MUNDO BLOCKCHAIN

Desarrollado por: Hans Castro

EMPLEOS.NET

Hans Castro

Educador y desarrollador de contenido

+506 89677882

@hanscastro11

hanscastro11

Sobre Hans Castro

Soy un emprendedor digital desde hace 6 años, me considero entusiasta de la tecnología y me encanta poder brindar valor a los estudiantes con información sobre uno de los temas que más me ha llamado la atención cuando lo descubrí. Soy de San José Costa Rica. y descubrí el mundo del blockchain en el año 2018 en una reunión de amigos cuando un amigo estaba en su computadora hablando sobre las criptomonedas y no le importaba la reunión en que estabamos, no me quise quedar con la duda de que era eso de lo que él venía tan entusiasmado y le pregunté, pues fue lo mejor que pude haber hecho, ese día mi vida cambio ya que conocí el nacimiento de un mercado basado en activos digitales, donde toman valor conforme su utilidad en las industrias.

Ese día me llevo a cuestionarme que era lo que estaba detrás del Bitcoin, porque Bitcoin había llegado a superar los $19.000 en ese momento y porque miles de proyectos estaban surgiendo y tomando tanto valor, eso me llevo a profundizar, investigar y relacionarme con todas las personas y proyectos relacionados a la tecnología Blockchain para así poder comprender el verdadero potencial de esta tecnología y porque está causando realmente una revolución. Durante 4 años he estado estudiando las cadenas de bloques, en el 2021 fui certificadopor una de las universidades más prestigiosas de tecnología, el Instituto Tecnológico de Massachusetts.

Este documento contiene miles de horas en investigación, experiencia e información que he acumulado durante todo este tiempo, para así poder ayudar a quien este también dispuesto en aprender

Descargo de responsabilidad.

El uso de activos digitales puede provocar la pérdida de dinero en períodos cortos o incluso largos pasado en la volatilidad de su precio. Los usuarios de activos digitales deben saber que los precios están sujetos a fluctuaciones de amplio rango y que la información publicada en este documento no garantiza que los usuarios de activos digitales no pierdan dinero (fiat).

La información proporcionada en este documento NO constituye asesoramiento de inversión, asesoramiento financiero, asesoramiento comercial o cualquier otro tipo de asesoramiento y no debe tratar el contenido del documento como tal.

CONTENIDOS

CAPÍTULO 1

-EVOLUCIÓN DEL DINERO
-EVOLUCIÓN DEL SISTEMA FINANCIERO
-MOVIMIENTO CYPHERPUNK
-HISTORIA DEL INTERNET
-EVOLUCIÓN DE LA WEB
-WEB 1, WEB 2 Y WEB 3

CAPÍTULO 2

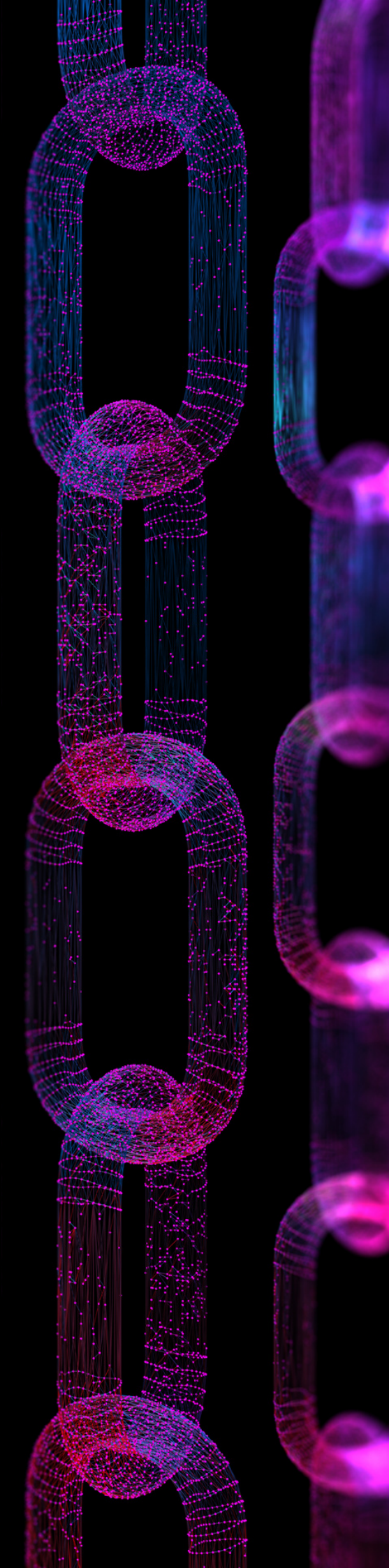
-CADENAS DE BLOQUES
-IMPLICACIONES DE LA TECNOLOGIA BLOCKCHAIN
-IMPORTANCIA DE LA TECNOLOGIA BLOCKCHAIN
-CARACTERISTICAS DE LA TECNOLOGIA BLOCKCHAIN
-ELEMENTOS CLAVES DEL BLOCKCHAIN
-TIPOS DE REDES BLOCKCHAIN
-USOS DE LA TECNOLOGIA BLOCKCHAIN

CAPÍTULO 3

-COMPONENTES DE LAS CADENAS DE BLOQUES
-REDES DESCENTRALIZADAS
-NODOS
-LIBRO CONTABLE
-MINERIA DE BLOQUES
-BLOQUES
-EXPLORADORES BLOCKCHAIN
-CRIPTOGRAFIA
-CLAVES CRIPTOGRAFICAS
-CRIPTOGRAFIA ASIMETRICA
-PROTOCOLOS
-HASH
-FIRMA DIGITAL
-PROTOCOLOS DE CONCENSO

CAPÍTULO 4

-SOLUCION AL DOBLE GASTO
-BLOCKCHAIN VRS MODELO CLIENTE SERVIDOR
-GENERACIONES BLOCKCHAIN
-PRINCIPALES CRIPTOMONEDAS
-BLOCKCHAIN 1, BLOCKCHAIN 2, BLOCKCHAIN 3, BLOCKCHAIN 4



EMPLEOS.NET

CONTENIDOS

CAPÍTULO 5

--BITCOIN
-HALVING DE BITCOIN
-UTILIDADES DE BITCOIN

CAPÍTULO 6

-ETHEREUM
-LENGUAJES DE PROGRAMACION
-CONTRATOS INTELIGENTES
-DAPPS
-PROTOCOLOS
-ETHEREUM 2.0

CAPÍTULO 7

-CARDANO
-SOLANA
-BINANCE

CAPÍTULO 8

-TOKENS
-PLATAFORMAS DE TOKENS
-NFT
-MERCADOS NFT
-PRINCIPALES PROYECTOS EN OPENSEA,

EMPLEOS.NET


"LAS CRIPTOMONEDAS SON UNA FORMA DE DINERO DISEÑADA PARA APROVECHAR EL PODER DE INTERNET."
NICK SZABO
(CIENTÍFICO DE LA COMPUTACIÓN Y CRIPTÓGRAFO)
EMPLEOS.NET

CAPÍTULO 1 : Evolución de los sistemas

La tecnología Blockchain se ha dado mucho a conocer después del surgimiento de uno de sus primeros usos que fueron las criptomonedas como medio de valor para el intercambio de bienes y servicios sin necesidad de intermediarios centralizados, hoy en día la más conocida es Bitcoin.

Lo más importante es entender desde un principio que las criptomonedas son como comparar una gota en el mar por toda la magnitud y todo lo que se puede hacer con la tecnología blockchain. El potencial de la aplicación de esta tecnología en diferentes industrias está cambiando el paradigma económico, social y organizacional de la vida cotidiana de las personas.

El cambio y la evolución siempre ha sido inevitables, siempre todo ha tenido su proceso para hoy ser la realidad en la que vivimos, por lo cual siempre debemos entender de dónde venimos y hacia dónde vamos de la forma más consciente posible y con la información correcta para ir logrando la adaptación a la evolución que se viene viviendo desde hace miles de años.

Evolución del dinero

El dinero es cualquier objeto de valor claramente identificable que es aceptado de forma general para el pago de bienes, servicios y deudas en un mercado o lo que es moneda de curso legal dentro de un país.

El dinero se considera un lenguaje que utilizamos para comunicar e intercambiar valor entre las personas. Usamos el dinero para realizar transacciones económicas, pero criptomonedas, se puede separar el concepto del dinero de la idea del Estado nación como emisor monetario soberano. Hemos evolucionado de la moneda basada en instituciones a la moneda basadas en redes informáticas.

Para que el dinero sea considerado como una herramienta adecuada para efectuar intercambios de valor, debe cumplir con todas y cada una de estas ocho características:

-Confiable
-Durable
-Escaso
-Fácil almacenamiento y transporte
-Fácil de identificar
-Fungible (Reemplazable)
-Difícil de falsificar
-Divisible

Además de las ocho características citadas, también destacamos tres funcionalidades básicas que tiene que cumplir el dinero, unidad de cuenta, reserva de valor y medio de pago e intercambio.

Esto nos lleva a definir el dinero como una herramienta para facilitar el intercambio indirecto y la preservación del valor, que sirve además como unidad de cuenta.

Evolución del dinero

La evolución del dinero y del comercio fue desarrollándose conforme las civilizaciones van creciendo a través de los años. Todo inició con la utilización de granos, trigo, cebada, rocas, ganado, conchas, semillas como forma de intercambio o trueque, alrededor del año 15 000 y 9 000 a. C

El Trueque

Es la acción de dar una cosa y recibir otra a cambio, especialmente cuando se trata de un intercambio de productos sin que intervenga el dinero.

"El trueque es la forma más primitiva de comercio"

Para que un sistema de trueque funcione, es fundamental que cada individuo quiera el bien ofertada por otro y que las cantidades deseadas coincidan con sus disponibilidades. La capacidad para llevar a cabo transacciones mediante trueque es limitada y costosa, ya que depende de una coincidencia de deseos.

Las monedas

En Mesopotamia, paralelamente al nacimiento de la civilización 2500 a.C, se tuvo la idea de utilizar un bien de intermedio que sirviera de canje, naciendo así el dinero, una herramienta que permitió comprar, vender e intercambiar bienes y servicios.

La acuñación y utilización de monedas como (oro, plata, bronce, cobre) como dinero tuvo origen en tres lugares del planeta tierra 600 a.C, los cuales hoy en día seria Turquía, China y la India.

Papel moneda

El papel moneda tiene su origen en China en el siglo VII, se creó para facilitar el comercioy a que era más fácil para transportarlo de un lugar a otro pero su uso no fue oficial hasta el año 812.

Evolución del dinero

Los usuarios no podían entender porque un trozo de papel valía lo mismo que un trozo de oro; esto provoco que la aceptación generalizada del dinero de papel necesitara cuatrocientos años. En Europa, lo primeros billetes de los que hay constancia parecen en Suecia en 1661 de la mano del comerciante Johan Palmstruch, quien los entregaba como recibido para quien depositaba oro u otro metal precioso.

Tarjetas de crédito y debito

El siguiente paso del dinero llegó en 1950 con la llegada de las tarjetas de crédito que al día de hoy más del 70% de la población tiene dinero de plástico como le hacen llamar.

Aplicaciones y billeteras digitales

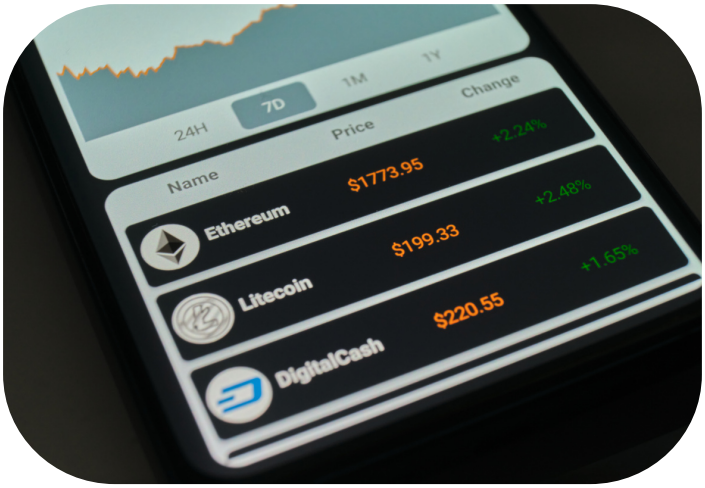
La siguiente generación de medios de pago viene dándose con la introducción de los celulares inteligentes en el año 2011 donde los usuarios ya empiezan a enviar y recibir dinero desde una aplicación desarrollada por una empresa de banco o de confianza.

