

GLOBAL BLOCKCHAIN GLOSSARY OF TERMS

- English
- Español
- Deutsche
- Français
- عربى
- 普通话



Please enjoy this resource of Global Blockchain Terms 2.0; now released in 6 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, Alexandre Cieux



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

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



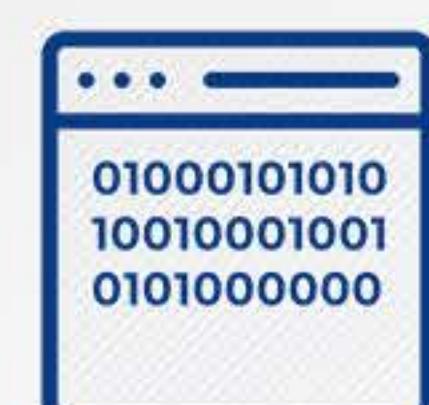
Cryptocurrency

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



Address

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



Aggregated Transactions

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



Alt-coin

Any cryptocurrency that exists as an alternative to bitcoin



API

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



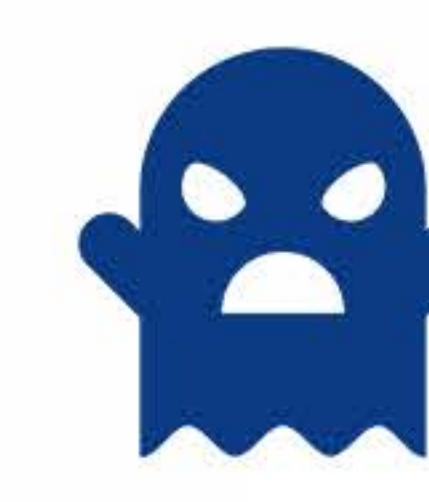
Bitcoin

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



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



CDN (Content Delivery Network)

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



CLI

Command Line Interface



Coin

Representation of a digital asset built on a new blockchain



Consensus Process

The process of reaching consensus on a ledger's content



Composer Rest Server

Generates a REST API from a deployed Blockchain



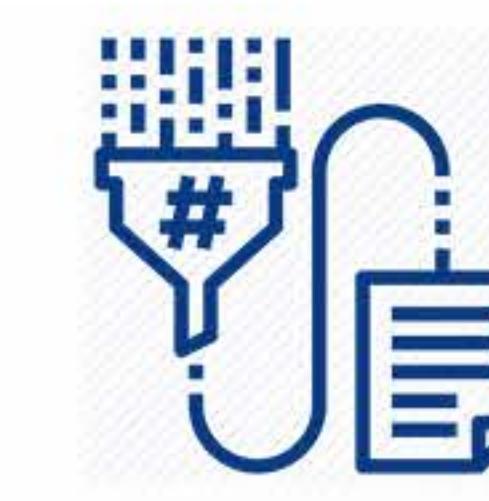
Container Technology

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.



CRUD

Create, retrieve, update, delete



Cryptographic Hash Function

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



DApps

Decentralized Applications



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



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



Digital Signature

A mathematical scheme used for presenting the authenticity of digital assets



ERC20

Ethereum request for comments standard



Fiat

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



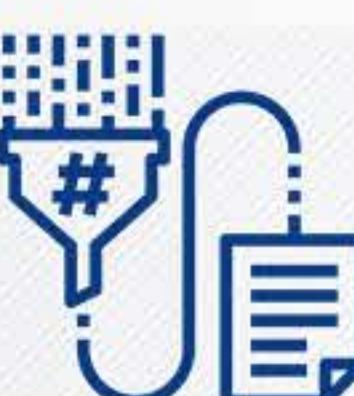
Gas (Ethereum)

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



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



Hash Function

A function that maps data of an arbitrary size



Hyperledger Composer

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



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.



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.



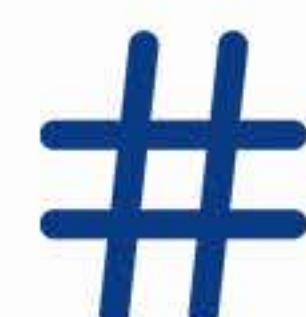
Decentralized

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



Double Spend

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



ET-Hash

The proof of work algorithm used by Ethereum 1.0



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.



Genesis Block

The initial block within a blockchain



Governance

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



Hot Wallet

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



Hyperledger Fabric

Hyperledger project hosted by Linux which hosts Smart Contracts called Chaincode



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.



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.



Digital Asset

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



Enum

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



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.



Fork

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



GitHub

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



Hard Fork

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



Hot/Cold Wallet

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



IDE (Integrated development Environment)

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



Invariant

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



Ledger

An append-only store of records



Digital Identity

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



EOA

Externally Owned Account



Exchange

A place to buy and sell cryptocurrency



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



Golang (Google language)

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



Hardware Wallet

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



Hyperledger

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



Immutable

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



IPFS

Inter Planetary File System



Liquidity

The ability of an asset to be converted into cash



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0



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



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



Node

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



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



Orderer Network

A computer network that allows nodes to share resource



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 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



Pub/Sub

Publish/Subscribe



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.



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.



NPM (Node Package Manager)

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



Oracle

An interface that connects smart contracts and data sources



Pragma(s) or Pragma-line

Defines which compiler version the smart contract uses



Ommer (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



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.



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 Activity

Active Stakeholders who maintain a full node are rewarded



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.



Public Blockchain

A publicly 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



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



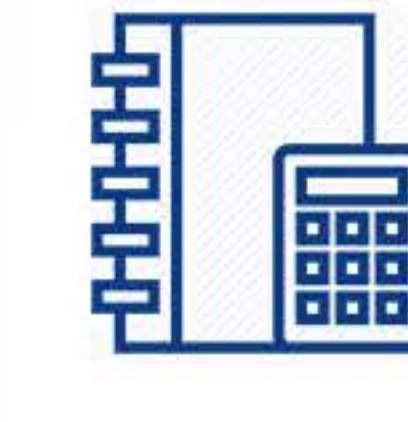
Token

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 visualization 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

ENGLISH



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 más usuarios para negociar y alcanzar acuerdos.

Altura del Bloque

Número 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 cálculos matemáticos, en esta se utilizan técnicas de encriptación las cuales son usadas para regular la creación de unidades de moneda y verificar la transferencia de fondos. Las criptomonedas operan de forma independiente de un banco central.

Dagger Hashimoto

Propuesta específica 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 usará Casper como una transición hacia prueba de participación (PoS).



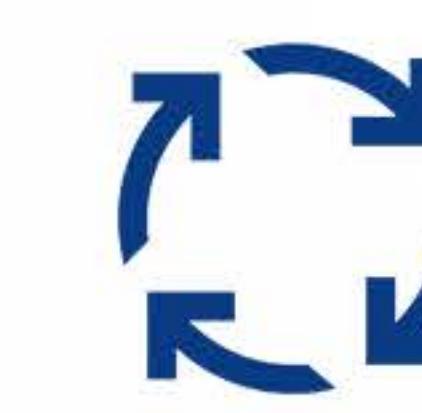
Canal

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.



Transacciones agregadas

Consolidar 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

Método para proteger comunicaciones usando códigos.



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.



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.



Firma electrónica / digitalizada

Un mecanismo matemático utilizado para identificar la autenticidad de activos digitales



ERC20

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



Fiat (Garantía)

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



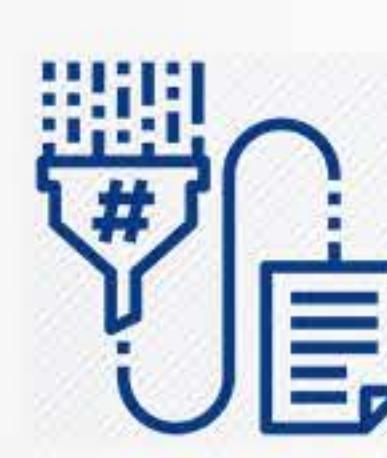
Gas (Ethereum)

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



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 como se propaga una epidemia.



Función hash

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



Hyperledger Composer

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



Oferta inicial de monedas (ICO)

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



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.



Descentralizado

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



Doble Gasto (Double Spend)

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



ET-Hash

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



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.



