Casper as a transition to proof of stake.



Channel

A Blockchain channel is a separate data channel allowing nodes to communicate in private, or transactions to be funded, etc., without the entire network seeing it.



Composer CLI

Hyperledger command line allowing for administrative tasks



Consensus Process

The process of reaching consensus on a ledger's content



CRUD

Create, retrieve, update, delete



DApps

Decentralized Applications



Address

Address (Cryptocurrency address) is used to send and receive transactions on the network



API

Application Programming Interface (part of a remote server that sends requests and receives responses)



Business logic layer

A part of code that determines the rules to be followed when doing business



CDN (Content Delivery Network)

Allows for a quick transition of assets needed to load internet content (html, js, css, etc.)



CLI

Command Line Interface



Composer Rest Server

Generates a REST API from a deployed Blockchain



Consortium Blockchain

A blockchain where the consensus process is controlled by a pre-selected set of nodes.



Cryptographic Hash Function

A function that receives an input of any size and returns a unique string of a uniform length



DDoS Attacks

A Distributed Denial-of-Service (DDoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet



Aggregated Transactions

Merging multiple transactions into one, allowing trustless swaps, and other advanced logic. Used in NEM.



Bitcoin

The first, and most popular, cryptocurrency based off the decentralized ledger of a blockchain created in 2009.



Business network card

Provides necessary information to connect a blockchain business network



Centralized

Maintained by a central, authoritative location or group



Coin

Representation of a digital asset built on a new blockchain



Confirmation

Indication that the blockchain transaction has been verified by the network through mining



Container Technology

A solution to run a software application reliably when deployed in a different environment other than the one in which it was created. Such as Docker or Kubernetes.



Cryptography

A method for securing communication using code



Decentralization

The transfer of authority and responsibility from a centralized organization, government, or party to a distributed network.



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH



Difficulty

Indication of how hard it is to verify blocks in Proof-of-Work mining



Decentralized

The concept of a shared network of dispersed computers (or nodes) that can process transactions without a centrally located, third-party intermediary.



Digital Asset

Any digital data that is formatted into binary code and includes the right to use it.



Digital Identity

A digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization, or electronic device.



Digital Signature

A mathematical scheme used for presenting the authenticity of digital assets



Double Spend

A scenario where someone tries to send a bitcoin transaction to two different recipients at the same time



Enum

A data type that represents the enumeration of values of the same type



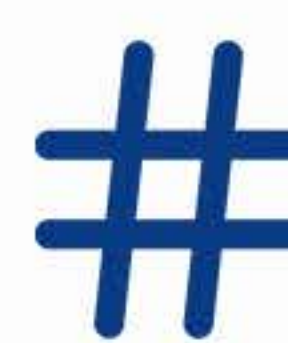
EOA

Externally Owned Account



ERC20

Ethereum request for comments standard



ET-Hash

The proof of work algorithm used by Ethereum 1.0



Ethereum

Blockchain application that uses a built-in programming language that allows users to build decentralized ledgers modified to their own needs. Smart contracts are used to validate transactions in the ledger.



Exchange

A place to buy and sell cryptocurrency



Fiat

Legal tender whose value is backed by the government that issued it. Ex: USD, EUR, CNY, JPY



FITS model for Blockchain applicability

A model for assessing the applicability of blockchain using: Fraud is prevalent, Intermediaries exist, Throughput is needed, Stable data is in the application.



Fork

A collectively agreed upon software update by all the nodes on the network.



Fungibility

The ability of a good or asset to be interchanged with other individual goods or assets of the same type. Applicable to Corda Distributed Ledger



Gas (Ethereum)

A measure of how much Ether is paid for a given action performed in Ethereum Blockchain



Genesis Block

The initial block within a blockchain



GitHub

A web based hosting service for version control using git. Used by blockchain



Golang (Google language)

Created by google in 2009, Golang is a programming language based on C



Gossip Protocol

A gossip protocol is a procedure or process of computer-computer communication that is based on the way social networks disseminate information or how epidemics spread. It is a communication protocol



Governance

The rules that are established for a Blockchain that determine how it is governed, administrated, and managed or protected



Hard Fork

Alters the blockchain data in a public blockchain. Requires all nodes in a network to upgrade and agree on the new version.



Hardware Wallet

A physical device that can be connected to the web and interact with an online exchange



Hash Function

A function that maps data of an arbitrary size



Hot Wallet

A wallet that is directly connected to the internet at all times



Hot/Cold Wallet

A cryptocurrency description where Hot wallets are like checking accounts whereas cold wallets are like savings accounts.



Hyperledger

Started by the Linux Foundation, Hyperledger is an umbrella project of open source blockchains



Hyperledger Composer

Hyperledger Composer is Blockchain Application Development framework which simplifies the blockchain application development on Hyperledger Fabric



Hyperledger Fabric

Hyperledger project hosted by Linux which hosts Smart Contracts called Chaincode



IDE (Integrated development Environment)

Application for software developers that primarily consists of a source code editor, build automation tool, and debugger



Immutable

"unable to be changed". Data stored in a blockchain is unable to be changed.(not even by administrators)



Initial Coin Offering (ICO)

The form in which capital is raised to fund new cryptocurrency ventures. Modeled after an Initial Public Offering (IPO). Funders of an ICO receive tokens.



Instantiate(d)

To instantiate is to create an instance of an object in an object-oriented programming (OOP) language. An instantiated object is given a name and created in memory or on disk using the structure described within a class declaration.



Invariant

A function, quantity, or property that remains unchanged when a specified transformation is applied.



IPFS

Inter Planetary File System



JSON

"JavaScript Object Notation" and is pronounced like the name "Jason". JSON is a text-based data interchange format designed for transmitting structured data. It is most commonly used for transferring data between web applications and web servers.



Kubernetes(s)

A set of building blocks ("primitives"), which collectively provide mechanisms that deploy, maintain, and scale applications. Also defined as an open-source container-orchestration system for automating deployment, scaling and management of containerized applications.



Ledger

An append-only store of records



Liquidity

The ability of an asset to be converted into cash



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH



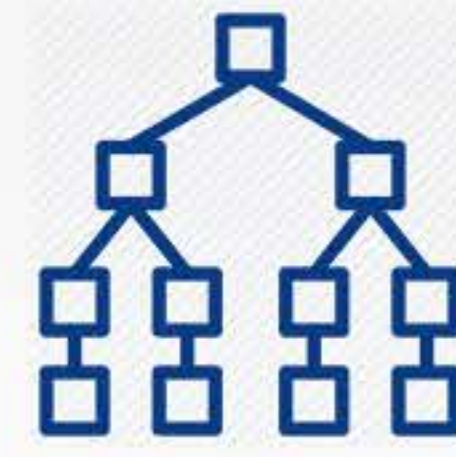
Lightning Network

A decentralized network using Smart Contract functionality in the blockchain to enable instant payments across a network of participants.



Market Cap

Total value held in a cryptocurrency



Merkle Tree

A tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes



Mining

The act of validating blockchain transactions. Requires computing power and electricity to solve "puzzles". Mining rewards coins based on your computing power.



Mining pool

A collection of miners who come together to share their processing power over a network and agree to split the rewards of a new block found within the pool



Mist

Browser for installing and using Dapps



MSP (Membership Service Provider)

A Hyperledger Fabric blockchain network can be governed by one or more MSPs



Multisignature (transaction)

Multi signature transactions require multiple parties to approve the transaction, determined by the rules.



Node

A copy of the ledger operated by a user on the blockchain



Nonce

A number only used once in a cryptographic communication (often includes a timestamp)



Nothing at Stake problem

This is caused by validator nodes approving all transactions on old and new software after a hard fork occurs



NPM (Node Package Manager)

Default package manager runtime environment node.js. NPM manages dependencies for an application.



Oauth protocol

Open Authorization is a standard that is used by third party services to keep and distribute user's information without exposing their password



Ommmer (aka Uncle)

A block which has been completely mined but has not yet been added to the Blockchain



On-chain governance

A system for managing and implementing changes to a cryptocurrency blockchain



Oracle

An interface that connects smart contracts and data sources



Orderer Network

A computer network that allows nodes to share resource



P2P (Peer to Peer)

Decentralized model where two parties complete a transaction without an intermediary third party. The buyer and seller interact directly.



PKI (Public Key Infrastructure)

A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.



Pragma(s) or Pragma-line

Defines which compiler version the smart contract uses



Private Blockchain

Blockchain that can control who has access to it. Contrary to a public blockchain a Private Blockchain does not use consensus algorithms like POW or POS, instead they use a system known as byzantine fault tolerant(BFT). BFT is not a trustless system which makes a BFT system less secure.



Proof of Activity

Active Stakeholders who maintain a full node are rewarded



Proof of Burn

Miners send coins to an inactive address essentially burning them. The burns are then recorded on the blockchain and the user is rewarded.



Proof of Capacity

Plotting your hard drive (storing solutions on a hard drive before the mining begins). A hard drive with the fastest solution wins the block



Proof of Elapsed Time

Consensus algorithm in which nodes must wait for a randomly chosen time period and the first node to complete the time period is rewarded



Proof of Stake (POS)

A consensus algorithm that chooses the owner of a new block based on the wealth they have or (Stake). There is not a block reward so the forgers take the transaction fee



Proof of Work (POW)

A consensus algorithm which requires a user to "mine" or solve a complex mathematical puzzle in order to verify a transaction. "Miners" are rewarded with Cryptocurrencies based on computational power.



Proof of Importance

Proof-of-Importance is a Blockchain consensus mechanism in NEM. Similar to proof-of-stake: nodes need to 'vest' an amount of currency to be eligible for creating blocks and are selected for creating a block roughly in proportion to some score.



Pub/Sub

Publish/Subscribe



Public Blockchain

A publically accessible blockchain



Public key cryptography

Encryption that uses two mathematically related keys. A public and private key. It is impossible to derive the private key based on the public key.



REST API (representational state transfer API)

Defines restraints based on HTTP



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH



RPC (Remote Procedure Calls)

A protocol that is used from one program to request a service on another program located on a network



RSA

RSA encryption system to encrypt a message with an individual's public key so that only that individual can decrypt the message in a reasonable amount of time



Satoshi Nakamoto

An individual or entity who created Bitcoin protocol having successfully solved the digital currency issue of the 'double spend'



Segwit

The process by which the block size limit on a blockchain is increased by removing signature data from Bitcoin transactions



SDK

A software development kit provides the necessary tools for a developer to create software on a specific platform



SHA-256

SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. SHA-256 is used in several different parts of the Bitcoin network: Mining uses SHA-256 as the Proof of work



Sharding

Dividing a blockchain into several smaller component networks called shards capable of processing transactions in parallel



Smart Contract

Self-executing contract with the terms of agreement written into the code



Solidity

A programming language used for writing smart contracts on the Ethereum network



Stablecoin

The definition for a cryptocurrency designed to minimize the effects of price volatility such as being pegged to a currency, or to exchange traded commodities (such as precious metals).



Stake Weighting

A function of Proof-of-Stake where the weight of his or her "vote" is a function of the proportion of tokens he or she owns



Token

Representation of a digital asset built on an existing blockchain



Token Economics

The study, design, and implementation of economic systems based on blockchain technology.