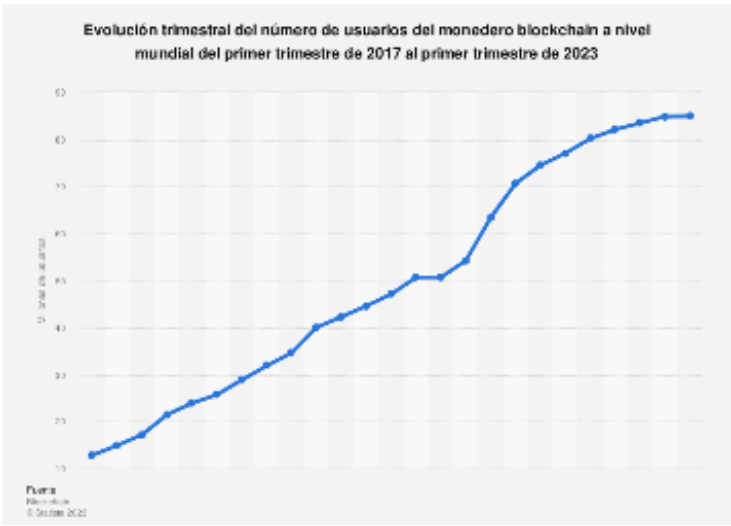
Evolución del dinero

Aplicaciones y billeteras digitales

Billeteras de Criptomonedas

Las billeteras de criptomonedas se utilizaron por primera vez en el 2009 con el surgimiento de la primer generación del blockchain y su primer aplicación para registrar datos distribuida mente en una red descentralizada, de esta forma nace el Bitcoin, como un medio de utilidad para enviar valor entre usuarios sin necesidad de terceros, fue apartir del año 2012 que la adopción y el uso de Bitcoin y más adelante otros proyectos de criptomonedas impulsarán el crecimiento y uso de billeteras virtuales que hasta el día de hoy no ha dejado de crecer como se muestra en el gráfico según el historial de personas con wallets.





Influencias sociales, financieras y tecnológicas

Durante el último siglo la humanidad ha visto un cambio muy fuerte en la evolución social, económica y tecnológica lo que ha creado la necesidad de buscar cada vez más soluciones a problemas. El surgimiento de la tecnología blockchain es un claro ejemplo de que para que existiera, primero debió a ver toda una problemática y un proceso evolutivo de la sociedad en áreas económicas, sociales y tecnológicas.

La evolución del sistema financiero

El patrón oro

El patrón oro es en el que la moneda está respaldada por oro. Es un sistema monetario en el que el emisor de la divisa garantiza que pueda dar al poseedor de sus billetes la cantidad de oro consignada en ellos.

La vigencia del patrón oro empezó durante el siglo XIX como base del sistema financiero internacional. Terminó a raíz de la Primera Guerra Mundial, puesto que los gobiernos que estaban en guerra necesitaban imprimir mucho dinero fiduciario para financiar el esfuerzo bélico sin tener la capacidad de respaldar ese dinero en metal precioso.

La evolución del sistema financiero

Acuerdos de Bretton Woods

Después de la segunda guerra mundial se hacen los Acuerdos de Bretton Woods, donde se decidió adoptar el dólar estadounidense como divisa internacional, bajo la condición de que la Reserva Federal (el banco central de ese país) sostuviera el patrón oro.

Los acuerdos de Bretton Woods son todas las resoluciones de la conferencia monetaria y financiera de las Naciones Unidas, realizada en la localidad de Bretton Woods (Nueva Hampshire, Estados Unidos), entre el 1 y el 22 de julio de 1944, que estableció las políticas económicas mundiales que estuvieron vigentes hasta principios de la década de 1970.

En los acuerdos, también se decidió la creación del Banco Mundial y del Fondo Monetario Internacional, usando el dólar estadounidense como moneda de referencia internacional. Ambas organizaciones empezaron a funcionar en 1946.

El dólar se convierte en dinero Fiat

El dinero fíat es el que se basa en la fé o confianza de la comunidad, es decir, que no se respalda por metales preciosos ni nada que no sea una promesa de pago por parte de la entidad emisora

Fue a partir de 1971 el presidente Nixon ordenó el 15 de agosto cerrar la ventanilla de cambios de oro por dólares y terminó así con el régimen de libre convertibilidad del dólar y el oro, cambiando la historia financiera profundamente de ahí en adelante por lo que el dólar se convirtió en una moneda fíat respaldada por una imposición gubernamental estadounidense y sin valor intrínseco, pero con un valor legal propio. Esto a consecuencia de que la economía estadounidense tenía por primera vez en lo que iba del siglo XX un déficit en la balanza comercial. Para corregir tal déficit y la baja del valor del dólar se necesitaría abandonar los Acuerdos de Breton Woods, convirtiendo de esa forma al dólar estadounidense en una moneda fíat, en un momento en que gozaba de una presencia en las finanzas globales a razón de las guerras solo habían destruido otro países de Europa. Otro factor importante para este cambio fue que la guerra de Vietnam, tanto en el plano económico como militar, drenaba las reservas estadounidenses.

El movimiento Cypherpunk

El movimiento Cypherpunk entiende la privacidad como el legítimo derecho que tiene de cada ciudadano del mundo de revelar sólo la información que desea, como queda expresado en el Manifiesto Cypherpunk de Eric Hughes: La privacidad es el poder de revelarse selectivamente al mundo.

Este movimiento más filosófico que tecnológico, ante la amenaza que suponía el control y la censura ejercida por los gobiernos y las autoridades centrales sobre el desarrollo de la información, de la tecnología y el intercambio de valor, llevó a sus miembros a defender la bandera de la privacidad. Para este movimiento el Cypherpunk es una persona que defiende la libertad de expresión, la libertad de información y la privacidad de las comunicaciones.

Los motivos de los Cypherpunk es encontrar en la tecnología criptográfica el medio para alcanzar sus objetivos en el mundo digital. En 1992 el ingeniero estadounidense Tim May recoge estas ideas en detalle en su obra:: Los cypherpunk estamos dedicados a construir sistemas anónimos. Defendemos nuestra privacidad con criptografía, con sistemas de reenvío de correo anónimo, con firmas digitales y con dinero electrónico. Los cypherpunks escribimos código. Sabemos que alguien tiene que escribir software para defender la privacidad y no podemos obtener privacidad a menos que todos lo hagamos.

En 2008 se inicia la historia de Bitcoin cuando Satoshi Nakamoto publicó por primera vez su libro blanco de la red bitcoin y lo envía a un pequeño grupo de defensores de la privacidad y especialistas en ciencias informáticas y criptográficas. Ese grupo estaba formado por los remitentes del movimiento cypherpunk.

Algunos de los participantes de esta lista mantuvieron el anonimato. Sin embargo, otros son públicamente conocidos, activos en la creación de herramientas de software para la mejora de la privacidad. Entre ellos encontramos a Julian Assange fundador de Wikileaks; Bram Cohen, creador de Bittorrent, Jacob Appelbaum, desarrollador de Tor; Phillip Zimmermann, creador de Pretty Good Privacy, Zooko Wilcox desarrollador de Digital Cash y

El movimiento Cypherpunk

fundador Zcash , Adam Back inventor de Hashcash, Hal Finney creador de la prueba de trabajo reutilizable, Wei Dai creador de B-money y Nick Szabo creador de Bit gold y padre del concepto de los contratos inteligentes.

Las ideas y el grupo ya había estado gestándose desde los años ochenta, especialmente impulsados por el trabajo de David Chaum, uno de los primeros especialistas en preocuparse por la privacidad de las transferencias financieras. Chaum está acreditado como el inventor del dinero digital seguro por sus trabajos de investigación. Estas ideas han sido descritas como las raíces técnicas de la visión del movimiento cypherpunk, que comenzó a finales de 1980, extiende estas ideas para habilitar la detección del doblegasto en 1988.

Bitcoin podría considerarse como un producto cypherpunk, no solo como en síntesis de varios proyectos inspirados en este movimiento, sino también en la realización de varios ideales y principios de libertad y privacidad.

Historia del Internet

Los inicios de Internet nos remontan a los años 60. En plena guerra fría, Estados Unidos crea una red exclusivamente militar, con el objetivo de que, en el hipotético caso de un ataque ruso, se pudiera tener acceso a la información militar desde cualquier punto del país. Esta red se creó en 1969 y se llamó ARPANET. En principio, la red contaba con 4 ordenadores distribuidos entre distintas universidades del país, Dos años después, ya contaba con unos 40 ordenadores conectados. Se crearon el Protocolo TCP/IP, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas (actualmente seguimos utilizando dicho protocolo). ARPANET siguió creciendo y abriéndose al mundo, y cualquier persona con fines académicos o de investigación podía tener acceso a la red.

Historia del Internet

Las funciones militares se desligaron de ARPANET y fueron a parar a MILNET, una nueva red creada por los Estados Unidos. La NSF (National Science Fundation) crea su propia red informática llamada NSFNET, que más tarde absorbe a ARPANET, creando así un gran red con propósitos científicos y académicos. El desarrollo de las redes fue abismal, y se crean nuevas redes de libre acceso, formando el embrión de lo que hoy conocemos como INTERNET.

En 1985 Internet ya era una tecnología establecida, aunque conocida por unos pocos. En el Centro Europeo de Investigaciones Nucleares (CERN), Tim Berners Lee dirigía la búsqueda de un sistema de almacenamiento y recuperación de datos. Berners Lee retomó la idea de usar hipervínculos. Robert Caillau quien cooperó con el proyecto, cuenta que en 1990 deciden ponerle un nombre al sistema y lo llamaron World Wide Web
(WWW) o telaraña mundial.

Orden Cronológico de la Historia del Internet

AÑO	EVENTO
1958	La compañía BELL crea el primer módem que permitía transmitir datos binarios sobre una línea telefónica simple.
1962	Inicio de investigaciones por parte de ARPA, una agencia del ministerio estadounidense de defensa, donde J. C. R. Licklider defiende exitosamente sus ideas relativas a una red global de computadoras.
1967	Primera conferencia sobre ARPANET
1969	Conexión de las primeras computadoras entre 4 universidades estadounidenses a través de la *Interface Message Processor* de Leonard Kleinrock
1969	El internet se abre al público.
1971	23 computadoras son conectadas a ARPANET. Envío del primer correo electrónico por Ray Tomlinson.
1972	Nacimiento del InterNetworking Working Group, organización encargada de administrar Internet.
1973	Reino Unido y Noruega se adhieren a Internet, cada uno con una computadora.
1979	Creación de los NewsGroups (foros de discusión) por estudiantes estadounidenses.
1981	Definición del protocolo TCP/IP y de la palabra «Internet»
1983	Primer servidor de nombres de sitios.
1984	1000 computadoras conectadas.
1987	10000 computadoras conectadas.
1989	100000 computadoras conectadas.
1990	Desaparición de ARPANET. Se crea el primer navegador web.
1991	Se anuncia públicamente la World Wide Web
1992	1 millón de computadoras conectadas.
1993	Aparición del navegador web NCSA Mosaic[4]
	Primer buscador de la historia, Wandex servía como un índice de páginas web.4
1994	Nace la web invisible, la primera versión de la deep web.
1996	10 millones de computadoras conectadas
1998	Nace Google.
2001	Explosión de la Burbuja.com. Nace la Wikipedia.
2004	Nace Facebook.
2005	Internet alcanza 1000 millones de usuarios.
2007	La aparición del iPhone populariza la web móvil.
2009	Comienzos de la mensajería instantánea en teléfonos móviles. Nace WhatsApp.