Bloque génesis / bloque 0

El primer bloque dentro de una blockchain



Gobernanza

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



Monedero en linea (Hot Wallet)

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



Hyperledger Fabric

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



Insticiar / 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



Kubernetes(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.



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.



EOA

Cuentas externas



Exchange

Lugar en el cual se compran y venden criptomonedas.



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



Golang (lenguaje Go)

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



Monedero Fisico (Hardware Wallet)

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



Hyperledger

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



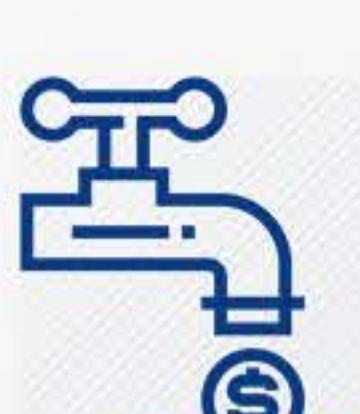
Inmutable

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



Sistema de archivos interplanetarios (IPFS)

Sistema de archivos interplanetarios



Liquidez

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



Blockchain terms 2.0



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



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



Nodo

Una copia del registro operado por un usuario de la blockchain



Protocolo Oauth

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



Red de solicitantes

Una red de ordenadores que permite a sus nodos compartir recursos



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 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



Pub/Sub

Publicar / suscribir



Capitalización de Mercado o Market Cap

Es el valor total retenido en una criptomonedas



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



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



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)



Gobernanza on-chain

Un sistema para gestionar e implementar cambios a una criptomonedas blockchain



NPM (Administrador de Paquetes de Nodos)

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



Oráculo

Una interfaz que conecta contratos inteligentes y fuentes de datos.



Pragma(s) o Pragma-line

Define qué versión del compilador utiliza el contrato inteligente



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



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 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.



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 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 usado 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



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)



Stablecoin

El término adjudicado a una criptomonedas 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)



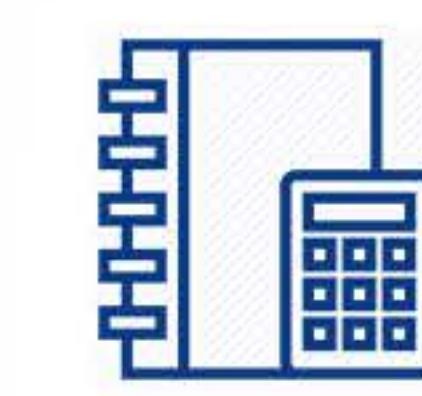
Solidity

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



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.



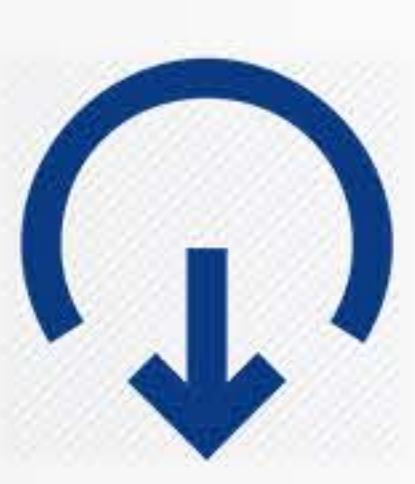
Máquina Virtual

Emulación de un sistema informático



Monedero

Protege los activos digitales del propietario.



Salida de transacción no utilizada (UTXO)

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



VYPER

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



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



Contrato inteligente (Smart Contract)

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



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.



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



Ubuntu

Sistema operativo de código abierto y distribución de Linux



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



Zeppelin o Zeppelin Abierto

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



Blockchain terms 2.0

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 (öffentliche)

Eine mathematische Konstruktion um digitale Transaktionen (oder Daten) in einem unveränderbaren, Peer-to-Peer Kontoführungssystem 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 Blockchaintkanal ist ein separater Datenkanal welcher es einzelnen Nodes erlaubt privat zu kommunizieren – beispielsweise Transaktionenverschick ohne, dass das ganze Netzwerk es sieht.



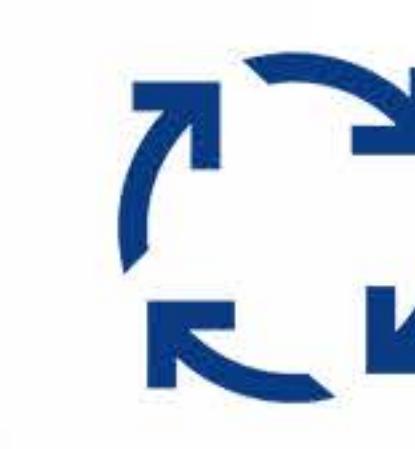
Composer CLI

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



Deutsche

Adresse

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



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



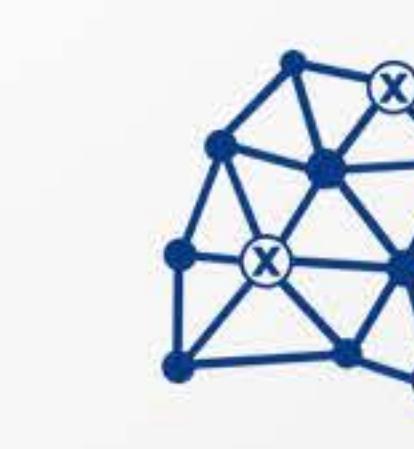
DDos Attacke

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



Dezentralisierung

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





Blockchain terms 2.0

Deutsche



Schwierigkeit

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



Digitale Signatur

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



ERC20

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



Fiat

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



Gas (Ethereum)

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



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.



Hashfunktion

Eine Funktion die Daten beliebiger Größe abbildet.



Hyperledger Composer

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



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.



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.



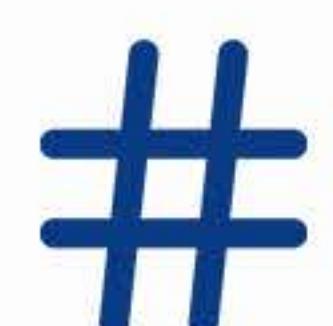
Dezentralisiert

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



Doppelte Ausgaben

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



ET-Hash

Der von Ethereum 1.0 genutzte Proof of Work Algorithmus



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



Genesis Block (Ursprungsblock)

Der erste, initiale Block einer Blockchain.



Führung

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



Heiße Geldbörse

Eine Brieftasche, die jederzeit direkt mit dem Internet verbunden ist



Hyperledger Fabric

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



Instanziieren

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



Kubernetes

Eine Menge an Erstellungsböcken (“Primitives”), die kollektiv einen Mechanismus zum Veröffentlichen, 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.



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.



EOA

Account mit externem Besitz



Austausch

Ein Ort zum Kaufen und Verkaufen von Kryptowährung



Austauschbarkeit

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



Goland (Google Programmiersprache)

Eine Programmiersprache basierend auf C, erfunden 2009 von Google



Hardware-Geldbörse

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



Hyperledger

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



Unveränderlich

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



IPFS

Inter Planetary File System (Interplanetares Dateisystem)

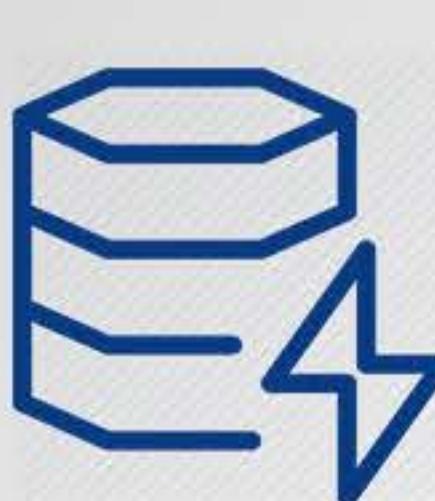


Liquidität

Die Fähigkeit eines Vermögenswerts, in Bargeld umgewandelt zu werden



Blockchain terms 2.0



Lightning Network

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



Mining pool

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



Node

Eine Kopie des Kontenbuches im Betrieb beim Benutzer auf der Blockchain



OAuth Protokoll

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



Orderer Network

Ein Computernetzwerk das es Nodes erlaubt Ressourcen zu teilen.



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.