Tokenless Ledger

A ledger that doesn't require a native currency to operate



Turing Complete language

A language that is able to perform calculations that a computer is capable of



Ubuntu

Free open source operating system and linux distribution



UTXO (Unspent Transaction Outputs)

Unspent transaction outputs are used to determine whether a transaction is valid



Virtual Machine

Emulation of a computing system



VMware

Subsidiary of Dell that provides cloud computing and platform virtualization software and services



VMware Player

Virtualization software package for x64 Computers running Microsoft or Linux



VYPER

A programming language created to be a formal introduction to smart contracts



Wallet

Stores the digital assets you own



Zeppelin (or Open Zeppelin)

Community of like-minded Smart Contract developers



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Español



Ataque del 51%

Es una situación en la cual una mayoría de mineros en la blockchain lanzan un ataque contra el resto de los nodos o usuarios). Este tipo de ataque permite un doble gasto o el robo de bienes.



Acuerdo de Registro

Un registro distribuido usado por dos o mas usuarios para negociar y alcanzar acuerdos.



Altura del Bloque

Numero de bloques conectados juntos en la Blockchain.



Tolerancia a faltas bizantinas (BFT)

La tolerancia a faltas bizantinas (BFT) es la propiedad de un sistema para resistir a una serie de fallos derivados de lo que se conoce como el "problema de los generales bizantinos". Esto significa que un sistema BFT es capaz de seguir operando, aunque algunos de sus nodos fallen o actúen de forma hostil.



Chaincode

Un programa que inicia y gestiona el estado del libro contable a través de aplicaciones implementadas



Coinbase

Es la mayor plataforma para la compraventa de Bitcoin y la conversión de Bitcoin a dólares u otra moneda



Consenso

Situación en la que todos los participantes de la red llegan a un acuerdo en cuanto a la validez de una transacción



Criptomoneda

Es una moneda digital basada en calculos matematicos, en esta se utilizan tecnicas de encriptacion las cuales son usadas para regular la creacion de unidades de moneda y verificar la transferencia de fondos. Las criptomonedas operan de forma independiente de un banco central.



Dagger Hashimodo

Propuesta especifica para un algoritmo de mining en Ethereum 1.0



Interfaz binaria de aplicación (ABI)

Una interfaz entre dos módulos de programa binarios, uno de ellos a menudo es una librería y el otro es ejecutado por un usuario



Altcoin

Cualquier criptomoneda que existe como alternativa al Bitcoin



Blockchain (pública)

Una estructura matemática para el registro de transacciones digitales (o datos) sobre una base de datos permanente en un registro de red P2P. Altamente resistente a las falsificaciones y a la par accesible a cualquiera.



Casper

Algoritmo de consenso que combina la prueba de trabajo (PoW) y prueba de participación (PoS). Ethereum usara Casper como una transición hacia prueba de participación (PoS).



Canal

Un canal blockchain es un canal separado del resto que permite a los nodos comunicarse en privado, o el pago de transacciones etc, sin que el resto de la red lo vea.



Composer CLI

Línea de comando Hyperledger que posibilita tareas administrativas



Proceso de Consenso

Proceso en el cual se llega a un acuerdo sobre el contenido de un registro.



Funciones CRUD

Crear, recuperar, actualizar y borrar



Dapps

Aplicaciones Descentralizadas



Dirección (Address)

Dirección (Dirección de Criptomonedas) es usada para enviar y recibir transacciones en la red.



API

Interfaz de programación de aplicaciones (parte de un servidor remoto que envía peticiones y recibe respuestas)



Capa de lógica de negocios / lógica empresarial

Es la parte del código que determina las reglas a seguir a la hora de hacer negocios



Red de entrega de contenidos (CDN)

Permite la transición rápida de activos necesarios para cargar contenido en internet (html, js, css, etc.)



CLI

Interfaz de línea de comandos (CLI)



Servidor Composer Rest

Genera una API rest desde una blockchain existente



Consorcios blockchain

Un consorcio de blockchain es tipo de blockchain en la cual el proceso de consenso está controlado por un subgrupo preseleccionado de nodos



Función hash criptográfica

Una función que recibe una entrada de cualquier longitud y devuelve un código único de longitud fija



Ataque de denegación de servicio (DoS)

Un ataque de denegación de servicio es un ciberataque con el que se pretende hacer inaccesible un recurso o servicio a la red de usuarios legítimos, interrumpiendo de forma temporal o permanente los servicios de un host conectado a internet.



Transacciones agregadas

Consolida múltiples transacciones en una sola transacción, haciendo posible intercambios no seguros entre terceros (swaps) así como otro tipo de lógica avanzada. Utilizadas en NEM



Bitcoin

La primera y más conocida criptomoneda, basada en un registro descentralizado blockchain y creada en el año 2009



Tarjeta de red empresarial

Aporta la información necesaria para conectar a una red empresarial blockchain



Centralizado

Mantenido por una central, con localización autoritaria o grupo



Moneda digital (coin)

Representación de un activo digital construido sobre tecnología blockchain



Confirmación

Señal que indica cuando la transacción de blockchain ha sido verificada por la red a través de la minería.



Containers (tecnología de contenedores)

Una solución confiable para la ejecución de aplicaciones de software cuando éstas se instalan en un entorno diferente al entorno en el que se crearon. Por ejemplo, Docker o Kubernetes



Criptografía

Metodo para proteger comunicaciones usando codigos.



Descentralización

Es la transferencia de autoridad y responsabilidades de una organización central, gobierno o grupo a una red distribuida.



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Español



Dificultad

Indicativo de que tan duro es verificar los bloques en una minería con Prueba-de-Trabajo.



Descentralizado

El concepto de una red compartida de ordenadores dispersos (o nodos) que pueden procesar transacciones sin un tercero o intermediario



Activo / recurso digital

Cualquier archivo de texto o contenido multimedia que está



Identidad Digital

Una identidad digital es un tipo de identidad adoptada o reclamada en el ciber-espacio por un individuo, organización o un dispositivo electrónico.



Firma electrónica / digitalizada

Un mecanismo matemático utilizado para identificar la autenticidad de activos digitales



Doble Gasto (Double Spend)

En este escenario alguien trata de enviar una transacción bitcoin a dos diferentes recipientes a la misma vez.



Enumerado (Enum)

Una clase de valor de dirección



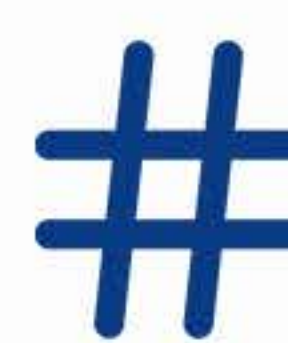
EOA

Cuentas externas



ERC20

(Estándar para solicitud de comentarios Ethereum). Una regla estándar usada para contratos inteligentes en una Blockchain Ethereum



ET-Hash

El algoritmo PoW (prueba de trabajo) utilizado en Ethereum 1.0



Ethereum

Aplicación blockchain que usa lenguaje de programación incorporado que permite a sus usuarios crear registros descentralizados adaptados a sus necesidades particulares. Utiliza contratos inteligentes (Smart contracts) para validar las transacciones en el registro principal.



Exchange

Lugar en el cual se compran y venden criptomonedas.



Fiat (Garantía)

Oferta legal, la cual esta respaldada por el gobierno que la emite. Ejemplo: Dolares, Euros, CNY, JPY.



Modelo para aplicación blockchain FITS

Determina si corresponde el uso de una blockchain cuando: prevalece el fraude, existen intermediarios, se requiere rendimiento, la aplicación contiene datos estables.



Fork (bifurcación)

Es básicamente una actualización del software acordada de forma colectiva por todos los nodos en la red.



Fungibilidad / de carácter fungible

La capacidad de un bien o activo de poder ser intercambiado por otros bienes individuales o activos de carácter similar. Aplicable al registro distribuido CORDA



Gas (Ethereum)

Una medida de cuanto Ether es pagado por una transacción en la Blockchain Ethereum



Bloque génesis / bloque 0

El primer bloque dentro de una blockchain



Github

Un servicio de alojamiento web para el control de versiones utilizando git. Usado por programadores blockchain



Golang (lenguaje Go)

Golang es un lenguaje de programación basado en C y creado por Google en 2009



Protocolo chisme

El protocolo de chisme (gossip protocol) es un procedimiento o proceso de comunicación entre computadoras basado en la manera de divulgar información en las redes sociales y de funcionamiento similar a cómo se propaga una epidemia.



Gobernanza

Las reglas sobre las cuales se establece una blockchain y que determinan cómo se gobierna, administra, gestiona y protege



Hard fork (bifurcación fuerte)

Modifica los datos de una blockchain pública. Requiere que todos los nodos en la red acepten la nueva versión y hagan una actualización.



Monedero Físico (Hardware Wallet)

Es un dispositivo físico que puede ser conectado a la red e interactúa con un intercambio (exchange) en activo.



Función hash

Una función que analiza y dibuja los datos de tamaño arbitrario.



Monedero en línea (Hot Wallet)

Un monedero que esta conectado directamente al internet todo el tiempo.



Monedero en línea / fuera de línea

Una descripción de criptomoneda en la que los monederos online son equiparables a cuentas corrientes, mientras que los monederos fuera de línea son como cuentas de ahorro



Hyperledger

El proyecto Hyperledger es una plataforma de código abierto para blockchain iniciado por la Fundación Linux.



Hyperledger Composer

Hyperledger Composer es un conjunto de herramientas blockchain que simplifican la construcción de aplicaciones de blockchain en Hyperledger Fabric



Hyperledger Fabric

Un proyecto Hyperledger hospedado por Linux que aloja contratos inteligentes llamados chaincode



Entorno de Desarrollo Integrado (IDEI)

Una aplicación para programadores, que consiste en un editor de código, un compilador y un depurador



Inmutable

"Incambiable", la información registrada en una blockchain es permanente, inmodificable incluso para administradores



Oferta inicial de monedas (ICO)

El proceso de captación de capital para la financiación de empresas usando criptomonedas. Los financiadores de una ICO reciben "tokens".



Instanciar / instaciado

Instanciar es crear una instancia de un objeto en un lenguaje de programación orientado a objetos (OOP). Un objeto instanciado recibe un nombre y se crea en la memoria o disco, usando la estructura descrita dentro de una declaración de su clase



Invariable

Una función, cantidad o propiedad que permanece de forma inalterada cuando se aplica una transformación específica



Sistema de archivos interplanetarios (IPFS)

Sistema de archivos interplanetarios



JSON

JSON (notación de objeto de JavaScript), pronunciado "Jason".JSON es un formato de texto para el intercambio de datos, diseñado para la transmisión de estructuras de datos. Se emplea habitualmente para transferir datos entre aplicaciones web y servidores web.



Kubernet(s)

Definido como un conjunto de bloques de construcción ("primitivos"), que, de forma colectiva, proporcionan mecanismos que instalan, mantienen y escalan aplicaciones. También se le describe como un sistema de código libre para el manejo de aplicaciones en contenedores, automatización del despliegue, escala y manejo de aplicaciones de contenedores.



Registro Principal

Una base única e inmodificable para guardar registro de actividades.



Liquidez

La habilidad que tiene un activo para ser convertido en dinero en efectivo.



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Español



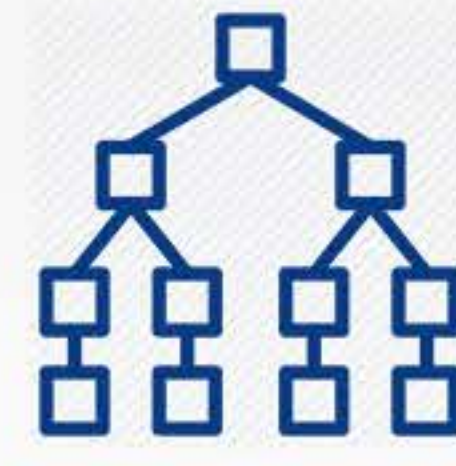
Red Lightning

Es una red descentralizada que usa funcionalidad "smart contract" (contratos inteligentes) en la blockchain para proporcionar pagos instantáneos entre los usuarios de una red



Capitalización de Mercado o Market Cap

Es el valor total retenido en una criptomoneda



Arbol de Merkle

Una estructura de datos en árbol, en la cual cada nodo hoja está etiquetado con el hash de un bloque de datos, y cada nodo que no es una hoja, está etiquetado con un hash criptográfico de las etiquetas de sus nodos hijos.