Evolución de la Web

Desde 1991 se permite tener interconexiones, cualquier persona podía tener una plataforma hacia el mundo, esto revolucionó la forma de comunicarnos, integrar la información y de aumentar el comercio en largas distancias
Todo inicia con la integración de datos desde que se usaba el internet en 1980 para compartir documentos en dos máquinas conectadas, a esto se le llama como intercambio electrónico.

En 1990 el desarrollo de la Web permite compartir funcionalidades además de los datos, lo que permite interoperabilidad de usuarios y ejecutar procedimientos en línea a través de una interfaz de aplicaciones.

Para el nuevo milenio en los 2000 aparece un nuevo nivel de funcionalidades y estandarización en la web, La Integración de Servicios que brinda más interacción con empresas y consumidores, se ejecutan muchos servicios en la red y nace la nueva era de los servicios Web, los protocolos HTTP y XML.

Desde el 2010 se desarrolla la evolución de los micro servicios, estos micro servicios han mejorado la arquitectura a través de técnicas de encapsulación y la capacidad de iterar rápidamente.

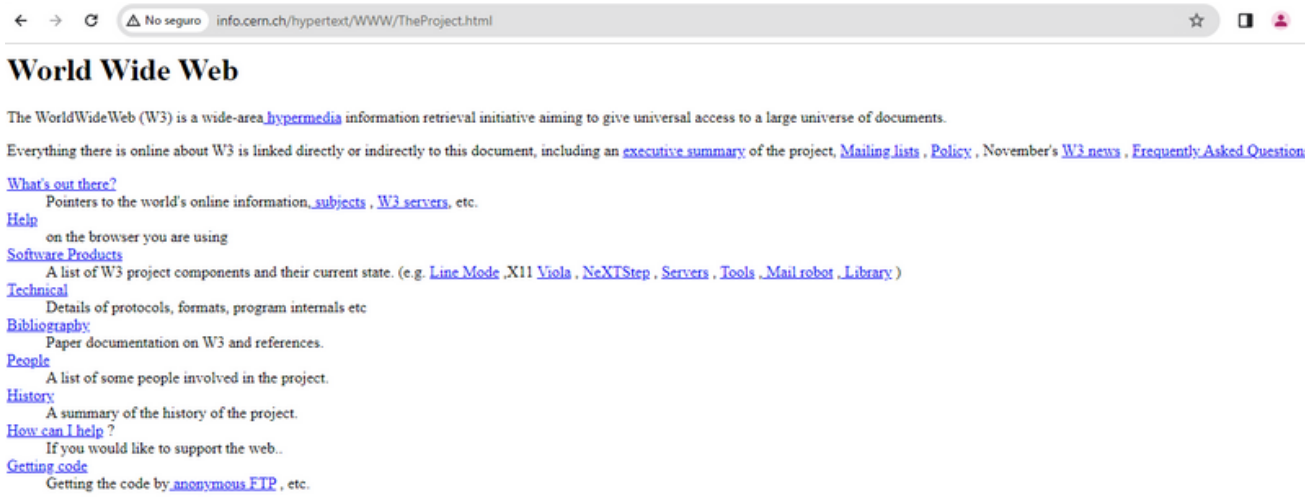
Para el 2020 la integración de blockchain, brinda el potencial de expandir el nivel de incluir datos y los procesos empresariales, lo que brinda gran agilidad para que las corporaciones realicen su integración.

Las cualidades que tiene la tecnología Blockchain como criptografía, inmutabilidad, trazabilidad implicarán más el desarrollo y el avance a través de los próximos años para la humanidad.

Evolución de la Web

WEB 1.0 (Solo Lectura)

En 1989, en el CERN de Ginebra, Tim Berners-Lee estaba ocupado desarrollando los protocolos que se convertirían en la World Wide Web. El primer Sitio web de la Humanidad: http://info.cern.ch/hypertext/WWW/TheProject.html



Internet alcanzó la adopción masiva a finales de los 90 y principios de los 2000, se utilizó predominantemente como una forma de obtener información a través del texto. La idea fue crear protocolos abiertos y descentralizados que permitieran compartir información desde cualquier lugar de la Tierra.

La Web 1.0 consistía principalmente en sitios web estáticos propiedad de empresas, y había una interacción casi nula entre los usuarios (los individuos rara vez producían contenido), lo que a que se conozca como la web de solo lectura.

Evolución de la Web

WEB 2.0 Lectura y escritura

El período Web 2.0 comenzó en 2004 con la aparición de las plataformas de redes sociales. En lugar de solo lectura, la web evolucionó para ser de lectura y escritura. En lugar de que las empresas proporcionen contenido a los usuarios, también comenzaron a proporcionar plataformas para compartir contenido generado por el usuario y participar en interacciones de usuario a usuario. A medida que más personas se conectaron a Internet, un puñado de las principales empresas comenzó a controlar una cantidad desproporcionada del tráfico y el valor generado en la web. La Web 2.0 también dio origen al modelo de ingresos impulsado por la publicidad. Si bien los usuarios podían crear contenido, no lo poseían ni se beneficiaban de su monetización.

Evolución de la Web

WEB 3.0 Lectura, escritura y propiedad.

La premisa de 'Web 3.0' fue acuñada por el cofundador de Ethereum, Gavin Wood, poco después del lanzamiento de Ethereum en 2014. Gavin puso en palabras una solución para un problema que sintieron muchos de los primeros en adoptar criptomonedas: la Web requería demasiada confianza. Es decir, la mayor parte de la Web que la gente conoce y usa hoy en día se basa en confiar en un puñado de empresas privadas para actuar en el mejor interés del público.

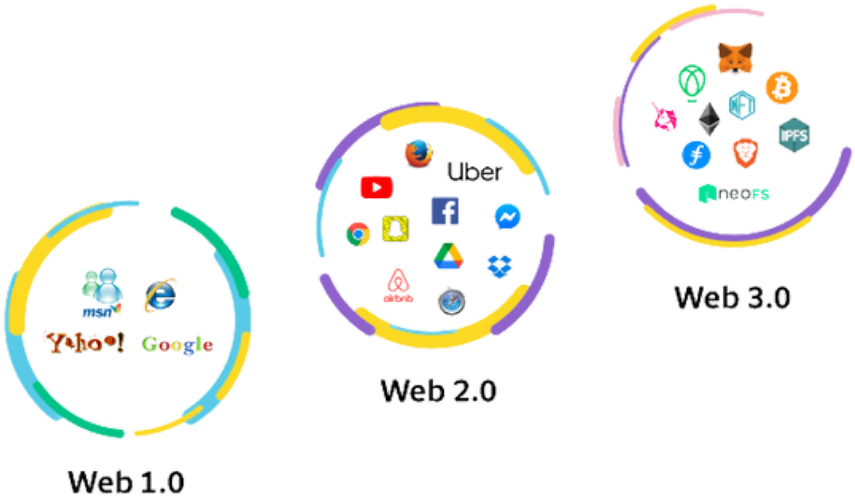
La centralización ha ayudado a miles de millones de personas a incorporarse a la World Wide Web y ha creado la infraestructura sólida y estable en la que se vive. Al mismo tiempo, muchas entidades centralizadas tienen control del contenido del usuario decidiendo qué debe y que no debe permitirse.

Evolución de la Web

Aquí es donde entra en juego la tecnología blockchain. La cadena de bloques es básicamente un gran registro público digital. Las cadenas de bloques se distribuyen en muchos nodos (las computadoras de las personas), razón por la cual escuchará que se las describe como "descentralizadas". Entonces, en lugar de un servidor central propiedad de la empresa, la cadena de bloques se distribuye a través de una red de igual a igual. Esto asegura que la cadena de bloques permanezca inmutable. Y debido a que la cadena de bloques registra y preserva la historia y actúa como una parte imparcial, las transacciones en ella pueden ser "sin confianza" en el sentido de que no requieren que confíes en alguien para realizar la transacción. Del mismo modo, debido a que las transacciones son realizadas por una red de computadoras, son "sin permiso" en el sentido de que no requieren el permiso de un tercero.

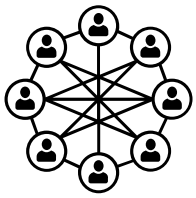
Web3 es la respuesta a este dilema. En lugar de una web monopolizada por grandes empresas de tecnología, Web3 adopta la descentralización y está siendo construida, operada y propiedad de sus usuarios. Web3 pone el poder en manos de individuos en lugar de corporaciones.

Web3 se ha convertido en un término general para la visión de una Internet nueva y mejor. En esencia, utilizar cadenas de bloques, criptomonedas y NFT es devolver el poder a los usuarios en forma de propiedad.



Principios de la Web3

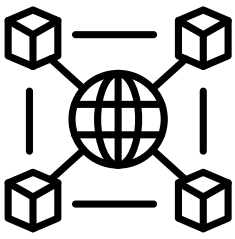
-**Descentralizado:** en lugar de grandes corporaciones de Internet y entidades centralizadas, la propiedad se distribuye entre sus creadores y usuarios.



-**Libertad**: Todos los usuarios tienen el mismo acceso para participar en Web3 y nadie queda excluido.

-Pagos nativos: Utiliza criptomonedas para gastar y enviar dinero en línea en lugar de depender de la infraestructura obsoleta de los bancos y los procesadores de pagos.

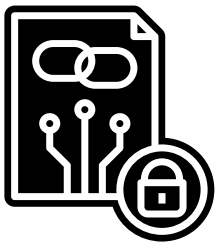
-Interoperabilidad: Los sistemas y aplicaciones en la Web 3.0 están diseñados para ser compatibles y trabajar de manera conjunta de forma más fluida, permitiendo la transferencia de datos y activos entre diferentes plataformas de manera eficiente.



Principios de la Web3

-Privacidad y Control de Datos: Se prioriza la privacidad del usuario y se le otorga mayor control sobre sus propios datos. La idea es que los usuarios decidan qué información compartir y con quién.

-Contratos Inteligentes: Los contratos inteligentes son programas autoejecutables que facilitan, verifican o hacen cumplir la negociación o ejecución de acuerdos sin necesidad de intermediarios.



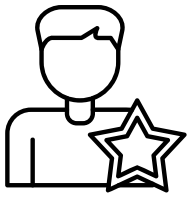
-Tokenización: Se refiere a la representación digital de activos, como monedas, bienes raíces o incluso tiempo, a través de tokens en blockchain. Esto facilita la transferencia y el intercambio de activos de manera eficiente y segura.

-Identidad Digital Descentralizada (DID): La Web 3.0 promueve la creación de identidades digitales descentralizadas, lo que significa que los usuarios tienen el control total sobre su información de identidad y pueden compartir selectivamente esa información según sea necesario.

Principios de la Web3

-Web Semántica: La Web Semántica es una parte integral de la Web 3.0, que se enfoca en mejorar la comprensión y el significado de la información en la web. Facilita la búsqueda y la interconexión de datos de manera más inteligente.

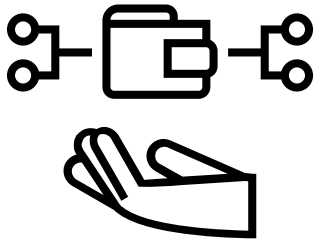
-Incentivos para la Participación: Se buscan modelos económicos que recompensen a los usuarios por participar activamente en la red, ya sea a través de la creación de contenido, la validación de transacciones o la contribución a la gobernanza.