Nachweis über verstrichene Zeit (Proof of Elapsed Time)

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



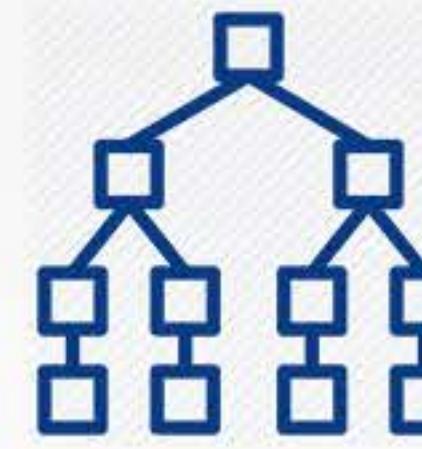
Pub/Sub

Publish/Subscribe – Veröffentlichen/Abonnieren



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.



Multi-Signatur (Transaktion)

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



NPM (Node Package Manager)

Die Standard Paket Manager Umgebung von NodeJS. NPM manages Abhängigkeiten für Anwendungen.



Orakel

Eine Schnittstelle, die intelligente Verträge und Datenquellen miteinander verbindet



Pragma(s) oder Pragma-Zeile

Definiert welche Compiler-Version der Smart Contract benutzt.



Nonce

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



Ommer (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.



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 wiederholen.



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

Aktivitätsnachweis (Proof of Activity)

Aktive Beteiligte die eine Full-Node betreiben werden belohnt.



Arbeitsnachweis (Proof of Work, PoW)

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



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.



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.



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.



Öffentliche Blockchain

Eine öffentlich zugängliche Blockchain



Blockchain terms 2.0



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 Schüssel um es zu ermöglichen die Nachricht in akzeptabler Zeit wieder zu entschlüsseln.



SDK (Softwareentwicklungssystem)

Ein oftwareentwicklungssystem 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).



Stablecoin (Stabile Münzen)

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



Tokenless Ledger

Ein Ledger, für das keine einheitliche Währung erforderlich ist



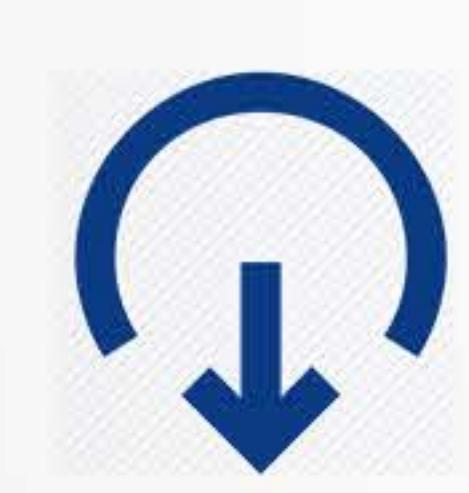
Solidität

Eine Programmiersprache zum Schreiben von intelligenten Verträgen im Ethereum-Netzwerk



Tokenökonomie

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



UTXO (Ungenutzter Transaktionsausgang)

UTXO wird benutzt um die Gültigkeit einer Transaktion zu bestimmen.



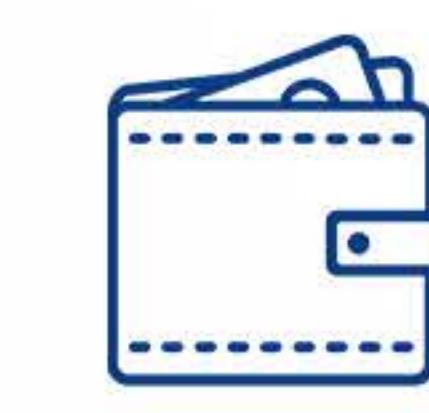
VYPER

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



Virtuelle Maschine

Eumlation eines Computersystems.



Wallet (Geldbörse)

Speichert digitale Güter



Deutsche



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.



Smart Contract (Intelligente Verträge)

Selbst-erfüllende Verträge mit den Vertragsbestimmungen als Computercode definiert.



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.



Ubuntu

Freies open-source Betriebssystem und Linux Distribution



Turing Vollständig

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



VMware Player

Ein Virtualisierungspaket für x64 Computer die Windows oder Linux benutzen.



VMware

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



Zeppelin (oder Open Zeppelin)

Eine Community von ähnlich gesinnten Smart Contract Entwicklern



Attaque 51%

Une situation dans laquelle une majorité de mineurs de la blockchain lance une attaque sur le reste des nœuds (ou utilisateurs). Ce type d'attaque permet la double-dépense ou le vol des avoirs.



Registre d'accord

Un registre distribué utilisé par deux utilisateurs ou plus pour négocier et parvenir à un accord.



Hauteur du bloc

Référence d'un bloc, utilisée pour l'identifier dans un réseau.



BFT (Tolérance aux Pannes Byzantines)

La tolérance de panne byzantine (BFT) est la propriété d'un système capable de résister à un type de pannes, dérivé du problème des généraux byzantins. Cela signifie qu'un système BFT est capable de continuer à fonctionner même si certains noeuds échouent ou agissent de manière malveillante.



Chaincode

Un programme qui initialise et gère un état de registre via des applications soumises.



Coinbase

La plus grande bourse d'achat-vente et de conversion de Bitcoin en dollars ou en une autre monnaie.



Consensus

Lorsque tous les participants d'un réseau s'accordent sur la validité d'une transaction.



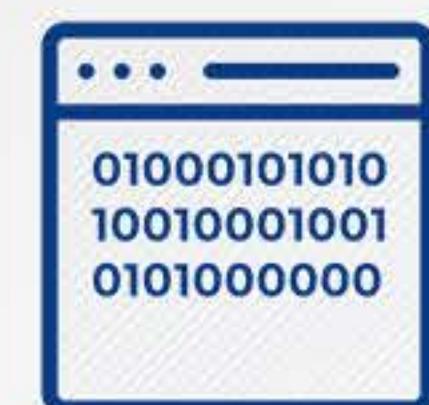
Cryptomonnaie

Une monnaie numérique basée sur les mathématiques, où des techniques de chiffrement sont utilisées pour réguler la génération d'unités de monnaie et vérifier le transfert de fonds. Les cryptomonnaies fonctionnent indépendamment d'une banque centrale.



Dagger Hashimoto

La spécification proposée pour l'algorithme d'extraction dans Ethereum 1.0.



ABI (Interface Binaire d'Application)

Une interface bas niveau, le plus souvent entre une bibliothèque et une application exécutée par un utilisateur.



Adresse

L'adresse (de cryptomonnaie) est utilisée pour envoyer et recevoir des transactions sur le réseau.



Transactions agrégées

Fusion de plusieurs transactions, permettant des échanges entre tiers sans confiance (swaps) ou autre autre logique avancée. Utilisées dans NEM.



Altcoin

Toute crypto-monnaie qui existe comme alternative au bitcoin.



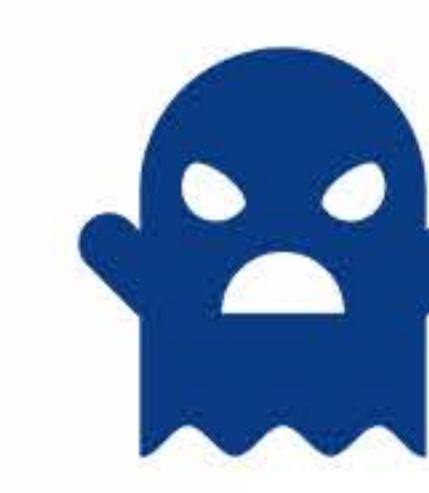
API

Interface de Programmation Applicative (partie d'un serveur distant qui envoie des demandes et reçoit des réponses).



Blockchain (Public)

Une structure mathématique pour stocker des transactions numériques (ou des données) dans un registre immuable, de pair à pair, quasi impossible à falsifier, tout en restant accessible à tous.



Casper

Algorithme de consensus qui combine une preuve de travail et une preuve d'enjeu. Ethereum va utiliser Casper comme transition vers la preuve d'enjeu.