Mining (minería blockchain)

El acto de validar transacciones en una blockchain. Requiere de potencia computacional y electricidad para resolver un rompecabezas. El mining recompensa con moneda virtual, basándose en tu capacidad de computación



Pool de mineros

Un conjunto de mineros que se unen para compartir su capacidad computacional en una red acuerdan en dividir la recompensa recibida por cada nuevo bloque encontrado dentro de su grupo



Mist

Navegador para la instalación y el uso de Dapps



(MSP) Proveedor de servicios de afiliación

Una red blockchain Hyperledger Fabric se puede dirigir por uno o varios proveedores de servicios de afiliación



Transacción multi-firma

Transacciones multi firma requieren de la aprobación de las múltiples partes para la ejecución de una transacción sujeta a reglas predeterminadas



Nodo

Una copia del registro operado por un usuario de la blockchain



Número aleatorio

Un número utilizado una sola vez en comunicación criptográfica (a menudo incluye un sello de fecha y hora)



El problema de "nada en juego"

Es causado por nodos validadores que aprueban todas las transacciones en versiones de software nuevas y antiguas, después que ocurre una bifurcación dura (hard fork)



NPM (Administrador de Paquetes de Nodos)

Gestor de paquetes node.js predeterminado para el entorno del tiempo. NPM gestiona las dependencias para una aplicación



Protocolo Oauth

Autorización abierta (Oauth) es un estándar utilizado por terceros para guardar y distribuir información de usuario sin revelar su contraseña



Ommer (o Uncle)

Es un bloque completamente minado, pero que aún no se ha añadido a la Blockchain



Gobernanza on-chain

Un sistema para gestionar e implementar cambios a una criptomoneda blockchain



Oraculo

Una interfaz que conecta contratos inteligentes y fuentes de datos.



Red de solicitantes

Una red de ordenadores que permite a sus nodos compartir recursos



P2P (inter pares o de igual-a-igual)

Modelo descentralizado en el cual dos partes completan una transacción sin necesidad de un intermediario o tercero. El comprador y vendedor interactúan de forma directa



Infraestructura de claves públicas (PKI)

Una serie de funciones, políticas y procedimientos necesarios para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales y administrar encriptación de clave pública



Pragma(s) o Pragma-line

Define qué versión del compilador utiliza el contrato inteligente



Blockchain privada

Una blockchain con control de acceso. Al contrario que en las públicas, en una blockchain privada no se utilizan algoritmos de consenso, como la prueba de trabajo (PoW) o de participación (PoS). En su lugar, se utiliza un sistema conocido como "tolerante a faltas bizantinas" (BFT). Un sistema BFT no es un sistema "sin confianza" (trustless) que hace a las BFT menos seguras.



Prueba de actividad (PoA)

Se recompensa a los participantes activos que mantienen un nodo completo



Prueba de quemado (PoB)

Los mineros "queman" monedas, enviándolas a una dirección inactiva. Este gasto se registra en la blockchain y se premia al usuario



Prueba de capacidad (PoC)

Parcelas de almacenamiento (plots) se guardan en el disco duro antes de empezar la minería. El disco duro que genere la solución de forma más rápida es el ganador.



Prueba de tiempo transcurrido (PoET)

Algoritmo de consenso en el cual los nodos han de esperar durante un periodo de tiempo aleatorio. El primer nodo en completar la espera será recompensado



Prueba de participación (PoS)

Algoritmo de consenso que elige al dueño de un bloque nuevo, basándose en su riqueza (o participación). No hay recompensa como tal, por el bloque. Los mineros obtienen un pago por transacción.



Prueba de trabajo (PoW)

Algoritmo de consenso que requiere que el usuario resuelva un rompecabezas matemático complejo (o puzzle) para verificar una transacción (minar). Los "mineros" son recompensados con criptomonedas basadas en su potencia computacional.



Prueba de importancia (PoI)

Prueba de Importancia (PoI) es un mecanismo de consenso en NEM. De forma similar que en la prueba de participación (PoS), los nodos tienen que apostar una cantidad de dinero, para optar a la creación de bloques. La selección es aproximadamente proporcional a una escala de puntuación.



Pub/Sub

Publicar / suscribir



Blockchain Publica

Una blockchain con acceso al publico en general.



Criptografía de clave pública

Método criptográfico que utiliza un par de claves relacionadas de forma matemática. Una llave pública y una llave privada. Es imposible obtener la clave privada, basándose en la clave pública.



API REST (representational state transfer API)

Define restricciones basadas en http



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Español



Llamada de procedimiento remoto (RPC)

Un protocolo que se utiliza desde un programa para solicitar el servicio de otro programa localizado en la red



RSA

Sistema criptográfico de uso para encriptar un mensaje con la llave pública de un individuo de manera que únicamente esa persona pueda descifrar el mensaje dentro de un periodo de tiempo razonable



Satoshi Nakamoto

Es un individuo o una entidad creadora del protocolo Bitcoin el cual tuvo éxito resolviendo el problema de "doble gasto" de una moneda digital.



Testigo segregado (Segwit)

El proceso por el cual se aumenta el límite de tamaño de un bloque, mediante la eliminación de datos del identificador (firma) en transacciones Bitcoin



SDK

Un kit de desarrollo de software (SDK) reúne un grupo de herramientas de programación para crear software en una plataforma determinada



SHA-256

El SHA-256 forma parte del conjunto de funciones hash criptográficas SHA-2, diseñadas por la NSA. SHA significa Secure Hash Algorithm. El SHA-256 es utilizado en varias partes de la red Bitcoin. La minería utiliza el SHA-256 como la PoW (prueba de trabajo)



Sharding (fragmentación)

Una técnica que consiste en fraccionar la blockchain en varios elementos de red, llamados "shards" (fragmentos), que son capaces de procesar transacciones en paralelo.



Contrato inteligente (Smart Contract)

Contrato autoejecutable que incluye las condiciones generales del acuerdo en el código



Solidity

Es un lenguaje de programación usado para escribir contratos inteligentes en Ethereum.



Stablecoin

El término adjudicado a una criptomoneda diseñada para minimizar los efectos provocados por la volatilidad de precios, al estar vinculada a una divisa o materia prima cotizada (por ejemplo, a metales preciosos)



Medida de participación

Una función del mecanismo PoS (prueba de participación) por la cual el peso del voto de una persona va en función a la proporción de monedas que le pertenecen.



"Token" unidad de moneda digital

La representación digital de un activo construido sobre una blockchain



Economía de Tokens

El estudio, diseño e implementación de sistemas económicos basados en tecnología blockchain



Registro Principal sin "Tokens"

Un registro principal que no requiere una moneda nativa para operar.



Lenguaje turing completo

Un lenguaje de programación capaz de llevar a cabo cálculos equivalentes a los de un ordenador



Ubuntu

Sistema operativo de código abierto y distribución de Linux



Salida de transacción no utilizada (UTXO)

Salidas de transacciones no utilizadas (UTXO) se usan para determinar la validez de una transacción



Máquina Virtual

Emulación de un sistema informático



VMware

Es una filial de Dell que proporciona servicios cloud computing (de computación en la nube), así como software y servicios de virtualización



VMare Player

Paquete software de virtualización para ordenadores x64 funcionando con Microsoft o Linux



VYPER

Lenguaje de programación creado para actuar como una introducción formal a contratos inteligentes (smart contracts)



Monedero

Protege los activos digitales del propietario.



Zeppelin o Zeppelin Abierto

Es una comunidad de desarrolladores de contratos inteligentes con ideas similares.



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Deutsche

51% Attacke



Eine Situation in der die Mehrheit von Minern eine Attacke auf den Rest der Nodes (oder User) auf einer Blockchain startet. Erlaubt die doppelte Ausgabe oder das Stehlen von Gütern.

Vertragsledger



Ein verteiltes Ledger, das von zwei oder mehr Benutzern verwendet wird, um zu verhandeln und eine Vereinbarung zu treffen

Blockhöhe



Anzahl der Blöcke, die in der Blockkette miteinander verbunden sind

Toleranz gegenüber Byzantinische Fehler



Byzantinische Fehler bezeichnen beliebig auftretende Fehler. Toleranz gegenüber solchen Fehlern heißt, dass solche Systeme weiter funktionieren obwohl einige Nodes nicht mehr funktionieren oder bösartig werden.

Chaincode



Ein Programm welches durch gesendete Anträge Kontenzustände initialisiert oder verwaltet

Coinbase



Die größte Börse um Bitcoin zu kaufen oder in US Dollar und andere Währungen zu tauschen.

Consensus (Einigkeit)



Wenn alle Teilnehmer eines Netzwerk zur Gültigkeit einer Transaktion zustimmen

Kryptowährung



Eine auf Mathematik basierende digitale Währung, bei der Verschlüsselungstechniken verwendet werden, um die Erzeugung von Währungseinheiten zu regulieren und den Geldtransfer zu überprüfen. Kryptowährungen arbeiten unabhängig von einer Zentralbank.

Dagger Hashimoto



Der vorgeschlagene Mining-Algorithmus für Ethereum 1.0

ABI (Applikations-Binär Interface)



Ein Interface zwischen zwei binären Programm-Modulen. Eines der Programme ist oft eine Library und das Andere wird vom Benutzer ausgeführt.

Alt-Coin



Eine Kryptowährung die als Alternative zu Bitcoin existiert

Blockchain (öffentlich)



Eine mathematisches Konstrukt um digitale Transaktionen (oder Daten) in einem unveränderbaren, Peer-to-Peer Kontonführungssystem zu speichern, welches sehr schwer gefälscht aber trotzdem zugänglich bleibt.

Casper



Consensus Algorithmus welcher Proof of Work und Proof of Stake vereint. Ethereum benutzt Casper im Übergang zu Proof of Stake.

Kanal



Ein Blockchainkanal ist ein separater Datenkanal welcher es einzelnen Nodes erlaubt privat zu kommunizieren – beispielsweise Transaktionen verschickt ohne, dass das ganze Netzwerk es sieht.

Composer CLI



Hyperledger Kommandozeileninterface um administrative Tasks auszuführen

Konsensprozess



Der Prozess des Konsenses über den Inhalt eines Ledgers

CRUD



Create, Retrieve, Update, Delete – anlegen, lesen, aktualisieren, löschen

Dapps



Dezentralisierte Applikationen



Adresse

Adresse (Adresse der Kryptowährung) wird zum Senden und Empfangen von Transaktionen im Netzwerk verwendet

API



Application Programming Interface, Teil eines entfernten Servers welches Anfragen empfängt und Antworten sendet.

Geschäftslogik Schicht



Ein Teil des Codes der Geschäftsprozesse abbildet.

CDN (Content Deliver Network)



Caching von Dateien um Internetinhalte schneller zu übertragen (html, js, css, etc.)

CLI



Kommandozeileninterface

Compoler Rest Server



Generiert eine RESTful API aus einer veröffentlichten Blockchain

Konsortiums-Blockchain



Eine Konsortiums-Blockchain ist eine Blockchain auf der Consensus Prozesse von vordefinierten Nodes gesteuert werden.