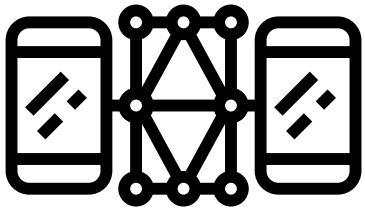
-DAO: Organizaciones autónomas descentralizadas y sin liderazgo único. En su lugar, se rigen por el grupo de usuarios que componen la organización. A menudo, los usuarios dentro de una DAO crearán propuestas que se votan para promulgar cambios. Los DAO tienen sus propios tokens que permiten a los usuarios demostrar su membresía y votar. Los DAO pueden tener una amplia gama de propósitos, desde donaciones caritativas
hasta redes comerciales y educación.

Principios de la Web3

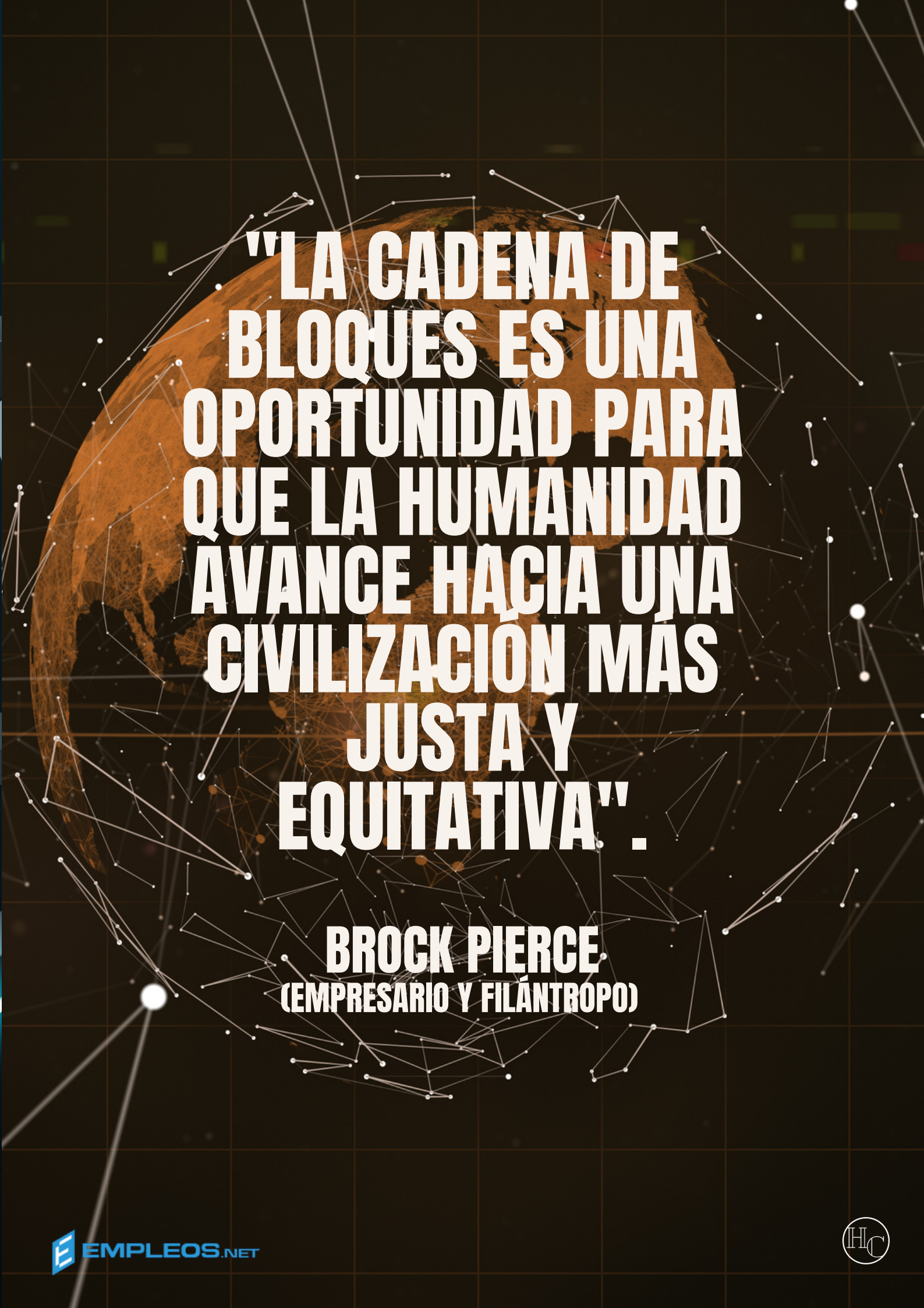
-Finanzas descentralizadas (DeFi): A menudo abreviado simplemente como "DeFi", es el término utilizado para describir todos los servicios financieros que operan con tecnología blockchain. DeFi permite transacciones rápidas, sin permiso y sin confianza.



-dApps: Es una forma abreviada de "aplicaciones descentralizadas". A diferencia de las aplicaciones utilizadas por la web 2.0 que son propiedad de una sola entidad, las dApps utilizan tecnología blockchain, aunque no necesariamente necesitan estar descentralizadas. Las dApps se pueden operar a través de una red peer-to-peer en la cadena de bloques, o pueden operar usando estructuras jerárquicas tradicionales, pero lo que las convierte en dApps es su utilización de protocolos descentralizados.



-Metaverso: El metaverso se refiere a una realidad virtual y aumentada en la que los usuarios pueden interactuar con el espacio digital


"LA CADENA DE BLOQUES ES UNA OPORTUNIDAD PARA QUE LA HUMANIDAD AVANCE HACIA UNA CIVILIZACIÓN MÁS JUSTA Y EQUITATIVA".
BROCK PIERCE
(EMPRESARIO Y FILÁNTROPO)
EMPLEOS.NET

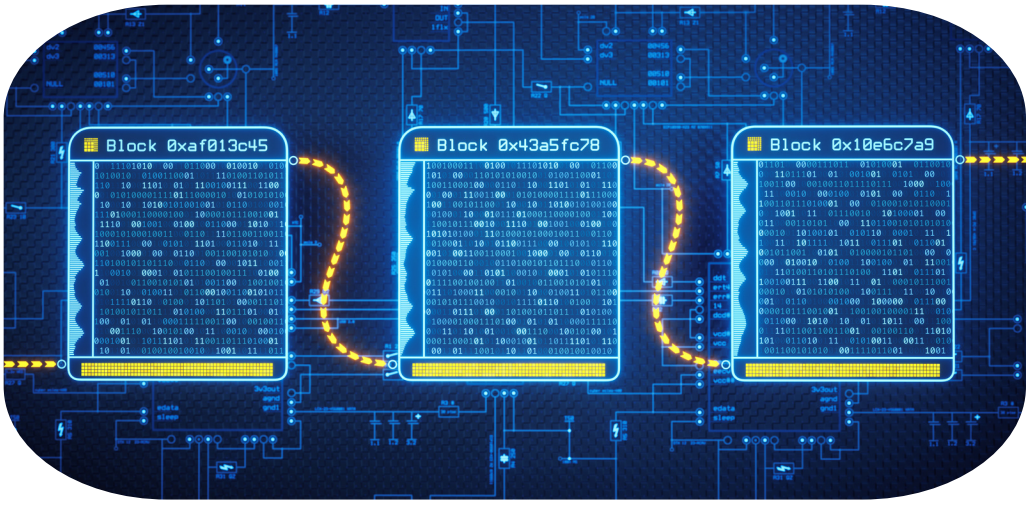
CAPÍTULO 2: CADENAS DE BLOQUES

Cadenas de bloques

Para los desarrolladores la tecnología blockchain es un conjunto de protocolos y tecnologías de cifrado para almacenar datos en una red distribuida para empresas y finanza, para los tecnológicos el blockchain es la fuerza impulsadora detrás de la próxima generación de internet y para otras personas el blockchain es una herramienta para remodelar radicalmente la sociedad y la economía ya que nos dirigimos a un mundo descentralizado.

La blockchain (cadena de bloques) es un tipo de red distribuida que permite desarrollar tecnologías como las criptomonedas, NFT y lo que llamamos Internet del Valor. Es una tecnología que permite crear un libro de contabilidad distribuido en una red de sin necesidad de contar con un servidor o base de datos central. La actualización y manejo de este libro de contabilidad, solo se puede realizar en consenso con todas las partes que forman la red.

Por esta razón, el poder de cómputo de todos los nodos de la red se usa no solo para introducir información, sino también para protegerla frente a modificaciones no autorizadas. Consecuencia de esto, la blockchain permite alcanzar niveles de seguridad muy altos en comparación con otras tecnologías.



CADENAS DE BLOQUES

Para que la tecnología blockchain funcione es necesario en primer lugar crear un software específico para la misma. Este software permite a los ordenadores crear la red que hará funcionar la blockchain de forma distribuida. Tal cual como sucede en el caso del software de Bitcoin y otras criptomonedas generalmente este software es de carácter abierto, esto implica que son públicos, transparentes y pueden ser usados, revisados y contribuidos por cualquier persona.

Al no tener base de datos ni servidor localizado, a una red de tipo blockchain se le atribuye la característica de ser una red distribuida. Esto significa que la información está replicada en todos los ordenadores del mundo que estén conectados a la misma blockchain. En el caso de que más del 50% de los ordenadores que forman esa red blockchain no sean de la misma persona o empresa, podemos decir que la red está descentralizada. Con esto podemos decir que, no tiene un “centro de emisión, control o poder”.

En esencia una red blockchain es solo una base de datos que permite leer y escribir nuevos registros. Todo ello sin poder modificar nada de lo que existe en ella. Todos los registros que se guardan en ella están vinculados entre sí con una matemática muy avanzada. haciendo imposible incluir algo que no sea coherente con el resto de registros incluidoss.

CADENAS DE BLOQUES

Implicaciones de la tecnología blockchain

La mayor implicación de la tecnología es que por primera vez en la historia de la humanidad, la gente en cualquier lugar puede confiar entre si y realizar transacciones persona a persona, sin necesidad de la gestión centralizada de instituciones, sino mediante la criptografía y códigos informáticos. Además refuerza enormemente nuestra capacidad de colaboración y cooperación entre organizaciones e individuos dentro de redes de pares que nos permiten potencialmente formar redes globales descentralizadas.

Importancia de la tecnología blockchain

Las empresas operan con base en la información. Cuanto más rápido la obtienen y más exacta es mejor. Blockchain es ideal para obtener esa información, puesto que proporciona datos inmediatos, compartidos y completamente transparentes almacenados en un libro mayor distribuido inalterable al que únicamente los miembros autorizados tienen acceso. Una red de blockchain puede hacer seguimiento de pedidos, pagos, cuentas, detalles de producción y mucho más. Adicionalmente se puede ver todos los detalles de una transacción de principio a fin, lo que le permite generar mayor confianza y eficiencia.

Beneficios de Blockchain

Normalmente las operaciones invierten mucho esfuerzo en el mantenimiento de registros duplicados y en la validación de partes externas. Los sistemas de mantenimiento de registros pueden ser vulnerables a fraudes y ciberataques. Una transparencia limitada puede ralentizar la verificación de datos. Además, con la llegada del Internet de las cosas, la cantidad de transacciones ha crecido exponencialmente. Todo esto ralentiza el negocio, perjudica los resultados y significa que necesitamos mejorar la manera de hacer las cosas. Blockchain puede ayudar a lograrlo**.**

CADENAS DE BLOQUES

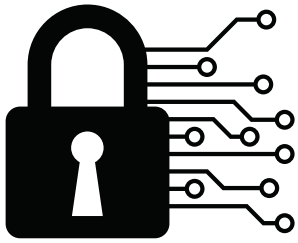
Beneficios de Blockchain

Mayor confianza

Con blockchain no confiamos en un banco, una empresa o gobierno. Prácticamente cuando usamos una blockchain la confianza está en el protocolo informático creado y mejorado por el pasar del tiempo por desarrolladores, programadores, matemáticos e ingenieros de la computación del mundo, siempre ha sido de código abierto para humanidad.

Mayor seguridad

Todos los miembros de la red deben llegar a un consenso acerca de la precisión de los datos y todas las transacciones validadas son inalterables ya que se registran de forma permanente. Nadie, ni siquiera un administrador del sistema, puede suprimir una transacción.