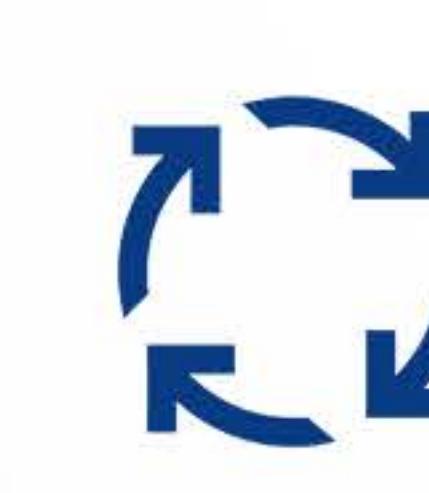
Canal

Un canal Blockchain est un canal de données séparé du reste permettant aux nœuds de communiquer en privé, de financer les transactions, etc. sans que le réseau ne le voit.



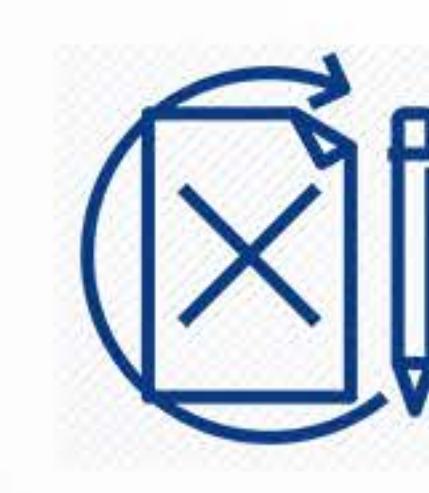
Composer CLI

Ligne de commande Hyperledger permettant des tâches administratives.



Processus de Consensus

Le processus de consensus garantit l'intégrité et la cohérence du registre.



CRUD

Créer, récupérer, mettre à jour, supprimer.



DApps

Applications Décentralisées.



Adresse

L'adresse (de cryptomonnaie) est utilisée pour envoyer et recevoir des transactions sur le réseau.



Transactions agrégées

Fusion de plusieurs transactions, permettant des échanges entre tiers sans confiance (swaps) ou autre autre logique avancée. Utilisées dans NEM.



Bitcoin

La première, la plus populaire, crypto-monnaie basée sur le registre décentralisé d'une blockchain et créée en 2009.



Carte réseau entreprise

Fournit les informations nécessaires pour connecter un réseau d'entreprise blockchain.



Centralisé

Maintenu par un groupe ou un lieu central faisant autorité.



Coin (pièce)

Représentation d'un actif numérique construit sur une technologie blockchain.



Confirmation

Indication que la transaction blockchain a été vérifiée par le réseau par le biais de l'extraction.



Conteneurisation

Une solution pour exécuter de manière fiable une application logicielle, lorsqu'elle est déployée dans un environnement différent de celui dans lequel elle a été créée. Par exemple Docker ou Kubernetes.



Cryptographie

Un procédé de sécurisation de communication à l'aide de code.



Fonction de hachage cryptographique

Une fonction qui reçoit une entrée de n'importe quelle taille et retourne une chaîne unique de longueur uniforme.



Attaque par déni de service (DDOS)

Une attaque par déni de service est une cyberattaque dans laquelle l'auteur cherche à rendre une machine ou une ressource réseau indisponible pour les utilisateurs en interrompant les services d'un hôte connecté à Internet.



Décentralisé

Concept de réseau partagé d'ordinateurs (ou de nœuds) dispersés pouvant traiter des transactions sans intermédiaire.



BLOCKCHAIN TRAINING ALLIANCE

FRANÇAIS



Difficulté

Indice de la difficulté, donné au calcul de validité d'un bloc.



Identité Numérique

Une identité numérique est une identité en ligne ou en réseau, adoptée ou revendiquée dans le cyberspace par un individu, une organisation ou un dispositif électronique.



ERC20

Jeton standard utilisé pour les contrats intelligents Ethereum.



Décret

Cours légal dont la valeur est soutenue par le gouvernement qui l'est. Par exemple: USD, EUR



Gas (Ethereum)

Mesure de la quantité d'Ether payée pour une action donnée exécutée dans Ethereum.



Protocole de potins

Procédure ou processus de communication ordinateur-ordinateur basé sur la manière dont les réseaux sociaux diffusent des informations ou propage des rumeurs. C'est un protocole de communication.



Fonction hash

Une fonction qui mappe des données d'une taille arbitraire.



Hyperledger Composer

Hyperledger Composer est un framework de développement d'applications Blockchain qui simplifie le développement d'applications sur Hyperledger Fabric.



Initial Coin Offering (ICO)

Levée de fonds pour financer de nouvelles entreprises de crypto-monnaie. Modélisée d'après une offre publique initiale (IPO). Les bailleurs de fonds d'une ICO reçoivent des jetons.



JSON

Se prononce comme le nom "Jason.". JSON est un format textuel d'échange de données, conçu pour la transmission de données structurées. Il est généralement utilisé pour transférer des données entre des applications et des serveurs Web.



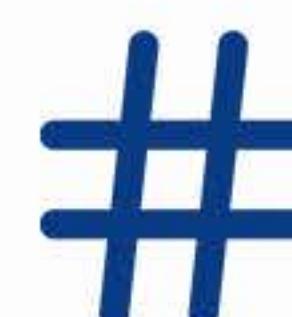
Décentralisé

Concept de réseau partagé d'ordinateurs (ou de nœuds) dispersés pouvant traiter des transactions sans intermédiaire.



Double Dépense

Un scénario où quelqu'un essaie d'envoyer un actif numérique unique à deux destinataires différents en même temps.



ET-Hash

L'algorithme de preuve de travail PoW utilisé par Ethereum 1.0



Modèle FITS pour l'applicabilité de Blockchain

Détermine si la blockchain est pertinente: la fraude est répandue, les intermédiaires existent, le débit est important, des données stables se trouvent dans l'application.



Block Genesis

Le bloc initial d'une blockchain.



Gouvernance

Règles établies pour une Blockchain qui déterminent son mode d'administration et de gestion ou encore de protection.



Portefeuille Chaud

Un portefeuille directement connecté à Internet à tout moment.



Hyperledger Fabric

Projet Hyperledger hébergé par Linux qui héberge des contrats intelligents appelés chaincode.



Instancier

Créer une instance d'un objet dans un langage de programmation orientée objet (OOP). Un objet instancié reçoit un nom et est créé en mémoire ou sur disque à l'aide de la structure (la classe).



Kubernetes(s)

Défini comme un ensemble de blocs ("primitifs"), qui fournissent collectivement des mécanismes de déploiement, de maintenance et de mise à l'échelle des applications. Également défini comme un système open-source d'orchestration de conteneurs pour automatiser le déploiement, la mise à l'échelle et la gestion des applications conteneurisées.



Actif numérique

Tout texte ou media formaté en binaire et incluant le droit de l'utiliser.



Enum

Un type de valeur d'adresse.



Ethereum

Application Blockchain utilisant un langage de programmation intégré permettant aux utilisateurs de créer des registres décentralisés et modifiés en fonction de leurs besoins. Les contrats intelligents sont utilisés pour valider les transactions dans le registre.



Fork (fourche)

Est essentiellement une mise à jour logicielle convenue collectivement par tous les nœuds du réseau.



GitHub

Un service d'hébergement Web pour le contrôle de version et utilisé par les développeurs.



Hard Fork

Modifie les données de la blockchain dans une blockchain publique. Tous les nœuds d'un réseau doivent être mis à niveau et se mettre d'accord sur la nouvelle version.



Portefeuille Chaud / Froid

Description de la crypto-monnaie où les portefeuilles chauds ressemblent à des comptes chèques alors que les portefeuilles froids sont des comptes d'épargne.



IDE - Environnement de Développement Intégré

Application destinée aux développeurs de logiciels et composée principalement d'un éditeur de code source, d'un outil d'automatisation et d'un débugueur.



Invariant

Une fonction, une quantité ou une propriété qui reste inchangée lorsqu'une transformation spécifique est appliquée.



Grand Livre

Un magasin d'enregistrements uniquement



Identité Numérique

Une identité digitale est une identité en ligne ou en réseau adoptée ou revendiquée dans le cyberspace par un individu, une organisation ou un dispositif électronique



EOA

Compte Externe



Échange

Un lieu d'achat et de vente de cryptomonnaies.



Fongibilité

Capacité d'un bien ou d'un actif à être échangé avec d'autres biens ou actifs du même type. Applicable au registre distribué Corda.



Golang (langage Google)

Créé par google en 2009, GOlang est un langage de programmation basé sur le langage C.