Kryptografische Hashfunktion



Eine Funktion die einen beliebig langen Eingangswert auf einen Ausgangswert fixer Länge abbildet.

DDos Attacke



Eine Denial-of-Service Attacke ist ein Cyberangriff welcher versucht eine Ressource (meist Server, Host) unerschickbar zu machen um so eine Dienstleistung zu unterbrechen.



Aggregierte Transaktionen

Zusammenführung mehrere Transaktionen in eine. Erlaubt sicheren Tausch und andere erweiterte logische Operationen. Verwendet in NEM.



Bitcoin

Die erste und populärste Kryptowährung basierend auf dezentralen Konten. Erfunden im Jahr 2009.



Geschäftsnetzwerk Karte

Stellt Informationen zur Verfügung um ein Blockchain Geschäftsnetzwerk zu verbinden.



Zentralisiert

Eine zentrale autoritative Gruppe oder Standort



Coin/Münze

Darstellung eines auf einer neuen Blockchain aufgebauten digitalen Vermögens



Bestätigung

Angabe, dass die Blockchain-Transaktion vom Netzwerk durch Mining verifiziert wurde



Container Technologie

Eine Lösung um Software Applikationen zuverlässig zu veröffentlichen, obwohl das Zielsystem vom Entwicklungssystem abweicht. Bspw Docker oder Kubernetes.



Kryptographie

Eine Methode zur Sicherung der Kommunikation mithilfe von Code



Dezentralisierung

Übertragung von Befugnissen und Verantwortlichkeiten von einer zentralisierten Organisation, Regierung oder Partei in ein verteiltes Netzwerk.



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Deutsche



Schwierigkeit

Angabe, wie schwer es ist, Blöcke in Proof-of-Work-Mining zu überprüfen



Dezentralisiert

Das Konzept eines geteilten Netzwerks bestehend aus verteilten Computern (oder Nodes) welches ohne zentrale Schnittstelle Transaktionen abarbeiten kann.



Digitales Gut

Any digital data that is formatted into binary code and includes the right to use it.



Digitale Identität

Eine digitale Identität ist eine Online- oder Netzwerkidentität, die von einem Einzelnen, einer Organisation oder einem elektronischen Gerät im Cyberspace angenommen oder beansprucht wird.



Digitale Signatur

Ein mathematisches Schema um die Echtheit von digitalen Assets darstellen zu können.



Doppelte Ausgaben

Ein Szenario, in dem jemand versucht, gleichzeitig eine Bitcoin-Transaktion an zwei verschiedene Empfänger zu senden



Enum

Eine einfache Wertart



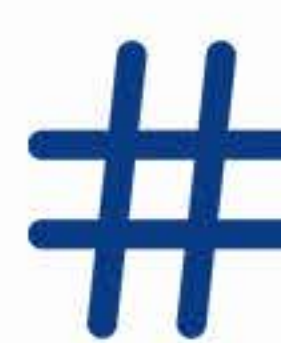
EOA

Account mit externem Besitz



ERC20

Ethereum Request for Comments, Issue Nummer 20 – beschreibt einen Token-Standard



ET-Hash

Der von Ethereum 1.0 genutzte Proof of Work Algorithmus



Ethereum

Blockchain Applikation die das Ausführen von Programmen erlaubt um dezentrale Kontenführungen nach Bedarf abzubilden. Smart Contracts (Intelligente Verträge) werden benutzt um die Transaktionen zu validieren.



Austausch

Ein Ort zum Kaufen und Verkaufen von Kryptowährung



Fiat

Gesetzliches Zahlungsmittel, dessen Wert von der ausstellenden Regierung gestützt wird. ZB: USD, EUR, CNY, JPY



FITS Modell für Blockchain Anwendbarkeit

Stellt fest ob eine Blockchain anwendbar ist: Betrug ist verbreitet, Mittelsmänner existieren, Durchsatz wird gebraucht, stabile Daten sind in der Applikation



Fork (gabeln)

Ist ein von allen Nodes kollektiv beschlossenes Softwareupdate.



Austauschbarkeit

Die Möglichkeit Waren oder Güter mit Waren oder Gütern der selben Klasse austauschen zu können. Anwendbar auf das verteilte Kontenbuch von Corda



Gas (Ethereum)

Eine Maßeinheit wie viel für eine bestimmte Operation auf der Ethereum Blockchain zu bezahlen ist.



Genesis Block (Ursprungsblock)

Der erste, initiale Block einer Blockchain.



Github

Ein web-basiertes Hostingservice für GIT-basierte Versionskontrolle. Wird von Blockchain Entwicklern benutzt.



Golang (Google Programmiersprache)

Eine Programmiersprache basierend auf C, erfunden 2009 von Google



Gossip Protokoll

Ein Gossip Protokoll ist ein Verfahren oder Prozess um Computer-zu-Computer Kommunikation so zu modellieren, dass sie der Art wie soziale Netzwerke Information verbreiten ähnlich sind. Es ist ein Kommunikationsprotokoll.



Führung

The rules that are established for a Blockchain that determine how it is governed, administrated, and managed or protected.



Hard Fork

Alters the blockchain data in a public blockchain. Requires all nodes in a network to upgrade and agree on the new version.



Hardware-Geldbörse

Ein physisches Gerät, das mit dem Internet verbunden werden kann und mit einem Online-Austausch interagiert



Hashfunktion

Eine Funktion die Daten beliebiger Größe abbildet.



Heiße Geldbörse

Eine Brieftasche, die jederzeit direkt mit dem Internet verbunden ist



Hot/Cold Wallet

Hot Wallets sind solche Geldbörsen, die mit dem Internet verbunden sind, ähnlich einer Kreditkarte. Cold Wallets sind aus dem Internet nicht erreichbar, ähnlich einem Sparbuch.



Hyperledger

Von der Linux Foundation initiiert werden unter dem Begriff Hyperledger Open-Source Blockchains angeboten.



Hyperledger Composer

Hyperledger Composer ist ein Blockchain Applikations Entwicklungs Framework. Es vereinfacht die Entwicklung von Blockchain Applikationen auf Hyperledger Fabric.



Hyperledger Fabric

Hyperledger Projekt welches von Linux gehostet wird und Chaincode genannte Smart Contracts bereitstellt.



IDE (Integrierte Entwicklungsumgebung)

Eine Applikation für Softwareentwickler die hauptsächlich aus Quellcodeeditor, Automatisierungstools für Buiding und Debugging beinhaltet.



Unveränderlich

“Nicht änderbare” Daten auf einer Blockchain sind unmöglich im Nachhinein zu verändern (auch nicht von Administratoren)



Initial Coin Offering (ICO)

Eine Form des Crowdfunding um Kapital für neue Kryptowährungsunternehmen zu beschaffen. Modelliert werden ICOs nach IPOs (Börseneinführung). Man erhält Token für die Finanzierung von ICOs.



Instanziieren

“Instanzieren” nennt man das Erstellen einer Instanz in einer Objekt orientierten Programmiersprache (OOP). Ein instanziiertes Objekt erhält einen Namen und die Struktur aus einer Klassendeklaration und wird im Speicher oder auf der Festplatte erstellt.



Invariant

Eine Funktion, Quantität oder Eigenschaft die bei spezifischen Transformationen unverändert bleibt



IPFS

Inter Planetary File System (Interplanetarisches Dateisystem)



JSON

“JavaScript Object Notation” und wird wie “Jason” ausgesprochen. JSON ist ein text-basiertes Datenaustauschformat um strukturierte Daten zu übertragen. Es wird häufig benutzt um Daten zwischen Web-Servern und Applikationen auszutauschen.



Kubernetes

Eine Menge an Erstellungsblöcken (“Primitives”), die kollektiv einen Mechanismus zum Veröffentlichlichen, Aufrechterhalten und Skalieren von Applikationen zur Verfügung stellt. Es ist auch ein open-source Container Orchestrierungssystem für automatische Veröffentlichung, Skalierung und Management von Container-basierten Applikationen.



Hauptbuch

Ein Nur-Anhänge-Speicher für Datensätze



Liquidität

Die Fähigkeit eines Vermögenswerts, in Bargeld umgewandelt zu werden



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Deutsche



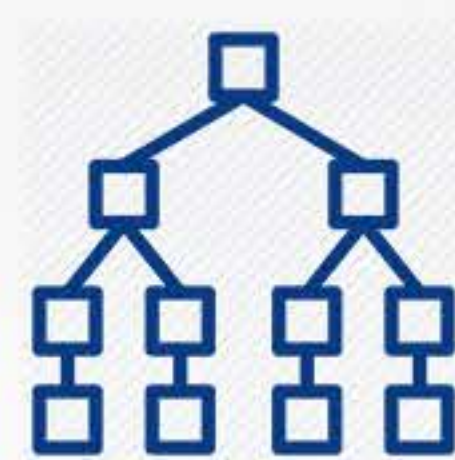
Lightning Network

Ein dezentralisiertes Netzwerk welches Smart Contract Funktionalität in der Blockchain benutzt um verzögerungsfreie Bezahlvorgänge über Netzwerkteilnehmer zu erlauben.



Marktkapitalisierung

Gesamtwert einer Kryptowährung



Merkle Tree

Ein Merkle Tree (dt.: Hash-Baum) ist ein Baum der in den Blättern die Daten enthält und in den Knoten die Hashwerte der Kinder.



Mining (Förderung)

Das Validieren der Blockchaintransaktionen. Es benötigt Rechenleistung und Elektrizität um ein Puzzle zu lösen. Die Belohnung sind Kryptomünzen basieren auf der Rechenleistung.



Mining pool

Eine Sammlung an Minern die die gemeinsame Rechenleistung über ein Netzwerk teilen und vereinbaren die Belohnung eines neu gefundenen Blocks zu teilen.



MIST

Ein Browser um dezentralisierte Applikationen (Dapps) zu installieren und zu benutzen.



MSP (Anbieter für Service Mitgliedschaften)

Ein Hyperledger Fabric Blockchain Netzwerk kann durch einen oder mehrere MSPs gesteuert werden.



Multi-Signatur (Transaktion)

Multi-Signatur Transaktionen benötigen die Zustimmung einer oder mehrerer Teilnehmer basierend auf gewissen Regeln.



Node

Eine Kopie des Kontenbuches im Betrieb beim Benutzer auf der Blockchain



Nonce

Eine einmalig benutzte Zahl bei kryptographischer Kommunikation (oft in Zusammenhang mit einem Zeitstempel)



Kein Anteil Problem (nothing at stake)

Passiert bei Überprüfungsnodes die alle Transaktionen alter und neuer Software bestätigen nachdem ein Hard-Fork passiert ist.



NPM (Node Package Manager)

Die Standard Paket Manager Umgebung von NodeJS. NPM managed Abhängigkeiten für Applikationen.



OAuth Protokoll

“Open Authorization” oder Offene Berechtigung ist ein Standard der von Drittsystemen benutzt wird um Benutzerdaten weitergeben zu können ohne das Passwort zu enthüllen.



Ommers (alias Uncle)

Ein Block der komplett gemined wurde, aber noch nicht der Blockchain hinzugefügt wurde.



On-chain Governance

Ein System um Änderungen einer Kryptowährungsblockchain zu managen oder zu implementieren.



Orakel

Eine Schnittstelle, die intelligente Verträge und Datenquellen miteinander verbindet



Orderer Network

Ein Computernetzwerk das es Nodes erlaubt Ressourcen zu teilen.