Más eficiencia

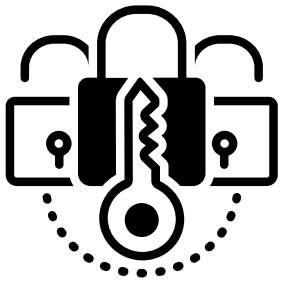
Con un libro mayor distribuido compartido entre los miembros de una red, se elimina el tiempo perdido en las acciones de conciliación de registros. Y para acelerar las transacciones, un conjunto de reglas, llamado contrato inteligente, se almacena en la cadena de bloques y se ejecuta automáticamente.

CADENAS DE BLOQUES

Características de la tecnología blockchain

Inmutabilidad

La incapacidad de realizar cambios en el historial es quizás la característica de seguridad más valorada de esta tecnología y es posible gracias al uso en conjunto de la descentralización y la criptografía.

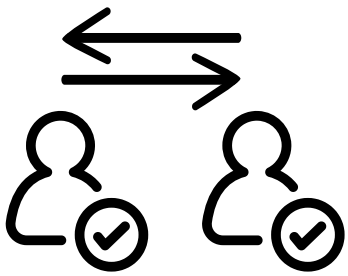


Criptografía

De la criptografía depende la integridad, la verificación de datos y la privacidad de esta tecnología, es usada para identificar de forma única e irrepetible cada transacción y bloque dentro de la blockchain.

Comunicación descentralizada de persona a persona

Permite que cualquiera pueda usar la red desde cualquier lugar del mundo, permite que cualquiera que forme parte de la misma, realizando las tareas necesarias para su funcionamiento. Así sin importante si uno o dos o cientos de nodos se caen, la red blockchain seguirá en funcionamiento.

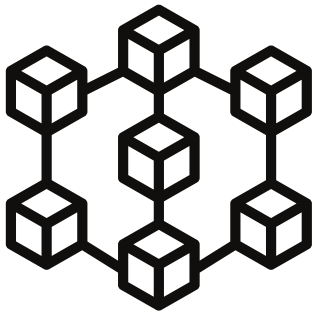


CADENAS DE BLOQUES

Elementos clave de la blockchain

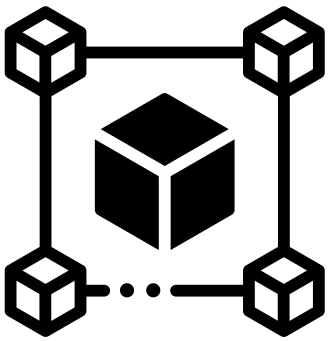
Tecnología de libro mayor distribuido

Todos los participantes de la red tienen acceso al libro mayor distribuido y a su registro inmutable de transacciones. Con este libro mayor compartido, las transacciones se registran sólo una vez, eliminando la duplicación del esfuerzo que es típico de las redes de negocios tradicionales.



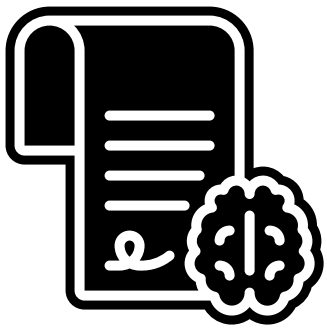
Registros inalterables

Ningún participante puede cambiar o alterar una transacción después de que se haya grabado en el libro mayor compartido. Si un registro de transacción incluye un error, se debe añadir una nueva transacción para revertir el error, pero ambas transacciones serán visibles.



Contratos inteligentes

Para acelerar las transacciones, un conjunto de reglas, llamado contrato inteligente, se almacena en la cadena de bloques y se ejecuta automáticamente. Un contrato inteligente puede definir las condiciones para las transferencias de garantía corporativas, incluyendo los términos de seguro de viaje que se pagará y mucho más.



Tipos de Redes Blockchain

Redes públicas blockchain

Las blockchain públicas permiten que cualquier persona pueda formar parte de la misma. Bien sea como usuario, minero o administrador de un nodo, las personas pueden acceder a la red y formar parte de ella sin restricción alguna.

Redes privadas blockchain

Una red de blockchain privada, similar a una red de blockchain pública, es una red descentralizada entre pares peer-to-peer. Sin embargo, una sola organización administra la red y controla quién tiene permiso para participar, decide cuándo ejecutar un protocolo de consenso y se encarga del mantenimiento del libro mayor compartido.

Blockchain de consorcios

Varias organizaciones pueden compartir las responsabilidades de mantener un blockchain. Estas organizaciones preseleccionadas determinan quién puede enviar transacciones o acceder a los datos. Un blockchain de consorcio es ideal para los negocios cuando todos los participantes deben estar autorizados y tienen una responsabilidad compartida para blockchain.

Redes de blockchain autorizadas

Las empresas que establecen una red privada de blockchain generalmente lo harán en una red de blockchain autorizada. Es importante señalar que las redes públicas de blockchain también pueden ser autorizadas. Esto impone restricciones en cuanto a quién puede participar en la red y en qué transacciones. Los participantes necesitarán una invitación o permiso para unirse.

Usos de la tecnología Blockchain

Gestión de la cadena de suministros

Cada activo puede ser monitoreado y rastreado a través de la cadena de suministro. Además, la información se puede rastrear y volver a verificar cuando sea necesario. Una gestión descentralizada de la cadena de suministro basada en blockchain puede registrar fácilmente información como la hora, la ubicación, el estado del producto. Se puede utilizar en cadenas de suministros alimenticios, farmacéuticos y muchos activos más.

Ejemplos de Gestión de la cadena de suministro en proyectos Blockchain

Food Trust por IBM y WalmartBext360 Usando blockchain para asignar trazabilidad a sus granos de café.

Identidad digital

El robo de identidad es uno de los problemas del siglo XXI que han llegado a Internet. Adema llevar una gran cantidad de documentos como licencia de conducir, pasaporte, documento nacional de identidad o cualquier otro documento de identidad asociado con las organizaciones para las que están trabajando. La solución es tener una identidad digital asociada con una persona. Se puede lograr con la ayuda de blockchain donde una persona solo tiene una identidad en toda la red.

Usos de la tecnología Blockchain

Junto con la identidad digital, los gobiernos pueden desplegar la votación en un entorno descentralizado

Ejemplos de Proyectos de blockchain de identidad digital:

Hyperledger Indy – Cubre identidad descentralizada
Civic – Sistema de identificación autónomo

Tokenización de Activos

Es el paso crucial hacia la protección de los activos del mundo real. Para hacer que el manejo de activos sea más eficiente y práctico, se realiza la tokenización de activos. Le permite acelerar el proceso de venta y compra de activos. Se puede utilizar principalmente en activos reales y en finanzas. Ayuda a que se negocien y se establezcan en la blockchain. Ignora por completo la forma estándar de resolver activos, mejorar la eficiencia y ahorrar tiempo, lo que lo convierte en uno de los mejores usos de blockchain.

Proyectos de blockchain de tokenización de activos
Polymath, Harbor, Alphapoint

Usos de la tecnología Blockchain

Mercado de la Energía

El mercado energético está completamente controlado por grandes compañías. Es un mercado cerrado controlado por la corporación que no deja nada para la población en general. Con blockchain, es más fácil para las personas generar, comerciar, registrar y liquidar energía, todo con la ayuda de contratos inteligentes y tecnología de registro distribuida. Con el uso de la tecnología blockchain, la energía se convierte en un activo, al igual que otros productos básicos. El mercado de la energía puede revolucionarse si hay un mercado de electricidad distribuida donde los consumidores también pueden actuar como productores, y viceversa.

Proyectos de blockchain del mercado energético

- Grid+
- Power Ledger

Usos de la tecnología Blockchain

Cuidado de Salud

El sector sanitario adolece de un enfoque centralizado, que conduce a una forma ineficiente de tratar a los pacientes. Los datos almacenados se siguen principalmente en diferentes estándares y formatos, lo que genera problemas cuando se trata de la recuperación y el almacenamiento de datos de los pacientes. Blockchain puede simplificar todos los problemas de salud al proporcionar un enfoque de registro descentralizado. Así se pueden acceder a los datos vitales del paciente con el permiso adecuado. Todos los datos también permanecerán seguros y solo el personal autorizado podrá acceder a ellos.

Proyectos de blockchain de atención médica

SimplyVital HealthMediBloc – mejora de los proveedores de servicios de salud
Dentacoin – tiene como objetivo mejorar la atención médica dental
AIDoctor – uso de IA en aplicaciones de salud

Usos de la tecnología Blockchain

Bienes Raíces

El mercado inmobiliario sufre de muchos problemas, cuando se trata de conectar vendedores y compradores. Los compradores tienen que reunirse con corredores o vendedores para facilitar un trato. Esto puede llevar desde unos pocos meses hasta un año.

La solución descentralizada blockchain puede ayudar a los inquilinos, propietarios, proveedores de servicios y cualquier otra entidad a interactuar y verificar la información de propiedad o incluso realizar transacciones de forma segura. El sector inmobiliario puede convertirse en una plataforma global donde el pago descentralizado será la norma. Mejora el proceso y ahorra costos. Una blockchain puede ocuparse de los diferentes aspectos de una transacción.

Proyectos de blockchain inmobiliario

Propy – permite la compra a través de blockchain
StreetWire – Mejore la adopción de tecnología en el mercado inmobiliarioHarbor – Ayuda a liquidar activos

Usos de la tecnología Blockchain

Notariado

El sistema heredado depende en gran medida del papeleo, los registros se mantienen en forma impresa, que son susceptibles a cambios y manipulación por parte de un tercero o partes maliciosas internas.

Blockchain eliminará la necesidad de confianza del proceso. Actualmente, la confianza juega un papel crucial en el proceso. Se debe a las características de blockchain, como la transparencia y la inmutabilidad. También proporciona prueba de existencia, que es esencial para el proceso notarial.

Por ejemplo, la existencia del documento desde el principio se puede probar con la ayuda de blockchain, ya que puede almacenar el momento en que se creó. La verificación es 100% precisa, teniendo en cuenta que los datos una vez escritos dentro de la blockchain no pueden modificarse de ninguna manera posible.

Proyectos de notariado en Blockchain

SilentNotary
Stampad.io
Acronis Notary

Usos de la tecnología Blockchain

Seguridad Alimenticia

La falta de transparencia ha generado problemas en los que no es posible rastrear los alimentos contaminados. La falta de transparencia se debe al uso de un enfoque basado en papel. No es posible rastrear alimentos, y es sencillo para cualquiera modificar los documentos con datos inexactos.

Además, todo el proceso de seguimiento de los alimentos es costoso.

Con blockchain cada alimento que se coloca en la cadena de suministro ahora se puede etiquetar adecuadamente con información vital como la temperatura de almacenamiento, la fecha de procesamiento, la fecha de vencimiento, la fábrica, el número de lote, etc. Además, los alimentos se pueden rastrear a lo largo de la cadena de suministro, asegurando que se puedan sacar los alimentos malos cuando sea necesario. Esto significa que los alimentos destinados al usuario final pueden alcanzar la mejor calidad posible.

Proyectos de blockchain de seguridad alimentaria

IBM Food Trust

Blockchain Food Safety Alliance Platform

Usos de la tecnología Blockchain

Música

La industria musical actual no es justa para todos los artistas. Se necesita mucho esfuerzo para hacerse notar en el mercado competitivo. Además de eso, está el intermediario que toma su propio corte, lo que significa menos ganancias para los propios creadores de música. Los problemas más críticos incluyen la piratería, donde los creadores de música no tienen control sobre ella. Blockchain puede ayudar a otorgar al creador de la música los derechos adecuados y también abordar la piratería en cierta medida. Automatizar toda la compra, venta y protección de la propiedad intelectual en una blockchain.