Portefeuille Matériel

Un périphérique physique conçu pour se connecter au Web mais qui isole les clés privées afin de protéger les fonds.



Hyperledger

Lancé par la fondation Linux, HyperLedger est un projet cadre de blockchains open source.



Immutable

« Impossible à modifier ». Les données stockées dans une blockchain ne peuvent pas être modifiées (même par les administrateurs).



IPFS (Inter Planetary File System)

Système de fichiers interplanétaire.



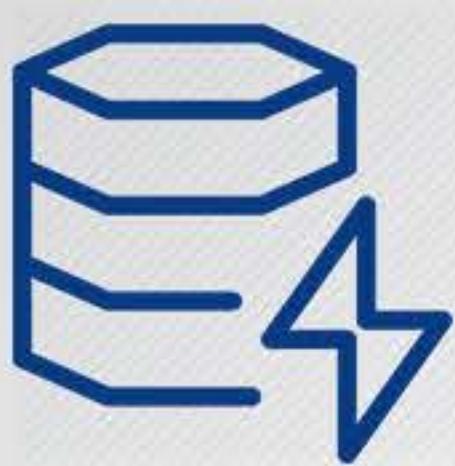
Liquidité

La capacité d'un actif à être converti en espèces.



Réseau Lightning

Un réseau décentralisé utilisant la fonctionnalité de contrat intelligent de la blockchain pour permettre.



Mining pool

Un groupe de mineurs qui se réunissent pour partager leur puissance de traitement et acceptent de partager les récompenses.



Nœud

Une copie du registre exploitée par un utilisateur sur la blockchain.



Protocole Oauth

Open Authorization est une norme utilisée par des services tiers pour conserver et diffuser les informations des utilisateurs sans révéler leur mot de passe.



Réseau de clients

Un réseau informatique qui permet aux nœuds de partager des ressources.



Blockchain Privée

Une blockchain permettant de contrôler qui y a accès. Contrairement à une blockchain publique, une blockchain privée n'utilise pas d'algorithme consensuel tels que POW ou POS, mais utilise un système appelé Byzantine Fault Tolerant (BFT). BFT n'est pas un système sans confiance (trustless) ce qui le rend moins sécurisé.



Preuve du Temps Écoulé (PoET)

Algorithme de consensus dans lequel les nœuds doivent attendre une période choisie de manière aléatoire. Le premier nœud à terminer la période est récompensé.



Pub/Sub

Publier / S'abonner



Capitalisation Boursière

Valeur totale dans une devise



Mist

Navigateur pour installer et utiliser les Dapps.



Nonce

Un numéro utilisé une seule fois dans une communication cryptographique (inclus souvent un horodatage)



Ommer (dit Uncle)

Un bloc qui a été complètement miné mais qui n'a pas encore été ajouté à la Blockchain.



P2P (pair à pair)

Modèle décentralisé où deux parties effectuent une transaction sans tiers. L'acheteur et le vendeur interagissent directement.



Preuve d'Activité

Les parties prenantes actives qui gèrent un nœud complet sont récompensées.



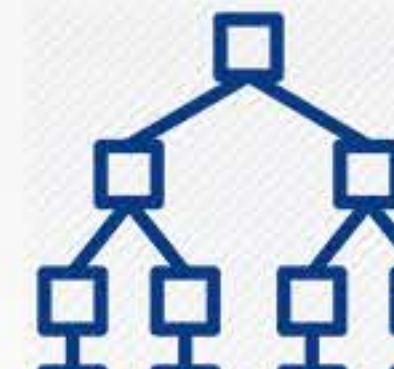
Preuve de participation ou d'enjeu (POS)

Un algorithme de consensus qui choisit le responsable d'un nouveau bloc en fonction de la richesse qu'il possède ou qu'il met en jeu. Le faussaire perdra ce qu'il a mis en jeu.



Blockchain Publique

Une blockchain accessible au public - qui peut être ouverte ou fermée sur la lisibilité des transactions.



Arbre de Merkle

Un arbre algorithmique dans lequel chaque feuille est étiquetée avec le hash d'un bloc de données. Chaque nœud non-feuille est étiqueté avec le hash cryptographique des étiquettes de ses nœuds enfants.



MSP (Fournisseur de Services aux Membres)

Un réseau blockchain Hyperledger Fabric peut être régi par un ou plusieurs MSP.



Mining (minage)

Acte de validation des transactions Blockchain. Nécessite de la puissance de calcul et de l'électricité pour résoudre des «énigmes». La récompense du minage en monnaie virtuelle est fonction de la puissance de calcul.



Multisignature (transaction)

Les transactions à signatures multiples exigent que plusieurs parties approuvent la transaction, déterminée par les règles.



NPM (Gestionnaire de Paquet de Nœud)

Environnement d'exécution du gestionnaire de packages par défaut node.js. NPM gère les dépendances d'une application.



Oracle

Une interface qui connecte les contrats intelligents et les sources de données issues du monde réel.



Pragma(s) or Pragma-line

Définit la version du compilateur utilisée par le contrat intelligent.



Preuve de capacité (PoC)

Traçage de votre disque dur (stockage des solutions sur un disque dur avant le début de l'extraction). Un disque dur avec la solution la plus rapide gagne le bloc.



Preuve d'Importance

Mécanisme consensuel dans la Blockchain NEM. Semblable à la preuve de participation: les nœuds doivent «affecter» un montant en devise pour pouvoir créer des blocs et sont sélectionnés pour créer un bloc proportionnellement à un certain score.



API REST (API de transfert d'état représentatif)

Définit les contraintes basées sur http.



Cryptographie à clé publique

Cryptage utilisant deux clés liées mathématiquement. Une clé publique et privée. Il est impossible de déduire la clé privée sur la base de la clé publique.



RPC (Appels de Procédure à Distance)

Protocole utilisé par un programme pour demander un service à un autre programme situé sur un réseau.



RSA

Système de cryptage RSA pour crypter un message avec la clé publique d'un individu. Seul cet individu pourra déchiffrer le message dans un délai raisonnable.



SDK

Un kit de développement logiciel fournissant les outils nécessaires au développeur pour créer des logiciels.



SHA-256

SHA-256 fait partie des fonctions de hachage cryptographique SHA-2 conçues par la NSA. SHA signifie Secure Hash Algorithm (algorithme de hachage sécurisé). SHA-256 est utilisée dans plusieurs parties du réseau Bitcoin: son minage utilise SHA-256 comme preuve de travail.



Stablecoin

Cryptomonnaie conçue pour minimiser les effets de la volatilité des prix, tel que le rattachement à une devise, ou pour échanger des produits (tels que des métaux précieux).



Solidity

Langage de programmation utilisé pour la rédaction de contrats intelligents sur le réseau Ethereum.



Token économie

Se réfère à l'étude, à la conception et à la mise en œuvre de systèmes économiques basés sur la technologie blockchain.



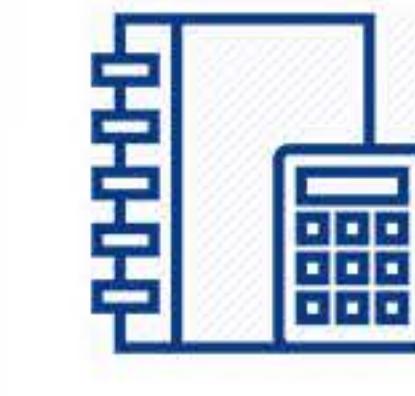
UTXO (Résultats de Transaction non Dépensés)

Les sorties de transaction non dépensées sont utilisées pour déterminer si une transaction est valide.



Vyper

Un langage de programmation créé pour être une introduction formelle aux contrats intelligents.



Registre sans jeton

Registre qui ne nécessite pas de cryptomonnaies ou de jetons pour fonctionner.



Machine Virtuelle

Simulation d'un appareil informatique créée par un logiciel d'émulation.



Wallet

Stocke les actifs numériques que vous possédez.



Satoshi Nakamoto

Un individu ou un groupe d'individus qui a créé le protocole Bitcoin, après avoir résolu avec succès le problème de la double dépense.



Segwit

Processus par lequel la taille maximale des blocs d'une blockchain est augmentée en supprimant les données de signature des transactions Bitcoin.