P2P (Peer-to-Peer)

Ein dezentralisiertes Modell in dem zwei Parteien eine Transaktion ohne Mittelsmann vollständig ausführen. Der Käufer und Verkäufer interagieren direkt.



PKI (Public-Key Infrastruktur)

Eine Menge an Regeln, Strategien und Prozeduren die gebraucht werden um Digitale Zertifikate und Public-Key Verschlüsselung zu erstellen, managen, verteilen, benutzen, speichern und widerrufen.



Pragma(s) oder Pragma-Zeile

Definiert welche Compler-Version der Smart Contract benutzt.



Private Blockchain

Eine Blockchain die kontrolliert wer Zugriff darauf hat. Anders als öffentliche Blockchains benutzt eine private Blockchain keine Consensus Algorithmen wie PoW oder PoS. Stattdessen wird ein System namens Toleranz gegenüber Byzantinischen Fehlern (Byzantine Fault Tolerance, BFT) benutzt. BFT ist nicht ganz so sicher wie PoW.



Aktivitätsnachweis (Proof of Activity)

Aktive Beteiligte die eine Full-Node betreiben werden belohnt.



Verbrennungsnachweis (Proof of Burn)

Miners schicken Münzen an eine inaktive Adresse und verbrennen diese Münzen damit. Die Verbrennung ist auf der Blockchain aufgezeichnet und entsprechend entlohnt.



Kapazitätsnachweis (Proof of Capacity)

Die Nutzung der Festplatte bevor das Mining beginnt. Eine Festplatte mit der schnellsten Lösung gewinnt den Block



Nachweis über verstrichene Zeit (Proof of Elapsed Time)

Consensus-Algorithmus bei der Nodes eine zufällig lange Zeit-Periode warten müssen und die erste Node die den Wartezyklus vervollständigt hat bekommt die Belohnung.



Anteilsnachweis (Proof of Stake, PoS)

Ein Consensus-Algorithmus der den Benutzer eines neuen Blocks basieren auf dem Vermögensstand auswählt. Es gibt keine Blockbelohnung, es werden nur die Transaktionskosten eingehoben.



Arbeitsnachweis (Proof of Work, PoW)

Ein Consensus-Algorithmus der für das Mining eines Blocks das Lösen eines komplexen mathematischen Puzzles erfordert. Miners werden für das zur Verfügungsstellen von Ressourcen belohnt.



Wichtigkeitsnachweis (Proof of Importance)

Wichtigkeitsnachweis ist ein Consensus-Algorithmus der Blockchain NEM. Ähnlich wie Anteilsnachweis (PoS): Nodes geben einer Menge an Währung die Möglichkeit neue Blöcke zu generieren und werden ungefähr proportional aufgrund eines Scores ausgewählt.



Pub/Sub

Publish/Subscribe – Veröffentlichen/Abonnieren



Öffentliche Blockchain

Eine öffentlich zugängliche Blockchain



Public Key Cryptography (Öffentlicher Schlüssel Kryptographie)

Verschlüsselungsverfahren welches zwei mathematisch verbundene Schlüssel benutzt, einen privaten und einen öffentlichen Schlüssel. Es ist unmöglich den privaten Schlüssel aufgrund des öffentlichen Schlüssels abzuleiten.



REST API (representational state transfer)

Definiert Schnittstellen für Maschine-zu-Maschine Kommunikation im World-Wide-Web über http.



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

Deutsche



RPC (Aufruf einer fernen Prozedur)

Ein Protokoll welches es einem Programm erlaubt ein anderes Service über ein Netzwerk anzusprechen.



RSA

RSA Verschlüsselung ist ein System zur Verschlüsselung mit einem öffentlichen Schlüssel um es zu ermöglichen die Nachricht in akzeptabler Zeit wieder zu entschlüsseln.



Satoshi Nakamoto

Eine natürliche oder juristische Person, die das Bitcoin-Protokoll erstellt hat und das Problem der digitalen Währung mit den doppelten Ausgaben erfolgreich gelöst hat



Segwit

Ein Prozess der durch Entfernung der Signatur-Daten von Bitcoin Transaktionen die Block-Größen-Limitierung erhöht.



SDK (Softwareentwicklungssystem)

Ein Softwareentwicklungssystem das alle nötigen Tools zur Entwicklung und Erstellung von Programmen einer spezifischen Plattform zur Verfügung stellt.



SHA-256

SHA-256 ist ein Mitglied der SHA-2 Hash Funktionen und wurde von der NSA entwickelt. SHA steht für Secure Hash Algorithm. SHA-256 wird für verschiedene Teile von Bitcoin benutzt: Mining benutzt SHA-256 als Arbeitsnachweis (PoW).



Sharding

Unterteilt die Blockchain in mehrere kleinere Komponenten die „Shards“ genannt werden. Dadurch können Transaktionen parallel abgearbeitet werden.



Smart Contract (Intelligente Verträge)

Selbst-erfüllende Verträge mit den Vertragsbestimmungen als Computercode definiert.



Solidität

Eine Programmiersprache zum Schreiben von intelligenten Verträgen im Ethereum-Netzwerk



Stablecoin (Stabile Münzen)

Die Definition einer Kryptowährung welche die Effekte von Preisvolatilität minimiert. Kann an eine Währung oder Handelsgüter (bspw Edelmetalle) gekoppelt sein



Stake Weighting (Anteilsgewichtung?)

Eine Funktion des Anteilsnachweises wobei das Gewicht einer Stimme proportional zur Anzahl der Tokens ist.



Token

Eine Repräsentation eines Digitalen Guts auf einer existierenden Blockchain.



Tokenökonomie

Beschreibt die Untersuchung, das Design und die Implementierung von Ökonomischen Systemen basieren auf Blockchain Technologien.



Tokenless Ledger

Ein Ledger, für das keine einheitliche Währung erforderlich ist



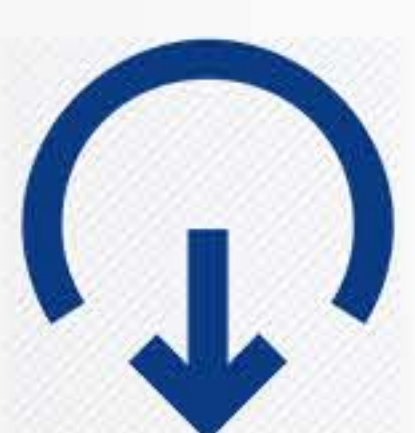
Turing Vollständig

Eine Sprache die, in der Theorie, die universelle Programmierbarkeit erlaubt.



Ubuntu

Freies open-source Betriebssystem und Linux Distribution



UTXO (Ungenutzter Transaktionsausgang)

UTXO wird benutzt um die Gültigkeit einer Transaktion zu bestimmen.



Virtuelle Maschine

Emulation eines Computersystems.



VMware

Eine Tochtergesellschaft von Dell die Cloud Computing und Plattform Visualisierungstools und Services anbietet.



VMware Player

Ein Virtualisierungspaket für x64 Computer die Windows oder Linux benutzen.



VYPER

Eine objekt-orientierte Python-ähnliche Programmiersprache für die Ethereum Virtual Machine.



Wallet (Geldbörse)

Speichert digitale Güter



Zeppelin (oder Open Zeppelin)

Eine Community von ähnlich gesinnten Smart Contract Entwicklern



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

عربي

51% هجوم

الحالة التي تطلق فيها غالبية المنقبون في بلوك تشين هجوماً على بقية الأطراف (أو المستخدمين). هذا النوع من الهجوم يسمح بمضاعفه الانفاق أو سرقة الأصول.



آية بي آي (واجهه التطبيق الثنائية)

واجهه بين اثنين من وحدات برنامج ثنائي، وغالبا ما يكون أحد البرامج مكتبه ويتم تشغيل الآخر من قبل مستخدم.



عنوان

عنوان (عنوان العملة المشفرة) مستخدم لإرسال وتلقي المعاملات على الشبكة.



معاملات مجمعة

دمج عدة معاملات في معاملة واحدة، والسماح بمقايضه غير موقوفة، وغيرها من المنطقيات المتقدمة. يستخدم في إن إي إم (الحركة الاقتصادية الجديدة).



دفتر الاتفاقية

دفتر موزع مستخدم من قبل اثنين أو أكثر المستخدمين للتفاوض والتوصل إلى اتفاق.



عملة بديلة

اي عمله بديلة لعملة بيتكوين.



آية بي آي

واجهه التطبيقات البرمجية (جزء من خادم) (يعيد يرسل الطلبات ويتلقى الاستجابات).



عملة بيتكوين

العملة المشفرة الاولى، والأكثر شعبية، المبنية على دفتر البلوك تشين اللامركزي والذي تم إنشاؤه في 2009.



ارتفاع الكتل

عدد الكتل المتصلة معا في سلسله بلوك تشين.



بلوك تشين

بنية رياضية لتخزين المعاملات الرقمية (أو البيانات) في دفتر غير قابل للتغيير، دفتر من نظير إلى نظير يصعب بشدة تزيفه مع البقاء في متناول اي شخص.



طبقه منطق الاعمال

جزء من التعليمات البرمجية التي تحدد الأحكام الواجب اتباعها عند القيام بالاعمال.



بطاقة شبكة الاعمال

توفير المعلومات الضرورية لتوصيل شبكة بلوك تشين.



التسامح مع الخطأ البيزنطي

التسامح مع الخطأ البيزنطي (بي إف تي) هو خاصية لنظام قادر على مقاومه فئة الإخفاقات المشتقة من مشكله الجزائيات البيزنطيين. وهذا يعني ان نظام بي إف تي قادر على الاستمرار في العمل حتى إذا فشلت بعض الأطراف أو عملت بشكل ضار.



كاسبر

خوارزميه توافق الآراء التي تجمع بين إثبات العمل وإثبات الرهان. اثيريام يستخدم كاسبر للانتقال لإثبات الرهان.



شبكة توصيل المحتوي

يسمح بالانتقال السريع من الأصول اللازمة لتحميل محتوى الإنترنت (إيتش تي إم إل، جى إس، سي إس إس، الخ).



مركزي

يتم الحفاظ عليه من قبل موقع مركزي أو مجموعه ذات سلطة.



تشين كود

برنامج يقوم بتهيئة وإداره حاله الدفاتر من خلال التطبيقات المقدمة.



قناة

قناه بلوك تشين هي قناه بيانات منفصلة تسمح للأطراف بالاتصال الخاص، أو بتمويل المعاملات، وما إلى ذلك، دون رؤية جميع أطراف الشبكة للاتصالات.



سي إل آي

واجهه سطر الأوامر.



عملة

تمثيل الأصول الرقمية التي بنيت على بلوك تشين جديد.



كوينبيس

أكبر تبادل لشراء وبيع لعملة بيتكوين وتحويل بيتكوين إلى الدولار أو العملات الأخرى.



ملحن سي إل آي

سطر أوامر الدفتر الذي يسمح بمهام اداريه.



خادم ملحن رست

ينشئ واجهه ريست للتطبيقات البرمجية من بلوك تشين منشور.



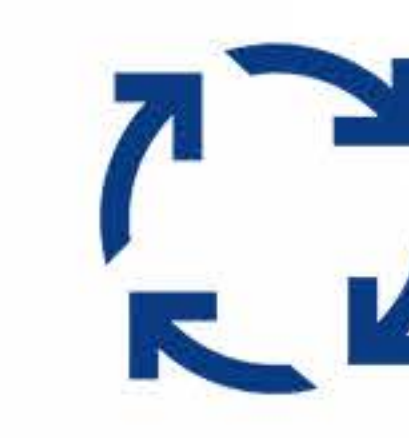
تأكيد

اشاره انه تم التحقق من معاملة بلوك تشين من قبل الشبكة من خلال التنقيب.