Proyectos de blockchain de música
Musicoin – plataforma de pago por juego
Mycelia – centro de desarrollo e investigación para músicos
Mediacoin - un lugar para publicar videos y música

Video juegos

Uno de los casos de uso únicos de blockchain para los videojuegos son los cripto coleccionables que han mostrado un crecimiento prometedor después de su creación. Aquí, los jugadores se sienten atraídos por los activos intangibles recogidos. Algunos de ellos mantienen su colección mientras que otros venden sus tenencias con un margen de beneficio. Blockchain también puede ayudar a los desarrolladores a crear nuevas funcionalidades para sus juegos.

Usos de la tecnología Blockchain

En este momento, blockchain es una excelente opción para los eSports, ya que proporciona una plataforma transparente, capaz de hacer redes seguras y rápidas. Para los jugadores en línea, las transferencias realizadas para comprar espadas especiales, armas u otros complementos para jugar su aventura son inversiones únicas e intransferibles. Eso es algo que las empresas quieren cambiar registrando esas compras usando blockchain. La tecnología blockchain está cambiando la industria gaming, puesto que permite la comunicación abierta entre jugadores y desarrolladores. Esto es posible porque los desarrollos en aplicaciones blockchain están impulsados por un consenso de la comunidad, Proporciona un entorno seguro para los desarrolladores y emprendedores de videojuegos, Ayuda a comprar y vender seguramente activos en los juegos, Blockchain en gaming permite la utilización de perfiles interoperables de jugadores, Se pueden almacenar de forma segura los activos del juego, Los gamers son los dueños verdaderos de sus activos en el juego, Evita fraudes., Es una tecnología abierta a la colaboración entre desarrolladores y jugadores para mejorar el juego.

Proyectos de blockchain para la industria de videojuegos
EnjinXAYA plataforma de juegos blockchain
Axion Zen- desarrolladores de CryptoKitties


"BLOCKCHAIN NO ES SOLO UNA TECNOLOGÍA, SINO UNA ARQUITECTURA DE CONFIANZA".
DON TAPSCOTT
(COAUTOR DE "BLOCKCHAIN REVOLUTION")
EMPLEOS.NET

CAPÍTULO 3: COMPONENTES DE LA BLOCKCHAIN

Componentes de la Blockchain

Las redes blockchain para su funcionamiento constan de varios componentes

-Redes Descentralizadas: Los Nodos son distribuidos por todas partes del mundo.

-Libro Contable: Registros de transacciones inmutables.

-Criptografía: Hashes, firmas digitales y criptografía asimétrica.

-Protocolo de Consenso: Incentiva a la red para el mantenimiento.

Redes Descentralizadas

Es una Red donde no existe un único nodo central, todos los nodos son iguales y con mismas características. En estas redes los nodos se conectan entre sí sin la necesidad de conectarse por uno o varios nodos centrales Los miembros de esta red no tienen que confiar ni conocerse entre sí, sino que cada integrante obtiene una copia del mismo registro de contabilidad del blockchain.

Nodo

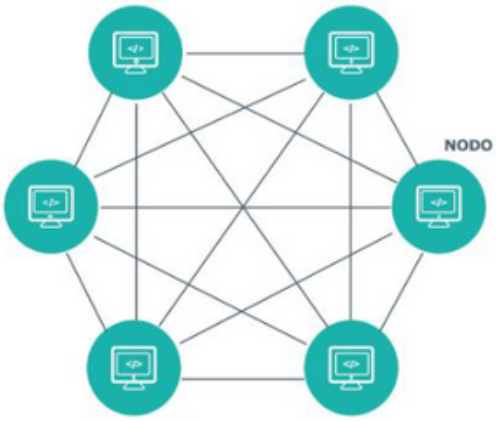
Un nodo es una copia de la información del Blockchain alojada en una computadora. Cuando se genera un registro nuevo por medio de un minero, se envía una copia a cada uno de los nodos de la red blockchain de ahí todos los nodos poseen copias sincronizadas de la cadena de bloques.

Con un solo nodo no se le puede llamar red. Para ello es necesario que más y más nodo se unan. Desde ese momento comienzan a sincronizar entre ellos e inician un proceso de operación y funcionamiento.

COMPONENTES DE LA BLOCKCHAIN

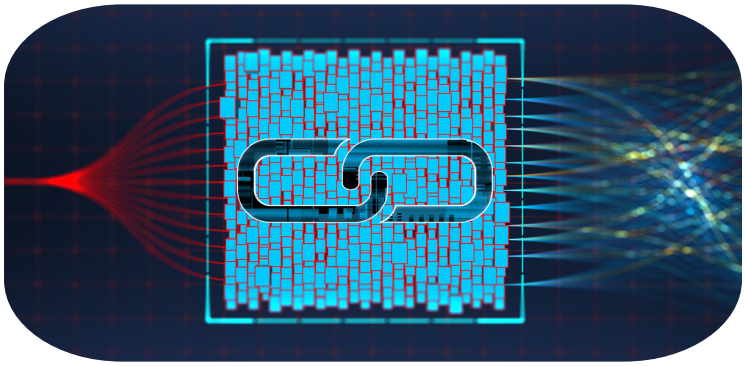
El proceso se sigue repitiendo con cada nuevo nodo agregado a la red, intercambiando información para que todos funcionen de forma coordinada. Así la blockchain opera como un sistema descentralizado. Esto por lo que los nodos deben compartirse y distribuirse la responsabilidad de crear, almacenar y transmitir la información dentro de la red. No existen niveles ni jerarquías, en la blockchain todos los nodos operan por igual.

Para que un nodo funcione correctamente se requiere de un cierto grado de capacidad y poder computacional, además de espacio de almacenamiento suficiente. Por ello, hoy en día es común que muchos usuarios inviertan en los recursos informáticos que desean destinar para desempeñar el papel de nodos.



Libro Contable

La blockchain funciona en base a crear un registro vinculado con todos los registros anteriores formando una cadena. De esta manera se crea un registro inalterable de información de toda la red, en la que cada cambio se realiza gracias al consenso de dicha red. Esto permite un registro contable detallado de cada operación y que cada empresa o entidad puede tener un control total de la contabilidad de sus operaciones.



COMPONENTES DE LA BLOCKCHAIN

Minería de Bloques

Los mineros en una Blockchain son nodos que producen bloques resolviendo problemas matemáticos. Si un minero produce un bloque que está aprobado por un consenso electrónico de nodos, entonces el minero es recompensado con monedas. Los mineros resuelven problemas matemáticos usando poder computacional que hacen cálculos aleatorios. Su trabajo es registrar y verificar nuevas transacciones en el blockchain, usando un hardware que proporciona su potencia computacional para validar estas transacciones, las cuales son agrupadas en bloques. Cuando un minero resuelve un problema matemático para verificar y registrar la transacción este envía la información a todos los nodos de la red y este minero genera una recompensa por a ver resuelto el problema matemático.

Bloques

Un bloque es un conjunto de transacciones confirmadas e información adicional que se ha incluido en la cadena de bloques.

Cada bloque minado debe pasar por el consenso de la red y reportarse como un bloque que ha logrado resolver el problema matemático asignado.

Una vez la red ha entrado en consenso el bloque es incluido en la blockchain y propagado por todos sus nodos. De esta forma, cada nodo de la red cuenta con el nuevo bloque y sirve de punto de verificación para el mismo.

Estos bloques son los que permiten el funcionamiento de la blockchain y sus transacciones.

COMPONENTES DE LA BLOCKCHAIN

Proceso de registro de los bloques en la cadena de bloques

-Los bloques ingresas en la cadena de bloques como registros permanentes.

-Después de que cada bloque es completado, se crea uno nuevo y hay un número incontable de bloques

-Todos los bloques se conectan entre si y en orden cronológico lineal.

-Las cadenas de bloques son inmutables, lo que significa que no se pueden eliminar.

-Cada bloque tiene un valor hash que depende del hash del bloque anterior para que estén todos vinculados.

Cada bloque válido lleva dentro de sí una serie de transacciones que son validadas junto a ese bloque. Cada transacción incluida en el bloque válido pasa a ser una transacción confirmada. De allí en adelante, cada bloque válido agregado a la blockchain sigue confirmando las transacciones anteriores. Con ello se permite asegurar al máximo cada transacción y bloque en la red.

COMPONENTES DE LA BLOCKCHAIN

Estructura de datos de los bloques

Cada bloque válido va acompañado de una estructura de datos que permite verificar este hecho. En la estructura se encuentra el hash del bloque, el Merkle Root, el timestamp, el nonce, los datos de las transacciones del bloque.

Hash

Es una operación criptográfica que genera identificadores únicos e irrepetibles a partir de una información dada. Los hashes son una pieza clave en la tecnología blockchain y tiene una amplia utilidad.

Se usa para identificar una función criptográfica muy importante en el mundo informático. Estas funciones tienen como objetivo primordial codificar datos para formar una cadena de caracteres única. Todo ello sin importar la cantidad de datos introducidos inicialmente en la función. Estas funciones sirven para asegurar la autenticidad de datos, almacenar de forma segura contraseñas y la firma de documentos electrónicos.

Ejemplo de hash:
0x2bc404bf49b592e442c2d84989bc4433a35563d0a5237e04b7c0f5a1982ce7c5

Características de los Hash

Longitud fija: Un hash tiene una longitud fija y finita, posee la cantidad de información que se haya introducido en el mismo.

Efecto avalancha: El más mínimo cambio en los datos que se hayan introducido cambiará el resultado del hash, por eso es muy fácil detectar si un documento ha sido alterado.

Árbol de Merkle: Es un modo de estructurar la información. Una estructura de datos creada con el objetivo de facilitar la verificación de grandes cantidades de datos organizados relacionando los mismos por medio de diversas técnicas criptográficas y de manejo de información.

COMPONENTES DE LA BLOCKCHAIN

Determinista: Solo hay un hash legítimo para cada entrada de datos determinada. Si aplicamos la función de hash al mismo documento varias veces, el resultado será siempre el mismo.

Resistencia débil y fuerte a colisiones: Hace referencia a que es imposible calcular un hash que permita encontrar otro hash igual. Mejor conocidos como pre-imagen y segunda pre imagen, es el concepto base de la seguridad de los hashes.

Función unidireccional: El hash es una función de un solo sentido que impide que accedan terceros a la información.

Son fáciles de calcular: Los algoritmos de hash son muy eficientes y no requieren de grandes potencia de cálculo para ejecutarse.

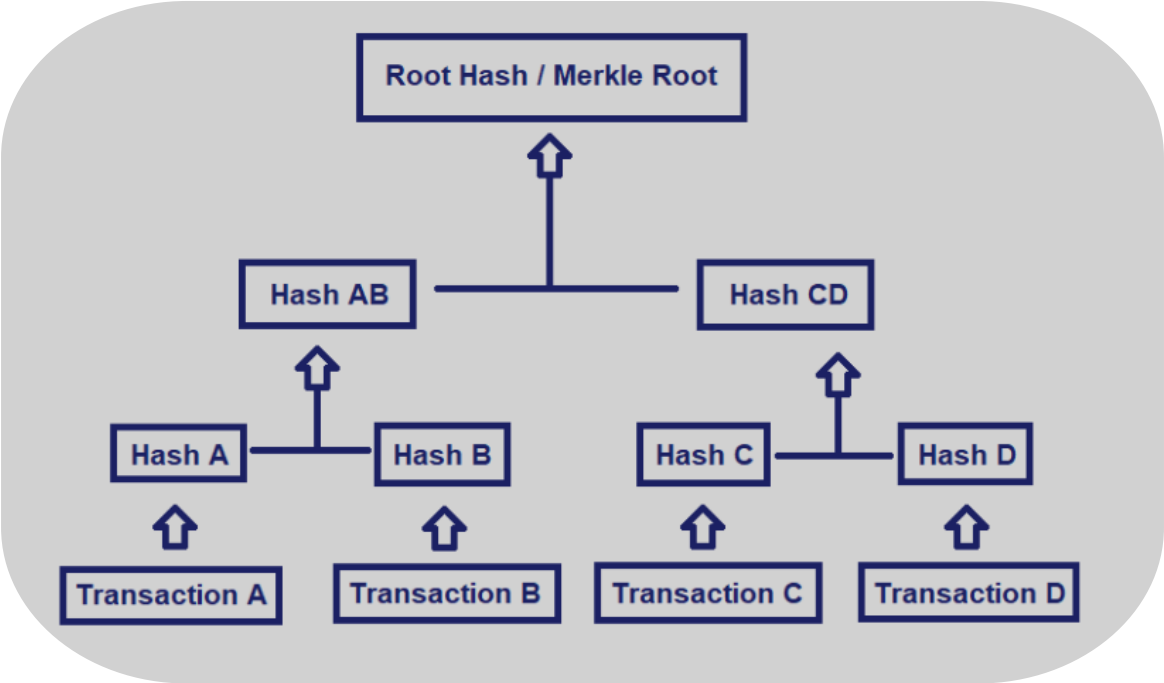
Son irreversibles: Tomar un hash y obtener los datos que dieron origen al mismo, en la práctica no puede ser posible. Este es uno de los principios que hacen a los hashes eguros.