Smart Contract (Contrat Intelligent)

Contrat auto-exécutant dont les termes de l'accord sont inscrits dans le code.



Sharding (éclatement)

Diviser une blockchain en plusieurs réseaux de composants plus petits appelés shards, (fragments) capables de traiter des transactions en parallèle.



Pondération des enjeux

Une fonction de preuve d'enjeu où le poids de son «vote» est fonction de la proportion de jetons qu'il possède.



Token (jeton)

Représentation d'un actif numérique construit sur une blockchain existante.



Ubuntu

Une distribution de Linux, un système d'exploitation libre et gratuit.



VMware

Filiale de Dell qui fournit des logiciels et des services de cloud computing et de visualisation de plateformes.



VMware Player

Logiciel de virtualisation pour ordinateurs x64 exécutant Microsoft ou Linux.



Zeppelin (ou Open Zeppelin)

Communauté de développeurs Smart Contract partageant les mêmes idées.



Blockchain terms 2.0

عربى

51% هجوم

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



(آي بي آي) واجهة التطبيق الثانية

واجهة بين اثنين من وحدات برنامج ثانٍ، غالباً 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 عده معاملات في معاملة واحدة، والسامح بمقاييسه غير موثقة، وغيرها من المنطقيات المتقدمة. يستخدم في إن آي إم (الحركة الاقتصادية الجديدة).

دفتر الاتفاقيه

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



عملة بديلة

أي عمله بديلة لعملة بيتكوين



(آي بي آي)

واجهه التطبيقات البرمجيه (جزء من خادم بعيد يرسل الطلبات ويتلقي الاستجابات



عملة بيتكوين

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

ارتفاع الكتله

عدد الكلب
المتصلة معاً في سلسله بلوك تشين



بلوك تشين

بنيه رياضيه لتخزين المعاملات الرقمية (أو البيانات) في دفتر غير قابل للتغيير، دفتر من نظير إلى نظير يصعب بشدة تزيفه مع البقاء في متداول اي شخص



طبقه منطق الاعمال

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



بطاقة شبكة الاعمال

توفير المعلومات الضروريه لتوصيل شبكه بلوك تشين

التسامح مع الخطأ البيزنطي

التسامح مع الخطأ البيزنطي (بي إف تي) هو خاصية لنظام قادر على مقاومه فئة الإخفاقات المشتركة من مشكلة الجنالات 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. أثيريات سيستخدم كاسبر للانتقال لإثبات الرهان



شبكة توصيل المحتوى

يسمح بالانتقال السريع من للأصول اللازمة لتحميل محتوي الإنترن特 (إيتش تي إم إل)، (جي إس إس، سي إس إس، الخ)



مركزي

يتم الحفاظ عليه من قبل موقع مركزي أو مجموعة ذات سلطة

تشين كود

برنامج يقوم بتهيئة وإدارة حالة 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 للإتصالات



سي إل آي

واجهه سطر الأوامر



عملة

قميل الأصول الرقمية التي بنيت على بلوك تشين جديد

كونبيس

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 ريسست للتطبيقات البرمجيه من بلوك تشين منشور



تأكيد

اشارة انه تم التحقق من معاملة بلوك تشين من قبل الشبكة من خلال التقىب

توافق الاراء

الاتفاق من جميع المشاركين في الشبكة على صحة المعاملة



إجماع عمليه

عملية الوصول إلى توافق الآراء بشأن محتوى دفتر



اتحاد بلوك تشين

بلوك تشين حيث يتم التحكم في عملية توافق الآراء من قبل مجموعة محددة مسبقاً من الأطراف



تكنولوجيا الحاويات

حل لتشغيل تطبيق برمجي بشكل يعتمد عليه عند نشره في بيئه مختلفه غير التي تم إنشاؤه فيها. مثل دوكر أو كيوهابتس

عمله مشفره

عمله رقميه تعتمد علي الرياضيات، حيث تستخدم تقنيات التشفير لتنظيم توليد وحدات العملة والتحقق من تحويل المول. 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



التشفيـر

طريقه لتأمين الاتصال باستخدام التعليمات البرمجية

داجر هاشيموتـو

المواصفات المقترنة لخوارزميه التقىب في اثيريات 1.0



دابس

تطبيقات لمركزية



هجمـات 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



اللامركـزيـه

نقل السلطة والمسؤولية من سلطة مركزية أو حكومة أو طرف الي شبكه موزعه



Blockchain terms 2.0

عربي



صعوبة

دلالة من مدى صعوبة التتحقق من الكتل في التقبيل باستخدام خوازمية إثبات العمل



المركززي

مفهوم الشبكة المشتركة لأجهزة الكمبيوتر المشتقة (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

هو فيه الكترونيه 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 أصاله الأصول الرقمية



الإنفاق 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



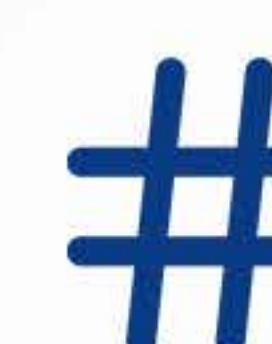
إي أو إيه

حساب خارجي مملوك



إي آر سي 20

طلب اثيريوم للتعليقات القياسية



أي تي هاش

خوارزمية إثبات العمل المستخدمة في اثيريوم 1.0



اثيريات

تطبيق بلوك تشين يستخدم لغة برمجية مضمنة تسمح للمستخدمين بناء 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، مثل: الدولار والين واليورو



نموذج فيتس لتطبيق البلوك تشين

نموذج لتقييم ملائمة بلوك تشين باستخدام الاختيار منتشر، الوسطاء موجودون، الانتاجية مطلوبة، البيانات المستقرة موجودة في التطبيق.



شوكة

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



التبادلية

قدر السلعة أو الأصل على أن يتم تفاعل مع السلع أو الأصول الفردية الأخرى من نفس النوع. ينطبق على دفتر كوردا الموزع



بروتوكول القيل والقال

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



جينيسس بلوك

اول كتلة داخل بلوك تشين



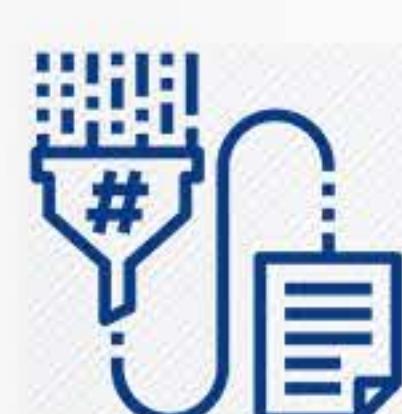
جيit هب

خدمه استضافه علي شبكة الانترنت للتحكم في الإصدارات باستخدام "جيit". مستخدمة من قبل مطورو بلوك تشين



جولانج

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



عملية الهاش

داله تقوم بتعيين بيانات بحجم عشوائي



المحفظة الساخنة

محفظه متصلة مباشرة بالإنترنت في جميع الأوقات



الشوكة الصلبة/الباردة

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



ملحن هايبرليدجر

ملحن هايبرليدجر هو اطار عمل تطوير تطبيقات لتيسير تطبيقات بلوك تشين على هايبرليدجر فاريبريك



نسيج هايبرليدجر

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



(آي دي اي) بيئه التطوير المتكاملة

تطبيق لمطوري البرامج التي تتكون في المقام الأول من محرك التعليمات البرمجية المصدرية، أداء أنهته الإنشاء، والمصحح



ثابت

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



العرض الاولى 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 اسم و يتم إنشاؤه في الذاكرة او على القرص الصلب باستخدام البنية الموصوفة ضمن تعريف الفتنه المتميي لها



ثابت

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



آي إف بي إس

نظام الملفات الكوكبية المشتركة



جيـة سـون

جاـفا سـكريـبت لـتـدوـينـ الكـائـنـاتـ "وـيـنـطـقـ مـثـلـ" اـسـمـ "جيـسـونـ". جـيـسـونـ هوـ توـسيـقـ لـتـابـلـ الـبـيـانـاتـ الـمـسـتـنـدـةـ إـلـىـ النـصـ، مـصـمـمـ لـتـقـلـيـدـ الـبـيـانـاتـ الـمـهـيـكـلـةـ. وـيـشـعـ اـسـتـخـدـمـهـ لـتـقـلـيـدـ الـبـيـانـاتـ بـيـنـ تـطـبـيقـاتـ الـوـبـ وـخـوـادـمـ الـوـبـ.