توافق الآراء

الاتفاق من جميع المشاركين في الشبكة على صحة المعاملة.



إجماع عملية

عملية الوصول إلى توافق الآراء بشأن محتوى دفتر.



اتحاد بلوك تشين

بلوك تشين حيث يتم التحكم في عملية توافق الآراء من قبل مجموعه محدده مسبقا من الأطراف.



تكنولوجيا الحاويات

حل لتشغيل تطبيق برمجي بشكل يعتمد على عند نشره في بيئة مختلفه غير التي تم إنشاؤه فيها. مثل دوكر أو كيوبيميس.



عمله مشفره

عمله رقميه تعتمد على الرياضيات، حيث تستخدم تقنيات التشفير لتنظيم توليد وحدات العملة والتحقق من تحويل الأموال. تعمل العملة الرقمية بشكل مستقل عن البنك المركزي.



كراد

إنشاء، استرداد، تحديث، حذف.



عملية تشفير الهاش

داله تتلقي مدخل من اي حجم وتقوم بإرجاع سلسله فريدة من طول موحد.



التشفير

طريقه لتأمين الاتصال باستخدام التعليمات البرمجية.



داجر هاشيموتو

المواصفات المقترحة لخوارزميه التنقيب في اثيريام 1.0.



دابس

تطبيقات لامركزية.



هجمات دي أو إس

هجوم "الحرمان من الخدمة" هو هجوم الكتروني يسعى مرتكب الجريمة فيه إلى جعل الجهاز أو الخدمة غير متاحين لمستخدميها المقصودين وذلك بتعطيل خدمات المضيف المتصل بالإنترنت بشكل مؤقت أو إلى أجل غير مسمى.



اللامركزيه

نقل السلطة والمسؤولية من سلطة مركزيه أو حكومة أو طرف إلى شبكة موزعه.



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

عربي



صعوبه

دلاله من مدي صعوبه التحقق من الكتل في التنقيب باستخدام خوارزمية إثبات العمل



لامركزي

مفهوم الشبكة المشتركة لأجهزة الكمبيوتر المشتتة (أو الأطراف) التي يمكنها معالجة العمليات بدون وسيط خارجي ذو موقع مركزي.



الأصل الرقمي

اي بيانات رقمية يتم تنسيقها على هيئة تعليمات برمجية ثنائية وتشمل الحق في استخدامها



الهوية الرقمية

هوية الكترونية أو متصلة بالشبكة تم تبنيها أو المطالبة بها في الفضاء السيبراني من قبل فرد أو منظمه أو جهاز الكتروني



التوقيع الرقمي

مخطط رياضيات يستخدم لتأكيد أصالة الأصول الرقمية



الانفاق المزدوج

السيناريو حيث يحاول شخص ما إرسال معاملة بيتكوين إلى اثنين من المستلمين المختلفين في نفس الوقت



إي نم

نوع بيانات يمثل تعدد قيم من نفس النوع



إي أو إية

حساب خارجي مملوك



إي آر سي 20

طلب إيثيريوم للتعليقات القياسية



أي تي هاش

خوارزمية إثبات العمل المستخدمة في إيثيريوم 1.0



اثيريام

تطبيق بلوك تشين يستخدم لغة برمجية مضمنة تسمح للمستخدمين ببناء دفاتر لامركزية معدلة لاحتياجاتهم الخاصة. تستخدم العقود الذكية للتحقق من صحة المعاملات في الدفتر.



صرافة

مكان لشراء وبيع العملات المشفرة



فيات

عملة رسمية تدعم قيمتها الحكومة التي أصدرتها. مثال: الدولار والين واليورو



نموذج فيتس لتطبيق البلوك تشين

نموذج لتقييم ملاءمة بلوك تشين باستخدام الاحتمال منتشر، الوسيط موجودون، الانتاجيه مطلوبه، البيانات المستقره موجوده في التطبيق.



شوكه

تحديث برنامج تمت الموافقة الجماعية عليه من قبل جميع الأطراف علي الشبكة



التبادلية

قدره السلعة أو الأصل علي أن يتم تفاعله مع السلع أو الأصول الفردية الأخرى من نفس النوع. ينطبق علي دفتر كوردا الموزع.



غاز (اثيريام)

مقياس لمقدار الأيثر الذي يتم دفعه لعملية معينة يتم تنفيذها في إيثيريام



جينيسيس بلوك

اول كتلة داخل بلوك تشين



جيت هب

خدمه استضافه علي شبكة الإنترنت للتحكم في الإصدارات باستخدام "جيت". مستخدمة من قبل مطوروا بلوك تشين



جولانج

لغة برمجة انشأتها جوجل في 2009، لغة جولانج أسست على لغة سي



بروتوكول القيل والقال

بروتوكول القيل والقال هو اجراء أو عمليه اتصالات كمبيوتر بكمبيوتر والتي تستند إلى طريقة شبكات التواصل الاجتماعي لنشر معلومات أو كيفية انتشار الاوبئه. انه بروتوكول اتصالات.



الحوكمة

الأحكام التي تم تأسيسها لسلسله بلوك تشين تحدد كيفية حوكمتها، وأدارتها أو حمايتها



الشوكه الصلبة

يغير بيانات البلوك تشين في بلوك تشين عام. يتطلب من جميع الأطراف في الشبكة الترقية والاتفاق علي الإصدار الجديد.



محفظه الاجهزه

جهاز فعلي يمكن توصيله بالويب والتفاعل مع الصرافة عبر الإنترنت



عملية الهاش

داله تقوم بتعيين بيانات بحجم عشوائي



المحفظة الساخنة

محفظه متصلة مباشرة بالإنترنت في جميع الأوقات



الشوكه الساخنة/ الباردة

وصف خاص بالعمله حيث المحافظ الساخنة مثل الحسابات الجارية في حين المحافظ الباردة مثل حسابات الادخار



هايرليدجر

بدأت من قبل مؤسسة لينوكس، هايرليدجر هو لمشروع مظلة المصدر المفتوح لبلوك تشين



ملحن هايرليدجر

ملحن هايرليدجر هو اطار عمل تطوير تطبيقات لتبسيط تطوير تطبيقات بلوك تشين علي هايرليدجر فابريك



نسيج هايرليدجر

مشروع هايرليدجر الذي يستضيفه لينوكس والذي يستضيف عقود ذكية تسمى تشين كود



(أي دي إي) بيئة التطوير المتكاملة

تطبيق لمطوري البرامج التي تتكون في المقام الأول من محرر التعليمات البرمجية المصدرية، أداة أتمتة الإنشاء، والمصحح



ثابت

غير قابل للتغيير. البيانات المخزنة في بلوك تشين غير قابلة للتغيير. (ليس حتى من قبل الاداريين)



العرض الاولي للعملة

الشكل الذي يتم به جمع رأس مال لتمويل مشاريع العملات المشفرة الجديدة. علي غرار الإصدار أول. يتلقى الممولون الرموز المميزة



إنشاء مثيل

إنشاء مثيل هو إنشاء مثيل في لغات البرمجه الموجهه إلى كائن. يتم إعطاء الكائن الذي تم إنشاء مثيل له اسما ويتم إنشاؤه في الذاكرة أو علي القرص الصلب باستخدام البنية الموصوفة ضمن تعريف الفئة المنتمي لها.



ثابت

دالة أو كمية أو خاصية تبقى بدون تغيير عند عمل تحويل محدد



آي إف بي إس

نظام الملفات الكوكبية المشترك



جيه سون

جافا سكريبت لتدوين الكائنات "وينطق مثل" اسم "جيسون". جيسون هو تنسيق لتبادل البيانات المستندة إلى النص، مصمم لنقل البيانات المهيكلة، ويشجع استخدامه لنقل البيانات بين تطبيقات الويب وخوادم الويب.



كوبرميت

مجموعة لبنات البناء ("الأوليات")، التي توفر بشكل جماعي أليات تنشر التطبيقات، والحفاظ عليها، وتوسيع نطاقها. يعرف أيضا بأنه نظام مفتوح المصدر لتصميم الحاويات، لأتمتة نشر التطبيقات الحاوية وتوسيع نطاقها وإدارتها.



دفتر

دفتر يمكن فقط الإضافة اليه



السيولة

امكانيه تحويل الأصل إلى نقد



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

عربي



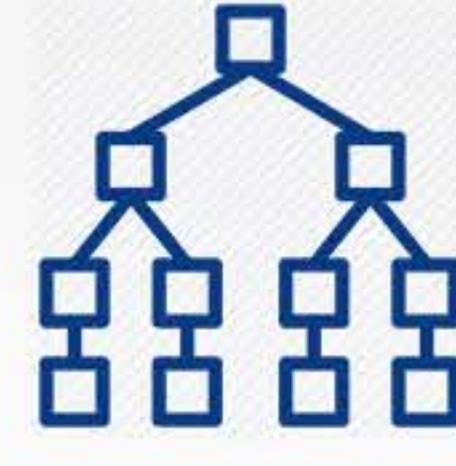
شبكة البرق

شبكة لامركزية تستخدم وظائف العقود الذكية في البلوك تشين لتمكين الدفع الفوري على شبكة من المستخدمين



رسملة السوق

القيمة الاجماليه المحتفظ بها في عمله مشفرة



شجره مركله

شجره يتم تعريف كل ورقه طرفية فيها بهاش كتله البيانات السابقة لها، ويتم تسميه كل ورقه غير طرفية بتعريف مشفر لتعريفات الأطراف التابعة لها



التنقيب

التحقق من صحة معاملات البلوك تشين، يتطلب قدرات حوسبية و طاقة وكهرباء لحل الغاز، التنقيب يكافئ بالعملات حسب الطاقة الحوسبية الخاصة بك



تجمع التنقيب

مجموعه من المنقبين الذين يجتمعون معا لتبادل الطاقة المعالجة علي شبكه ويتوافقوا علي تقسيم مكافأة العثور على كتله جديده داخل التجمع



ميست

متصفح لتثبيت واستخدام التطبيقات اللامركزية



(إم إس بي) مقدم خدمه العضوية

يمكن حوكمة شبكه بلوك تشين فابريك من قبل واحد أو أكثر من مزود خدمه العضوية



(متعدد التوقيعات) المعاملة

تتطلب معاملات التوقيع المتعدد الى أطراف متعددة للموافقة علي المعاملة، تحددها الأحكام.



طرف

نسخه من دفتر يشغله مستخدم علي بلوك تشين



نونس

رقم يستخدم مره واحده فقط في اتصال مشفر ((غالبا ما يتضمن طابع زمني



مشكله لا شيء في الرهان

يحدث هذا بسبب مصادقه وموافقة الأطراف علي كافة المعاملات علي البرامج القديمه والجديده بعد حدوث التفرع الصلب



(إن بي إم) مدير حزم الأطراف

مدير الحزم الافتراضي في بيئة تشغيل جافا سكريبت، يدير تبعيات التطبيقات



بروتوكول أووث

التحويل المفتوح هو معيار يستخدم من قبل خدمات الجهات الخارجية للاحتفاظ بمعلومات المستخدم وتوزيعها دون تعريض كلمه المرور الخاصة بهم



(أومر) أو عم

كتله تمت عملية التنقيب عليها بالكامل ولكن لم تضاف بعد إلى البلوك تشين



الحوكمة علي السلسلة

نظام لإداره وتنفيذ التغييرات إلى عملات البلوك تشين المشفرة



اوراكل

واجهه تربط بين العقود الذكية ومصادر البيانات



شبكة الطلبيات

شبكة كمبيوتر تسمح للأطراف بمشاركه الموارد



(بي تو بي) الند للند

نموذج لا مركزي حيث يكمل طرفان معامله بدون طرف ثالث وسيط، يتفاعل المشتري والبائع مباشرة.