Merkle Root

Es una estructura de datos, permite que gran número de datos separados puedan ser ligados a un único valor de hash. El mayor uso de los árboles de Merkle es hacer seguros los bloques de datos recibidos en las blockchain, asegurar que estos son recibidos sin daños y sin ser alterados.

La razón por lo que esto funciona es porque los hashes se propagan hacia arriba: si un usuario malintencionado intenta hacer un cambio en una transacción en la parte inferior del árbol de Merkle, este cambio provocará un cambio en la parte superior y seguidamente otro cambio, hasta que finalmente, se produzca un cambio en la raíz del árbol y por tanto en el hash del bloque, haciendo que el protocolo tenga que registrarlo como un bloque completamente diferente.

COMPONENTES DE LA BLOCKCHAIN



Timestamp

El timestamp o marca de tiempo es un pequeño dato almacenado en cada bloque a modo de serial único y que tienen como principal función determinar el momento exacto en el que el bloque ha sido sido minado y validado por la red blockchain.

El parámetro temporal o timestamp, se basa en un ajuste instantáneo que usa las marcas de tiempo por todos los nodos de la red. Esto se debe a la forma descentralizada de la misma y busca mantener a los nodos de la red lo mejor sincronizados posible.

Esto permite que el tiempo de la red se ajuste de manera constante, con ello se evita la manipulación. Además una marca de tiempo, hace que el bloque sea imposible de ser repetido en un futuro, ya que además de la hora, también se almacena la fecha de creación del bloque, por lo tanto, no existe la posibilidad de que se repita el mismo hash.

valor Nonce

El valor de nonce que también puede ser utilizado como una medida de seguridad contra ataques maliciosos. Por ejemplo, si un atacante intenta alterar un bloque en la blockchain, necesitaría calcular un nuevo hash para el bloque modificado. Sin embargo, el valor de nonce en el bloque original es único, lo que significa que cualquier cambio en el contenido del bloque alteraría el valor de nonce. Como resultado, el hash del bloque alterado no coincidiría con el valor de nonce original, y el ataque sería detectado y rechazado por la red de blockchain. El valor de nonce es un componente crítico para la seguridad y la integridad de la tecnología blockchain. A través de su uso en la minería de criptomonedas y la validación de transacciones, el valor de nonce garantiza que la blockchain sea segura y resistente a ataques maliciosos.

Exploradores Blockchain

Los exploradores Blockchain son sitios web donde podemos encontrar la información sobre los datos de los bloques y de las transacciones que se encuentran dentro de los bloques.

Información de los bloques:

Altura: Se refiere a la altura o al número de bloques creados dentro una red blockchain en un determinado momento. por ejemplo bloque 100, bloque 3456

Fecha: Se identifica la fecha y hora exacta en la que se minó el bloque.

Tiempo de recepción: Indica el momento en el que la red ha recibido el bloque.

Retransmitido por: Generalmente te indica el nodo que ha transmitido el bloque a los demás nodos interconectados a la red.

Dificultad: La dificultad de minería es un índice utilizado para medir la dificultad de encontrar un bloque.

Tamaño del bloque: Se mide en bytes y refleja el límite máximo en el que un bloque puede incluir transacciones.

COMPONENTES DE LA BLOCKCHAIN

Versión: Este número indica la versión del protocolo que está corriendo el nodo encargado del minado de ese bloque.
Nonce: Es un número arbitrario que se utiliza como protocolo de autenticación. Es una combinación de números con el hash para evitar la manipulación de la información del bloque.
Recompensa de bloque: Refleja las recompensas generadas por la red cada vez que es minado un nuevo bloque

Información de las transacciones dentro de un bloque

Transacción hash: Es el dato para Identificar la transacción
Confirmaciones: Muestra la cantidad de confirmaciones que ha recibido el bloque desde su minado.
Fecha y hora: Brinda el dato exacto en la que se produjo la transacción dentro de la red.
Dirección receptora: La dirección receptora de los fondos.
Dirección emisora: La dirección quien envió los fondos
Cantidad: El dato de la cantidad de fondos transmitida en la transacción.
Feed de transacción: Es el costo generado por efectuar movimientos de fondos en la red.
Bloque: Es el dato del número de bloque a la que la transacción pertenece.

Sitios Web Exploradores blockchain:

Bitcoin: blockchain.com
Ethereum: etherscan.io
Cardano: explorer.cardano.org
Solana: explorer.solana.com
Decentral Chain: decentralscan.com

COMPONENTES DE LA BLOCKCHAIN

Firma digital

Para llevar a cabo una transacción necesitas dos cosas: una billetera, que básicamente es una dirección y una clave privada. La clave privada es una cadena de números aleatorios, pero a diferencia de la dirección, la clave privada debe mantenerse en secreto.

Cuando alguien decide enviar monedas a alguien más, debe firmar el mensaje que contiene la transacción con su clave privada.

Una vez que se envía el mensaje, se transmite a la red de Blockchain. La red de nodos luego trabaja en el mensaje para asegurarse de que la transacción que contiene sea válida. Si confirma la validez, la transacción se coloca en un bloque y después de eso no se puede cambiar la información al respecto.Se centra en el desarrollo de sistemas basados en algoritmos que aumentan su complejidad a medida que la tecnología avanza.

La criptografía es uno de los pilares fundamentales en los que se basa la tecnología blockchain. Ésta permite el funcionamiento de la red, garantiza los mecanismos de consenso entre los usuarios y la integridad de la blockchain.

Claves criptográficas

Una clave criptográfica es una cadena de números y letras. Las claves criptográficas están hechas por generadores de claves o keygens. Estos keygens utilizan matemáticas muy avanzadas que involucran números primos para crear claves.

Criptografía Asimétrica

Desde su nacimiento la tecnología blockchain ha buscado la forma de brindar la mayor seguridad posible. En la búsqueda de tales niveles de seguridad, la criptografía asimétrica ha jugado un papel muy importante. Su uso permitió la generación de claves públicas (direcciones) y privadas que permiten asegurar, enviar y recibir criptomonedas de forma segura.

De hecho, la tecnología blockchain ha sido una perfecta herramienta para probar y desarrollar nuevas técnicas criptográficas.

COMPONENTES DE LA BLOCKCHAIN

La criptografía asimétrica nos permite poseer dos tipos de claves criptográficas, una clave **privada** y una clave **pública**, las cuales son dependientes una de la otra.

La clave privada: también conocida como, frase de seguridad o semilla es muy importante porque nos permite acceder a los fondos y por claras razones se debe guardar bien en un lugar seguro y no compartirla con nadie. Ser el único poseedor de la clave privada es lo que nos hace ser los únicos dueños y los únicos en poder acceder para hacer transacciones con los fondos que tengamos en una billetera virtual. Por lo general en las billeteras virtuales son una serie de palabras que suelen ser de 12 a 15 palabras.

Ejemplo frase semilla 12 palabras:

carro casa perro lapiz arbol motocicleta teatro dinero metal frutas cortina caracol

La clave pública es la dirección para poder recibir o enviar fondos a la cuenta de algún usuario, esta clave si se puede compartir con usuarios y es siempre la misma ya que es dependiente a la clave privada.
Funciona como el correo electrónico que con brindar la dirección ya los usuarios nos pueden enviar o nosotros enviar un mensaje.

Ejemplo clave pública:

0xA9872d9ea134d97CF056d8Fe8815340218bfF21A

COMPONENTES DE LA BLOCKCHAIN

Protocolos

La Blockchain consta de especificaciones de comportamiento individuales, un gran conjunto de reglas que están programadas en ésta. Esas especificaciones se llaman protocolos. La implementación de protocolos específicos esencialmente hizo de Blockchain lo que es una base de datos de información peer-to-peer (punto a punto), distribuida y segura.

Protocolos de Consensos

En Blockchain un algoritmo de consenso es el mecanismo usado por una red Blockchain, para seleccionar el estado correcto de un registro después de realizar una transacción. De esta manera lo que indique el algoritmo de consenso se convierte en la verdad que todos los nodos deben seguir.

Este mecanismo regula e incentiva la forma en que los nodos que sellan bloques llegan a un acuerdo entre sí para poder hacerlo e incorporar ese bloque a la cadena.

Proof of Work (POW) Prueba de trabajo

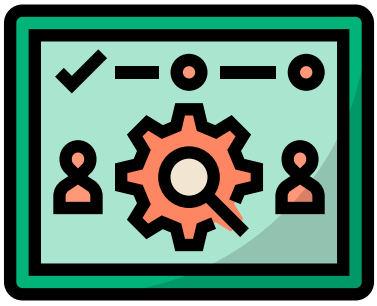
Es el primer algoritmo de consenso de blockchain y fue utilizado por primera vez por Bitcoin, la criptomoneda líder del mercado actualmente. En la minería del PoW, los mineros resuelven acertijos matemáticos complejos que requieren mucha potencia computacional. El primero en resolver el rompecabezas crea un bloque y recibe una recompensa por ello. La forma de resolverlo es básicamente una 'adivinanza', ya que no existe algún método alternativo más que al ensayo y error.

COMPONENTES DE LA BLOCKCHAIN

Proof of Work (POW) Prueba de trabajo

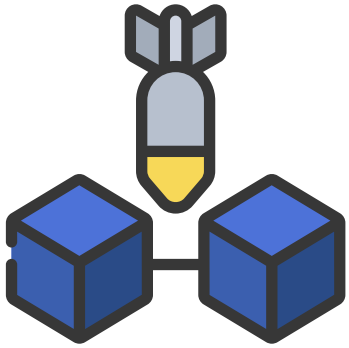
Proceso de Validación:

En un sistema de Prueba de Trabajo, los participantes de la red, conocidos como mineros, compiten para resolver problemas matemáticos complejos. El primero en resolver el problema tiene el derecho de proponer un nuevo bloque a la cadena de bloques y es recompensado con nuevas criptomonedas (por ejemplo, bitcoins) y las tarifas de transacción



Resistencia a Ataques:

PoW proporciona seguridad a través del costo computacional. Resolver los problemas matemáticos y encontrar un bloque válido requiere una cantidad significativa de poder computacional. Esto hace que sea costoso y difícil para un atacante malintencionado alterar el historial de transacciones o tomar el control de la red.



Minería:

La minería es el proceso mediante el cual los mineros utilizan hardware especializado para realizar cálculos intensivos y competir por la posibilidad de agregar un nuevo bloque a la cadena. En el contexto de Bitcoin, los mineros utilizan ASICs (circuitos integrados de aplicación específica) para realizar estos cálculos.

COMPONENTES DE LA BLOCKCHAIN

Consumo de Energía:

Una crítica común a PoW es su alto consumo de energía. El proceso de minería requiere una gran cantidad de poder computacional, lo que conduce a un consumo significativo de electricidad. Este aspecto ha llevado a discusiones sobre la sostenibilidad y la eficiencia energética en blockchain.