كـوبـرمـيت

مـجمـوعـةـ لـبنـاتـ الـبـنـاءـ ("ـأـلـوـاـيـاتـ")ـ،ـ الـتـيـ توـفـرـ بشـكـلـ جـمـاعـيـ أـلـيـاتـ تـشـرـتـ الـتـطـبـيقـاتـ،ـ وـالـحـفـاظـ عـلـيـهـ،ـ وـتوـسـعـ نـطـاقـهـ.ـ يـعـرـفـ أـيـضاـ بـأـنـهـ نـظـمـ مـفـتوـحـ الـمـصـدـرـ لـتـصـمـيمـ الـحاـوـيـاتـ،ـ لـأـقـتـهـ نـشـرـ الـتـطـبـيقـاتـ الـحـاوـيـةـ وـتوـسـعـ نـطـاقـهـ وـإـدارـهـهـ.



دفتر

دفتر يـمـكـنـ فـقـطـ إـضـافـةـ الـيـةـ



الـسـيـوـلـهـ

امـكـانـيـهـ تـحـوـيـلـ الـأـصـلـ إـلـىـ نـقـدـ



Blockchain terms 2.0

عربي



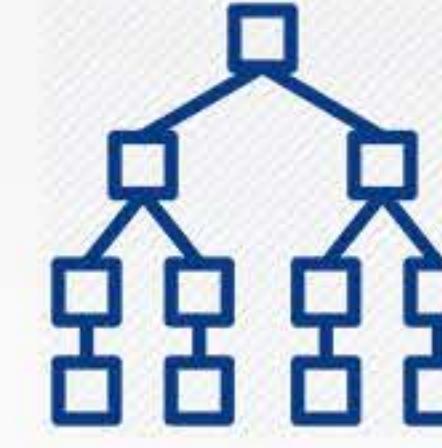
شبكة البرق

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



رسملة السوق

القيمة الاجمالية المحتفظ بها في عمله مشفرة



شجره مرکله

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



لتنقيب

التحقق من صحة معاملات البلوك تشين. يتطلب قدرات حوسية وطاقة وكهرباء لحل الغاز. التنقيب يكافئ بالعملات حسب الطاقة الحوسية الخاصة بك.



تجمع التنقيب

مجموعه من المنقبين الذين يجتمعون معاً لتبادل الطاقة المعالجة علي شبكه بلوك تشين فابريك من مكافأة العثور على كتله جديده داخل التجمع



ميست

متصفح لثبتت 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 إلى أطراف متعددة للموافقة على المعاملة، تحددها الأحكام.



طرف

نسخه من دفتر يشغلها مستخدم علي بلوك تشين خدمات الجهات الخارجية لاحتفاظ بمعلومات المستخدم وتوزيعها دون تعريف كلمه المرور الخاصة بهم



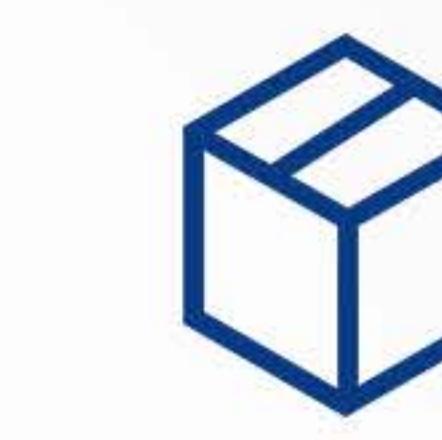
نونس

رقم يستخدم مره واحدة فقط في اتصال مشفر ((غالباً ما يتضمن طابع زمني



مشكله لا شيء في الرهان

يحدث هذا بسبب مصادقه وموافقة الأطراف على كافة المعاملات على البرامج القديمة والجديدة بعد حدوث التفزع الصلب



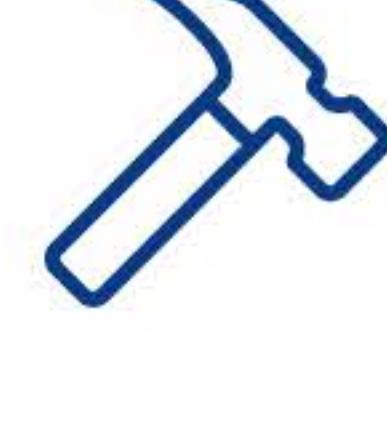
(إن بي إم) مدير حزم الأطراف

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



بروتوكول أووث

التخوين المفتوح هو معيار يستخدم من قبل خدمات الجهات الخارجية لاحتفاظ بمعلومات المستخدم وتوزيعها دون تعريف كلمه المرور الخاصة بهم



(أومر أو عم)

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



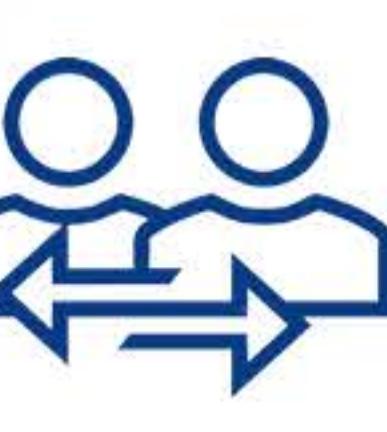
الحكومة على السلسلة

نظام لإدارة وتنفيذ التغييرات إلى عمليات البلوك تشين المشفرة



شبكة الطلبيات

شبكة كمبيوتر تسمح للأطراف بمشاركة الموارد



(بي تو بي) الند للند

نموذج لا مركزي حيث يمكن طرفان معامله بدون طرف ثالث وسيط. يتفاعل المشتري والبائع مباشره.



بي كية آي (البنية التحتية للمفتاح العمومي)

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



برامجما أو خط براجما

تعريف إصدار برنامج التحويل البرمجي الذي يستخدمه العقد الذي



بلوك تشين خاص

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



إثبات النشاط

يتم مكافاه أصحاب المصلحة النشطين الذين يحافظون علي أطراف كاملة



إثبات الحرق

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



إثبات السعة

التآمر بالقرص الصلب (تخزين الحلول على 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 زمنيه تم اختيارها عشوائياً ويتم مكافاه أول طرف يكمل الفترة الزمنيه



(إثبات الرهان) بي أو إس

خوارزميه توافق الآراء التي تختار مالك كتله جديده استناداً 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 أغذار رياضيه معقده من أجل التحقق من المعاملة. يكافأ المنقبين بالعمليات المشفرة علي أساس القدرة الحوسية.



إثبات الأهميه

إثبات الأهميه هو خوارزميه توافق الآراء في إن أي إم (الحركة الاقتصادية الجديدة). مماثله لخوارزميه إثبات الرهان: الأطراف بحاجه إلى وضع مبلغ من العملة لتكون مؤهله لإنشاء كتل 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

التشفيير الذي يستخدم اثنين من المفاتيح ذات الصلة الرياضية. مفتاح عام وخاص. من المستحيل إشتقاق المفتاح الخاص استناداً إلى المفتاح العمومي



رست إيه بي

(آي) نقل الحالة التمثيلية

يعرف القيد القائمه علي ايتش تي بي



Blockchain terms 2.0

عربى



آر بي سي (استدعاءات الاجراء البعيد)

بروتوكول يستخدم من برنامج لطلب خدمه من برنامج آخر موجود على الشبكة



آر إس إيه

نظام تشفير لتشغير رسالة ب密فتاح العمومي
خاص بشخص بحيث يمكن لهذا الشخص فقط
فك تشفير الرسالة في قدر معقول من الوقت



سا تو شى ن كا مو تو

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



سي جويت

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



إس دي كيه

توفر مجموعه تطوير البرامج الأدوات الضروريه
للمطور لإنشاء برنامج علي منصة معينه



إس إيتش إيه 256

أحد أعضاء دالات تجزئه التشفير إس إيتش إيه
256 المصممه من قبل إن إس إيه. معنى
إس إيتش إيه هو عملية تشفير الهاش. تستخدم
في عده أجزاء مختلفه من شبكة بيتكوين:
التنفيذ يستخدم إس إيتش إيه 256 لإنبات
العمل



شارد ينج

تقسيم بلوك تشين إلى عده شبكات أصغر
تسمى شظايا قادره علي معالجه المعاملات
بالتوازي



العقد الذكي

عقد ذاتي التنفيذ مع شروط اتفاقية مكتوبة في
الرمز



سو ليد يتي

لغة برمجه تستخد للكتابه العقود الذكيه علي
شبكة اثيريوم



العملة المشفرة المستقرة

عمله مشفره مصممه للتقليل من اثار تقلبات
الأسعار مثل الربط بعمله، أو لتبادل السلع
(المتداوله) (مثل المعادن الثمينه).