بي كية أي (البنية التحتية) للمفتاح العمومي

مجموعه من الأدوار والسياسات والإجراءات اللازمة لإنشاء الشهادات الرقمية وإدارتها وتوزيعها وإستخدامها وتخزينها وإبطالها وأداره تشفير المفاتيح العمومية



براجما أو خط براجما

تعريف إصدار برنامج التحويل البرمجي الذي يستخدمه العقد الذي



بلوك تشين خاص

بلوك تشين يمكنه السيطرة علي من لديه حق الدخول عليه. علي عكس البلوك تشين الخاص لا يستخدم خوارزميات توافق الآراء مثل إثبات العمل أو إثبات الرهان، بدلا من ذلك يستخدم نظام معروف باسم متسامح الخطأ البيزنطي، وهو ليس نظام موثوق به مما يجعله اقل أمانا



إثبات النشاط

يتم مكافاه أصحاب المصلحة النشطين الذين يحافظون علي أطراف كاملة



إثبات الحرق

يقوم المنقبون بإرسال العملات المشفرة إلى عنوان غير نشط وحرقهم، ثم يتم تسجيل الحرق علي البلوك تشين ويكافأ المستخدم



إثبات السعة

التأمر بالقرص الصلب (تخزين الحلول علي القرص الصلب قبل بدء التنقيب)، القرص الصلب الأسرع في حل المشكلة يفوز بالكتله



إثبات الوقت المنقضي

خوارزميه توافق الآراء التي يجب ان تنتظر الأطراف لفترة زمنية تم اختيارها عشوائيا ويتم مكافاه أول طرف يكمل الفترة الزمنية



(إثبات الرهان) (بي أو إس)

خوارزميه توافق الآراء التي تختار مالك كتله جديده استنادا إلى الثروة لديهم أو (الحصة). ليست هناك مكافاه كتله ولذلك يأخذ المزورون رسوم معاملات



(إثبات العمل) (بي أو دبليو)

خوارزميه توافق الآراء التي تتطلب من المستخدم "التنقيب" أو حل ألغاز رياضية معقدة من أجل التحقق من المعاملة. يكافأ المنقبين بالعملات المشفرة علي أساس القدرة الحوسبية.



إثبات الأهميه

إثبات الأهميه هو خوارزميه توافق الآراء في إن أي إم (الحركة الاقتصادية الجديدة). مماثله لخوارزميه إثبات الرهان: الأطراف يحاجه إلى وضع مبلغ من العملة لتكون مؤهله لإنشاء كتله ويتم اختيارها بناء على خلق كتله متنسبه مع بعض النقاط



باب / صاب

النشر/الاشتراك



بلوك تشين عام

بلوك تشين يمكن الوصول اليه علنا



تشفير المفتاح العمومي

التشفير الذي يستخدم اثنين من المفاتيح ذا الصلة الرياضية. مفتاح عام وخاص. من المستحيل إشتقاق المفتاح الخاص إستنادا إلى المفتاح العمومي.



رست إية بي

(أي) (نقل الحالة التمثيلية)

يعرف القيود القائمة علي إيتش تي بي بي



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

عربي



(آر بي سي) استدعاءات الاجراء البعيد
بروتوكول يستخدم من برنامج لطلب خدمه من برنامج آخر موجود علي الشبكة



آر إس إية
نظام تشفير لتشفير رسالة بالمفتاح العمومي خاص بشخص بحيث يمكن لهذا الشخص فقط فك تشفير الرسالة في قدر معقول من الوقت



ساتوشي نكاموتو
الفرد أو الكيان الذي أنشأ بروتوكول بيتكوين بعد ان نجح في حل مشكله العملة الرقمية "من الانفاق المزدوج"



سيجويت
عملية زيادة حد حجم كتله علي بلوك تشين عن طريق إزالة بيانات التوقيع من معاملات البيتكوين



إس دي كية
توفر مجموعه تطوير البرامج الأدوات الضرورية للمطور لإنشاء برنامج علي منصة معينه



إس إيتش إية 256
أحد أعضاء دالات تجزئته التشفير إس إيتش إية 256 المصممة من قبل إن إس إية. معنى إس إيتش إية هو عملية تشفير الهاش. تستخدم في عدة أجزاء مختلفه من شبكة بيتكوين: التنقيب يستخدم إس إيتش إية 256 لإثبات العمل



شاردينج
تقسيم بلوك تشين إلى عدة شبكات أصغر تسمى شطايا قادره علي معالجه المعاملات بالتوازي



العقد الذي
عقد ذاتي التنفيذ مع شروط اتفاقية مكتوبة في الرمز



سوليديتي
لغة برمجته تستخدم للكتابة العقود الذكية علي شبكه اثيريام



العملة المشفرة المستقرة
عمله مشفرة مصممه للتقليل من اثار تقلبات الأسعار مثل الربط بعمله، أو لتبادل السلع (المتداولة) مثل المعادن الثمينة



ترجيح الحصة
وظيفة إثبات الرهان حيث وزن "التصويت" متناسب مع نسبة الرموز التي يملكها المستخدم



الرمز
تمثيل الأصول الرقمية المبنية علي بلوك تشين موجود



الاقتصاد الرمزي
دراسة وتصميم وتنفيذ نظم اقتصادية علي أساس تكنولوجيا بلوك تشين



دفتر غير الرمزي
دفتر موزع لا يتطلب عمله أصليه للعمل



لغة تورينج كامله
نظام قادر علي التعرف علي مجموعات أحكام مختلفة لمعالجه البيانات



اوبونتو
نظام تشغيل مفتوح المصدر ومجاني من توزيع لينوكس



يو تي إكس أو (أخطبوط المعاملات الغير منفقة)
استخدام مخرجات المعاملة غير المنفقة لتحديد ما إذا كانت المعاملة صالحه



جهاز ظاهري
مضاهاة نظام الحوسبة



في إم وير
الشركة التابعة ل "ديل" التي توفر الحوسبة السحابية وبرامج وخدمات تصور المنصات



لاعب في إم وير
x64 حزمه برامج التصور لأجهزة كمبيوتر أو Microsoft تعمل بنظام التشغيل Linux



فايبر
لغة برمجته تم إنشاؤها لتكون مقدمه رسميه للعقود الذكية



محفظة
يخزن الأصول الرقمية التي تملكها



(منطاد) أو منطاد مفتوح
مجتمع من مطوري العقود الذكية ذوي العقول المتشابهه



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

中国

51% 攻擊

當大多數在區塊鏈中的礦工開始對其他節點(或使用者)進行攻擊的情況;這類攻擊會導致花費資源加倍或者資產被盜竊。



ABI (應用程式二進位介面)

在兩個二進位程式模組之間的介面,其中一個程式通常是程式庫,另一個則會由使用者來執行。



地址

地址(加密地址)用于在網路上發送和接收交易



聚集式交易

將多項交易匯集成在一起,讓其可無需認證就相互置換,以及其他先進的邏輯。使用於NEM中。



協議分類帳

由兩個或多個用戶協商並達成協議的分佈式分類帳



替代幣

任何可做為比特幣替代品的加密貨幣。



API

應用程式編輯介面(可傳送要求及接收回應之遠端伺服器的一部分)。



比特幣

在2009年創造出來的第一款,同時也是最普遍被使用、以區塊鏈去中心化帳本為基礎的加密貨幣。



阻斷高度

区块中连接在一起的区块数



區塊鏈 (公開)

一種用於將數位交易資訊(或資料)儲存在無法竄改的點對點帳本中,因此極不容易偽造,同時又能讓任何人都可以存取的數學結構。



商務邏輯層

用於決定經營企業時所要遵守各種規則的規章內容。



企業網路卡

提供連接到區塊鏈企業網路所需之必要資訊



拜占庭故障容忍度 (BFT)

在一般的名詞中,拜占庭故障容忍度(BFT)就是一個系統能抵抗因為拜占庭常見問題所引發失效類型的特性。這代表即使在某些節點出現失效或異常作業的情況下,一個BFT系統仍可繼續運作。



Casper

結合了工作量證明和權益證明的共識演算法。以太坊以後會使用casper做為權益證明的移轉機制。



CDN (內容傳遞網路)

可快速轉換搭載網際網路內容(html、js、css等)所需的各種資產。



中心化

由一個集中式、進行授權的位置或群組進行維護。



鏈碼

透過所提交的應用程式而創造和管理一個帳本狀態的程式。



頻道

個區塊鏈頻道就是分離的資料頻道,可讓節點私下進行通訊或者對交易進行投資等,而不會讓整個網路上的人都看到。



CLI

指令列介面。



貨幣

在一個新的區塊鏈上所建立的數位資料代表資訊。



貨幣基底

買賣比特幣的最大交易額,且會將比特幣轉換成美金或其他貨幣。



生成CLI

可用於執行管理工作的超級帳本指令列。



生成REST伺服器

從所部署的區塊鏈中產生一個REST api。



確認

指示區塊鏈事務已由網絡通過挖掘進行驗證



共識

一個網路中所有參與者都同意的一項交易正確性的情況。



共識進程

在分類帳內容上達成共識的過程



聯合區塊鏈

所謂的聯合區塊鏈,就是其中的共識流程是由事先選取好的一組節點進行控制的區塊鏈。



容器技術

是一個可被部署在與原本所產生環境不同的環境中並穩定執行的一項軟體應用程式,例如 Docker 或 Kubernetes。



Cryptocurrency

基于数学的数字资产,其中加密技术用于管理资产的生成并转移。加密货币独立于中央银行运作



CRUD

創造、取回、更新、刪除。



加密程式功能

用於取回任何規模的輸入資料,並回傳一個有固定長度、獨一無二字符串的功能。



加密

一種使用代碼保護通信的方法



Dagger Hashimoto

針對在以太坊1.0中挖礦演算法所建議使用的規格。



DApps

去中心化的應用程式。



DDoS 攻擊

一種拒絕服務的攻擊行為,也就是意圖入侵者在找尋機會以暫時或無限制的中斷主機服務與網際網路的連結,藉此讓一部機器或網路資源無法被原本要使用的人員存取。



分权

权力和责任从集中式系统,政府或党派转移到分布式网络。



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

中国



困

指示在工作量中明挖掘中度的



去中心化

讓處理交易的分散式電腦(或節點)形成共享網路,可在沒有集中管理的第三方轉介的情況下處理交易的一種概念。



數位資料

任何以二進位來源碼的形式存在,且包含使用權限的文字或媒介。



数字身份

数字身份是个人,或子网中采用或声明的在网身份。



數位簽名

一種用於代表數位資料授權認證的數學規劃方法。



双倍花

有人試圖同時向兩個不同的收件人發送比特幣交易的情況



Enum

一個位址數類別。



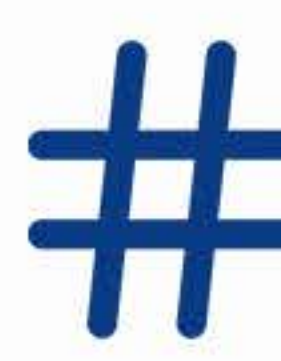
EOA

外部擁有的帳號。



ERC20

以太坊提出對備註標準的要求。



ET-Hash

以太坊1.0所使用的工作量證明演算法。



以太坊

使用一種內建的程式編輯語言,讓使用者可根據其本身的需求進行修改,並建構去中心化帳本的區塊鏈應用程式。會使用智慧合約驗證在帳本內的交易內容。



交

加密的地方



菲亞特

法定貨幣,其價值由發行它的政府支持。例如:美元,歐元,人民幣,日元



區塊鏈應用性的FITS 模型

決定區塊鏈是否可適用於:應用程式內詐騙情形普遍、存在轉介、需要流量、穩定的資料等情況。



分叉

網路上的所有節點基本上全都贊同軟體更新內容的情況。



可交換性

項商品或者資料可與其他有相同類別的個別商品或資料進行交換的能力。適用於Corda分散式帳本。



氣體(以太坊)

用於量測在以太坊區塊鏈內執行一項作業所支付以太數量的方法。



創世區塊

區塊鏈中最開始形成的區塊。



GitHub

修改在公開區塊鏈中的區塊鏈資料。需要在網路中的所有節點都升級和同意新的版本。



Golang (Google 語言)

Golang是一個由google 在2009年所建立,以C為基礎的程式編輯語言。



Gossip 協定

一個gossip協定就是電腦與電腦進行通訊的程序或流程;這是以社群網路傳播資訊或是以流行疾病散布的方法為基礎所建構。屬於一種通訊協定。



監督

為了區塊鏈所建立的一套規則,可決定如何進行監督、管理及管控或保護。



硬分叉

Alters the blockchain data in a public blockchain. Requires all nodes in a network to upgrade and agree on the new version.