ترحیح الحصة

وظيفة إثبات الرهان حيث وزن "التصويت"
متناسب مع نسبة الرموز التي يملكونها
امسخدم



الرمز

تمثيل الأصول الرقمية المبنية علي بلوك تشين
موجود



الاقتصاد الرقمي

دراسة وتصميم وتنفيذ نظم اقتصاديه علي أساس
تكنولوجيا بلوك تشين



دفتر غير الرمزي

دفتر موزع لا يتطلب عمله أصليه للعمل



لغة تورينج كامله

نظام قادر علي التعرف علي مجموعات أحکام
مختلفة معالجه البيانات



أوبونتو

نظام تشغيل مفتوح المصدر ومجاني من توزيع
لينوكس



يو تي إكس أو (أخطبوط المعاملات الغير منفذة)

استخدام مخرجات المعامله غير المنفذه لتحديد
ما إذا كانت المعامله صالحه



جهاز ظاهري

مضاهاه نظام الحوسبة



في إم وير

الشركة التابعة ل "ديل" التي توفر الحوسبة
السحابية وبرامج وخدمات تصوّر المنصات



لاعب في إم وير

64x حزمه برامج التصور لأجهزه كمبيوتر
أو Microsoft Windows تعمل بنظام التشغيل
Linux



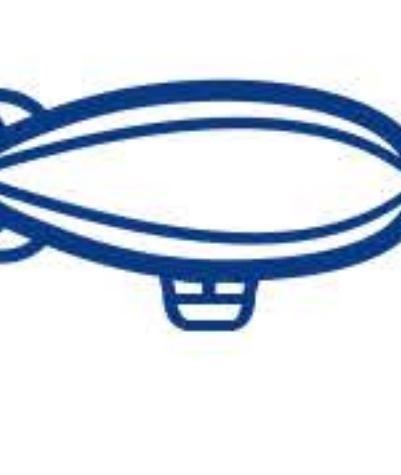
فاير

لغة برمجه تم إنشاؤها لتكون مقدمه رسميه
للعقود الذكيه



محفظه

يخزن الأصول الرقمية التي يملكونها



(منطاد أو منطاد مفتوح

مجتمع من مطوري العقود الذكيه ذوي
العقل المتشابه



普通话

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。

替代幣

任何可做為比特幣替代品的加密貨幣。



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



阻塞高度

区块中接在一起的块数



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。



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。



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。



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。



Cryptocurrency

基于数学的数字区块，其中加密技术用于管理区块位的生成并转移资金的转移。加密独立于中央银行运作。



Dagger Hashimoto

針對在以太坊1.0中挖礦演算法所建議使用的規格。



地址

地址(加密区块地址)
用于在网路上发送和接收交易



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。



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。



企業網路卡

提供連接到區塊鏈企業網路所需之必要資訊



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。



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。



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。



生成CLI

可用於執行管理工作的超級帳本指令列。



共識進程

在分類帳內容上達成共識的過程



CRUD

創造、取回、更新、刪除。



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。



CLI

指令列介面。



生成REST伺服器

從所部署的區塊鏈中產生一個REST api。



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。



貨幣

在一個新的區塊鏈上所建立的數位資材代表資訊。



確認

指示區塊鏈事務已由網絡通過挖掘進行驗證



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。



加密

一種使用代碼保護通信的方法



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、獨一無二字串的功能。



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向分布式网路转移。





普通话



困

指示在工作量證明挖掘中遇到的困难。



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。



數位簽名

一種用於代表數位資材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。



ERC20

以太坊提出對備註標準的要求。



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。



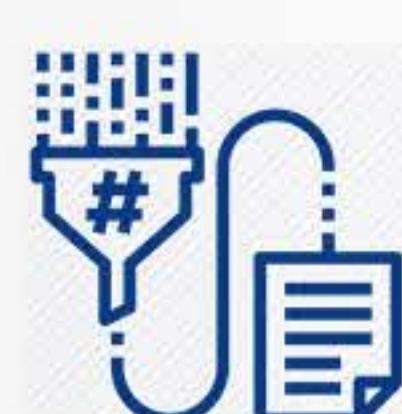
氣體(以太坊)

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。



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。



Hash 功能

畫出一個任意大小資料地圖的功能。



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。



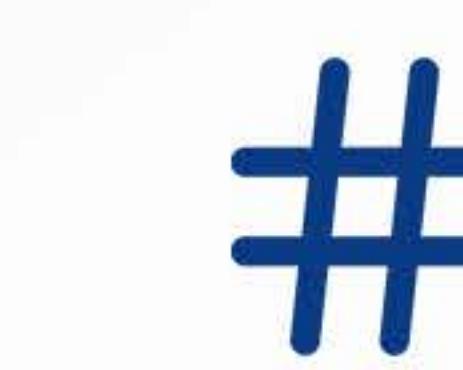
初次貨幣發行(ICO)

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。



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。



ET-Hash

以太坊1.0所使用的工作量證明演算法。



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、需要流通量、穩定的資料等情況。



創世區塊

區塊鏈中最開始形成的區塊。



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。



熱錢包

一個隨時直接連接到互聯網的钱包。



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



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。



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布署、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,可用於容器化應用程式進行自動化布署、放大規模及管理作業。



數位資材

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。



數字身份

數字身份是個人,組織或子組織在網際空間中採用或聲明的在線或網際身份。



Enum

一個位址數的類別。



EOA

外部擁有的帳號。



交

指加密的地方



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。



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

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



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。



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



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。



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)。



IPFS

星際檔案系統。



流動性

資產轉換為現金的能力



普通话

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。



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。



節點

一位使用者在區塊鏈上所操作帳本的拷貝內容。



Oauth 協定

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



Orderer 網路

可讓多個節點共享資源的一個電腦網路。



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，而是使用被稱為是拜占庭故障容忍度(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。



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。



Pub/Sub

公布／註冊。



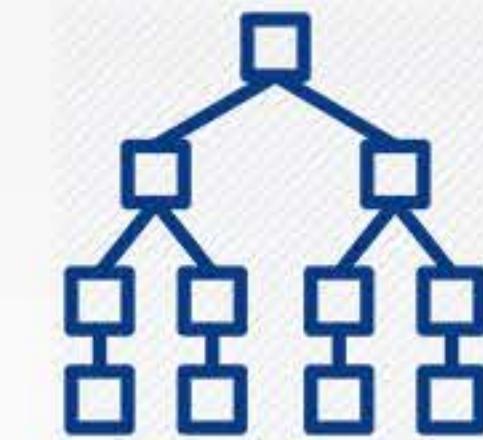
市囝

加密貨幣持有的總價



Mist

安裝和使用Dapps的瀏覽器。



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。



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。



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。



神諭

連接智能合約和數據源的界面



Pragmas

可定義智慧合約所使用的編譯器版本。



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。



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占用的地址，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。



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。



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導出私人鑰匙。



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

普通话



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。



密囑度

一种用于在以太坊网上写智能合的程言



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材的相關內容。



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



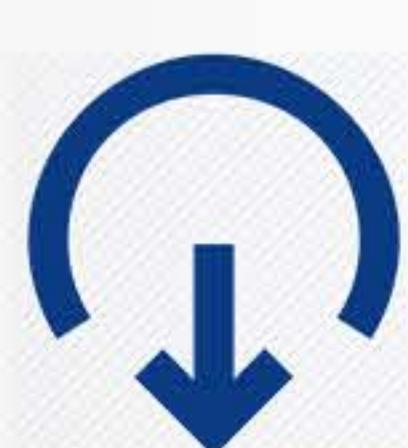
圖靈完整語言

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。



Vyper 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材。



Zeppelin

（或 Open Zeppelin）由理念相同的智慧合約開發者所組成的社群。