硬件錢包

可以連接到Web並與在線交換進行交互的物理設備



Hash 功能

畫出一個任意大小資料地圖的功能。



熱錢包

一個隨時直接連接到互聯網的錢包



熱/冷錢包

項對加密貨幣的描述方式,其中熱錢包就像是支票存款帳戶,冷錢包則像是儲蓄存款帳戶。



超級帳本

由linux基金所創始,超級帳本是開放式來源區塊鏈的保護計畫。



超級帳本生成

超級帳本生成是可簡化在超級帳本網絡上,區塊鏈應用程式開發作業的區塊鏈應用程式開發架構。



超級帳本網絡

由linux所主導的超級帳本專案,可掌控被稱為是鏈碼的智慧合約



IDE (整合式開發環境)

軟體開發者所使用,主要以來源碼編輯器、建構自動化工具及偵錯器所組成的應用程式。



不可變更

無法變更儲存在區塊鏈中「無法變更」資料。(甚至連管理員都無法變更)。



初次貨幣發行 (ICO)

要創建新的加密貨幣事業時用於籌措資金的表單。這是以初次公開發行(IPO)為模型所建構。ICO的創始人都會收到金鑰。



產生實例

產生實例就是在一個以物件為主的程式編輯(OOP)語言中建立一個物件的作業方法。一個產生實例的物件會有一個名稱,並使用在分類宣稱資料中所描述的結構,而在記憶體或磁碟中產生。



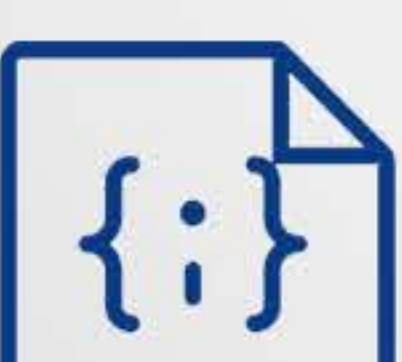
不變的因素

在進行指定的轉變時會保持不變的功能、數量或者特性。



IPFS

星際檔案系統。



JSON

「JavaScript 物件描述」且唸起來像是「傑森Jason」這個名字是一種以文字為基礎的資料交換格式,專門設計用於傳送結構化的資料;這最常被用於在網頁應用程式與網頁伺服器之間傳送資料。



Kubernetes (s)

被定義成是一組建構用區塊(「原始單元」),整體而言可提供各種機制而對應用程式進行部署、維護及放大規模等作業;另外也被定義成是一個開放式來源碼容器協作系統,可用於對容器化應用程式進行自動化部署、放大規模及管理作業。



萊傑

僅附加存儲的記錄



流動性

資產轉換為現金的能力



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

中国



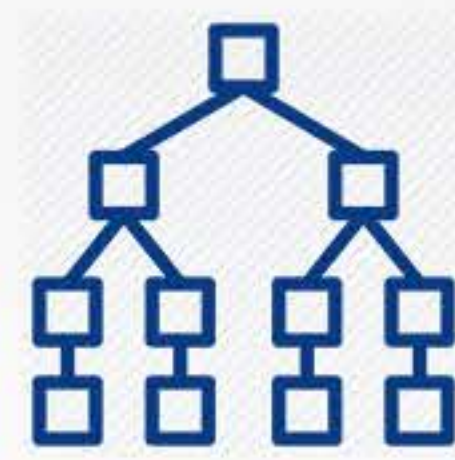
Lightning 網路

Lightning 去中心化網路在區塊鏈中使用智慧合約功能, 在參與者構成的網路中實現立即付款。



市價

加密貨幣持有的總價。



Merkle樹

在這棵樹上每一個葉片節點都會以一個資料區塊的hash進行標示, 且每一個非葉片節點都會以其子節點標籤的加密hash進行標示。



挖礦

驗證區塊鏈交易的行為。需要運算能力及電力以解決「謎題」。挖礦成功就可依照您的運算能力贏得貨幣。



挖礦團體

一群集聚在一起, 並在同一個網路上分享他們的運算能力, 且同意平分在團體內找到的新區塊所產生獎勵的一群礦工。



Mist

安裝和使用Dapps的瀏覽器。



MSP

(會員服務供應商) 一個超級帳本網路區塊鏈網路可由一或多個MSP進行監督。



多重簽名

多重簽名交易會需要多方核准該交易, 而且以各種規定做最後的決定。



節點

一位使用者在區塊鏈上所操作帳本的拷貝內容。



Nonce

在加密通訊作業中只被使用一次的數字 (通常會包含一個時間標記)。



權益內容空白的問題

這是因為在發生硬分叉的情況後, 驗證器節點認可了在舊有和新軟體上的所有交易而造成。



NPM

(節點封包管理員) 預設的封包管理員執行運行環境 node.js。NPM會針對一個應用程式管理其相關內容。



Oauth 協定

開放式授權是一項標準, 通常是協力廠商服務作用於在不需顯示其密碼的情況下, 保存和分送使用者資訊。



Ommmer

(也被稱為是老爹) 這是一個已經被完全開挖, 但還沒有被增加到區塊鏈中的區塊。



鏈上監督

管理加密貨幣區塊鏈, 以及對其進行修改的一套系統。



神諭

連接智能合約和數據源的界面。



Orderer 網路

可讓多個節點共享資源的一個電腦網路。



P2P (點對點)

在這個去中心化模型中, 兩個關係人會在沒有中間第三方的情況下完成交易。買方和賣方直接進行互動。



PKI

(公開鑰匙基礎架構) 在產生、管理、分送、使用、儲存及撤銷數位認證, 以及在管理公開鑰匙加密作業時所需的一組功能定位、政策與程序。



Pragmas s Pragma

可定義智慧合約所使用的編譯器版本。



私人區塊鏈

可控制哪些人可進行存取的區塊鏈; 與其相反的是開放式區塊鏈。私人區塊鏈並不會使用POW或POS這類的共識演算法, 而是使用被稱為拜占庭故障容忍度(BFT)的系統。BFT並不是會降低BFT系統的安全防護的不可靠系統。



活動量證明

維持讓整個節點都獲得獎勵的積極活動相關人士。



消耗證明

礦工將貨幣傳送到一個沒有被使用的地址, 讓這些貨幣完全被消耗掉。消耗的過程會被記錄在區塊鏈上, 且使用者會收到獎勵。



容量證明

繪製您的硬碟內容 (在開始挖礦前將硬碟上的解決方案儲存下來)。具有最快速解決方案的硬碟就可以贏得區塊。



處理時間證明

所有節點都必須加入並等待一段不隨機選取的時間長度, 且第一個結束此時間長度的節點就會獲得獎勵的一種共識演算法。



權益證明 (POS)

根據擁有者所掌握的財產或 (權益) 進行選擇的一種共識演算法。由於並沒有區塊獎勵, 因此偽造者要負擔交易費用。



工作量證明 (POW)

這種共識演算法會需要使用者進行「挖礦」, 或者要解決一個複雜的數學謎題以便驗證一項交易。「礦工」會根據其運算能力獲得加密貨幣以做為獎勵。



重要性證明

重要性證明是一個在NEM中的區塊鏈共識機制。與權益證明類似之處在於: 節點需要「給出」一定數量的貨幣, 才具備建立區塊的資訊, 且根據某些評分按照比例被選出來建立區塊。



Pub/Sub

公布/註冊。



公共區塊鏈

公共可訪問的區塊鏈



公開鑰匙加密法

使用兩套數學相關鑰匙——公開和私人——加密方法。無法利用公開鑰匙推导出私人鑰匙。



REST API (代表性狀態傳送API)

用於根據http定義各種限制條件。



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

中国



RPC (遠端程序呼叫)

一個程式用於要求另一個位在網路上的程式提供某項服務的一種協定。



RSA

RSA加密系統會使用一個屬於個人的公開鑰匙對一項訊息進行加密,因此只有那個人才可在合理的時間內對訊息進行解密。



Satoshi Nakamoto

創建比特幣協議的個人或實體已成功解決了“雙重支出”的數字貨幣問題



Segwit

藉由刪除比特幣交易內的簽名資料,以增加區塊鏈上區塊尺寸限制的一種流程。



SDK

一套軟體開發套件,可提供各種必要的工具,讓開發者可在特定的平台上產生軟體



SHA-256

SHA-256 是NSA所設計SHA-2加密hash功能的其中一環, SHA代表的是安全性Hash 演算法。SHA-256被使用在比特幣網路中的許多不同部分:進行挖礦時會用SHA-256當作工作量證明。



撕碎

將一個區塊鏈切割成許多更小的區段網路行為被稱為撕碎,這樣就可以平行處理多個交易。



智慧合約

可使用編寫在程式碼內的合約條文而自動執行的合約。



智能合約

一種用於在以太坊網上寫智能合約的語言



穩定貨幣

其定義就是被設計用於減少對價格波動性影響的加密貨幣,例如鎖定某一個貨幣,或者交換所交易的商品(例如貴金屬)。



權益比重

權益證明中的一項功能,讓某個使用者的「投票權」比重會是他所擁有的認證碼比例的函數。



認證碼

代表在現存區塊鏈上所建置數位資料的相關內容。



驗證碼經濟

基本上參照到建構在區塊鏈技術經濟系統的研究、設計及執行等作業。



無標記分類帳

不需要本機貨幣操作的分類帳



圖靈完整語言

可執行一部電腦能力所及的運算語言。



Ubuntu

免費的開放式來源作業系統及linux分散作業。



UTXO (未支付的交易輸出)

未支付的交易輸出會被用於決定一項交易是否有效。



虛擬機器

一套運算系統的模擬內容。



VMware

Subsidiary of dell的子公司,專門提供雲端運算及平台視覺化軟體和服務。



VMware 玩家

在執行Microsoft或Linux的X64電腦上使用的視覺化軟體套件。



VYPER

被創造出來正式推薦給智慧合約的程式編輯語言。



錢包

用於儲存您所擁有的數位資料。



Zeppelin (或 Open Zeppelin)

由理念相同的智慧合約開發者所組成的社群。