Descentralización Inicial:

En las primeras etapas de muchas blockchain basadas en PoW, la minería puede ser llevada a cabo por entusiastas individuales con hardware de uso doméstico. Sin embargo, con el tiempo, ha evolucionado hacia operaciones más grandes y centralizadas, principalmente debido a la eficiencia de los ASIC.

En resumen, la Prueba de Trabajo es un protocolo de consenso que ha demostrado ser efectivo para garantizar la seguridad y la integridad de la cadena de bloques, pero enfrenta desafíos en términos de consumo de energía y centralización a medida que evoluciona con el tiempo.

Proof of Stake (POS) Prueba de participación

Un algoritmo de prueba de participación es un protocolo de consenso distribuido para redes distribuidas que asegura una red de una criptomoneda mediante la petición de pruebas de posesión de dichas monedas.

COMPONENTES DE LA BLOCKCHAIN

Con POS la probabilidad de encontrar un bloque de transacciones y recibir el premio correspondiente es directamente proporcional a la cantidad de monedas que uno tiene acumuladas, evitando así que la confianza venga dada por la cantidad de trabajo invertida.

Un validador en la red son los responsables al igual que los mineros en prueba de trabajo de ordenar transacciones y crear nuevos bloques para que todos los nodos puedan ponerse de acuerdo sobre el estado de la red.

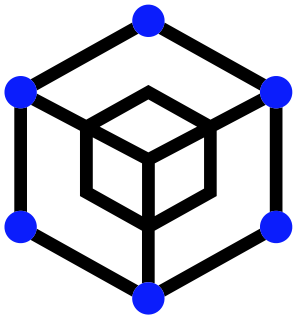
Proof of Stake (POS) Prueba de participación

Validación a través de Participación:
En lugar de utilizar poder computacional para resolver problemas matemáticos, PoS asigna el derecho de proponer y validar bloques en función de la cantidad de criptomonedas que un participante posee y está dispuesto a "apostar" o "bloquear" como garantía.

COMPONENTES DE LA BLOCKCHAIN

Nodos Forjadores o Validadores:

Los participantes en PoS son a menudo denominados "nodos forjadores" o "validadores". Su capacidad para proponer y validar bloques está vinculada a la cantidad de criptomonedas que poseen y están dispuestos a comprometer.

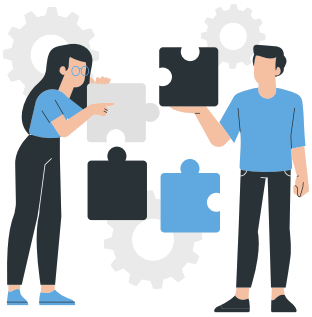


Incentivos a la Posesión:

En PoS, los participantes son incentivados para mantener sus criptomonedas a largo plazo, ya que cuanto más posean, mayor será la probabilidad de que se les elija para validar bloques y recibir recompensas.

Sin Problemas Matemáticos Intensivos:

A diferencia de PoW, no hay problemas matemáticos intensivos que resolver en PoS. La validación se basa en el interés financiero de los participantes en la red.



E**ficiencia Energética:**

PoS es considerado más eficiente desde el punto de vista energético en comparación con PoW. No requiere la cantidad masiva de energía necesaria para alimentar la minería de PoW, ya que la validación se basa en la participación y no en la capacidad de cómputo.

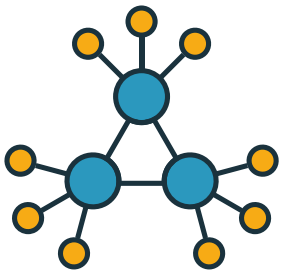
COMPONENTES DE LA BLOCKCHAIN

Desarrollo de Proyectos:

Varios proyectos blockchain han optado por implementar PoS o están considerando hacerlo. Ethereum, la segunda criptomoneda más grande por capitalización de mercado, tiene planes para cambiar de PoW a PoS con Ethereum 2.0.

Descentralización:

PoS ha sido elogiado por su potencial para promover una mayor descentralización en comparación con PoW, ya que no requiere la concentración de poder de cómputo en manos de unos pocos mineros.



En resumen, la Prueba de Participación es un enfoque alternativo de consenso que ha ganado popularidad debido a su eficiencia energética potencial y su capacidad para promover la participación a largo plazo en las redes blockchain.

"BLOCKCHAIN ES LA RESPUESTA PARA CASI TODAS LAS VULNERABILIDADES QUE ENFRENTAMOS HOY".

DON TAPSCOTT
(COAUTOR DE "BLOCKCHAIN REVOLUTION")

EMPLEOS.NET

CAPÍTULO 4:
GENERALIDADES DE LA BLOCKCHAIN

Blockchain solución al doble gasto

El doble gasto es un defecto potencial del dinero digital en sistemas centralizados por el que una misma moneda digital o token puede gastarse más de una vez. Esto es posible porque cada moneda consta de un archivo digital que puede duplicarse o falsificarse. Al igual que con el dinero falsificado, el doble gasto conlleva inflación dado que se crean nuevas monedas fraudulentas que anteriormente no existían. Esto devalúa la moneda en relación a otras unidades monetarias y disminuye la confianza de los usuarios, así como dificulta la circulación y posesión de la moneda. En el caso concreto de las criptomonedas, este se protege contra los ataques de doble gasto agregando cada transacción a la blockchain y verificándola después. Para ello, utiliza un sistema descentralizado, basado en una gran red de nodos que confirman la transacción.

Cuando más vulnerable es Bitcoin a este tipo de ataques, es durante el inicio de la transacción en la red y por eso, a más veces se confirme, menos probable será el riesgo de sufrir un ataque.

Cuando más vulnerable es Bitcoin a este tipo de ataques, es durante el inicio de la transacción en la red y por eso, a más veces se confirme, menos probable será el riesgo de sufrir un ataque. Bitcoin fue la primera criptomoneda creada y lanzada con éxito en el mercado. Pero los primeros intentos de crear una moneda digital tuvieron lugar a principios de los años 80. David Chaum creó la primera moneda digital, conocida como e-Cash. Esta moneda fue la que dio origen al concepto de dinero electrónico y a la posibilidad de que éste pudiera ser duplicado. Sin embargo, en su propuesta Chaum incluyó un sistema que impedía un ataque de doble gasto.

Este sistema era un mecanismo criptográfico, conocido como firmas ciegas u opacas, que evitaban que el emisor conociera el origen del dinero. Y mantenía un servidor central para el control de las monedas y para evitar el doble gasto. Sin embargo, este servidor fue el punto débil de dicho sistema. El hecho de ser centralizado significaba que atacar dicho servidor y hacerse de su control exponía a los usuarios de e-Cash.

Luego, con la propuesta e implementación de Bitcoin, Satoshi Nakamoto planteó el reemplazo del sistema centralizado, por uno basado en el consenso. Donde múltiples nodos conectados a la red son los encargados de realizar las validaciones y confirmaciones de las operaciones. Esta tecnología es lo que hoy conocemos como blockchain. Y por el trabajo realizado, los nodos reciben una recompensa que los incentiva a trabajar de forma honesta. Así, si un nodo deshonesto quiere realizar un ataque de doble gasto, tiene que competir por el poder de hash que poseen los demás nodos conectados. Y mientras más vaya creciendo la red, más difícil será ejecutar un ataque. Bitcoin y otras criptomonedas operan bajo la tecnología blockchain, que posee dos mecanismos para evitar los ataques fraudulentos de doble gasto. Primero, se realiza una validación y registro de todas las transacciones realizadas.

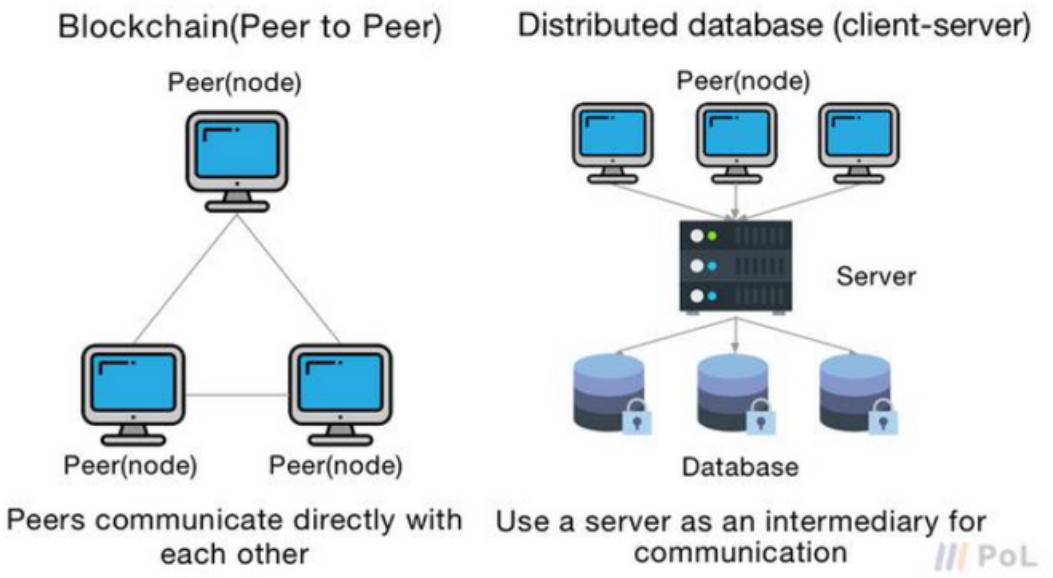
En el caso de Bitcoin, es un registro abierto, verificable y auditable. En segundo lugar, se realiza una verificación para comprobar la autenticidad de cada operación mediante la aplicación de un instrumento conocido como Prueba de Trabajo (PoW) y en otras criptomonedas Prueba de Participación (POS).

GENERALIDADES DE LA BLOCKCHAIN

Blockchain alejado del modelo cliente-servidor

El modelo cliente-servidor es la topología de red dominante en Internet. En este modelo topológico, los nodos en Internet son servidores o clientes. Un cliente que quiere una tarea realizada se pone en contacto con un servidor y realiza una solicitud. El servidor puede optar por responder a la solicitud o ignorarla. Algunos de los servidores también pueden ser clientes atendidos por otros servidores. Debemos observar que existe un grado de centralización en esta topología, lo cual suelen ser más vulnerables para ataques cibernéticos.

Una red blockchain es una red de pares de igual a igual. Es una red peer-to-peer (P2P), todos los nodos de la red son iguales en capacidad. En una red P2P, los nodos son pares entre sí. Un nodo es una copia de la información de Blockchain alojada en una computadora. Cuando se genera un registro nuevo se envía una copia a cada uno de los nodos, de ahí que las computadoras online poseen copias sincronizadas de la cadena de bloques. El objetivo principal de los nodos es aumentar la seguridad y la integridad de la información, debido a que son copias de la misma



GENERALIDADES DE LA BLOCKCHAIN

Generaciones de Blockchain

En el desarrollo de Internet, se puede señalar eventos históricos que pueden usarse para dividir el proceso en etapas y más hablamos de la tecnología Blockchain. Entre estos hitos importantes se encuentran la creación de las primeras redes informáticas de gran área en la década de 1960, el desarrollo de un sistema de correo electrónico en la década de 1970, la creación de Ethernet en esa década, el lanzamiento de la red mundial en la década de 1990 y la creación de los primeros buscadores y motores de búsqueda más adelante en esa década, entre otros. Después de cada uno de estos desarrollos distintivos, Internet cambió de manera espectacular. Cada paso fue fundamental para crear Internet que conocemos y en el que confiamos hoy.
De manera similar, es posible mirar hacia atrás en el desarrollo de blockchain y también dividirlo en etapas. Ya que están marcadas por desarrollos e inventos importantes. La tecnología Blockchain solo ha existido por una fracción del tiempo que Internet tiene, por lo que es probable que aún haya desarrollos importantes por venir. Los expertos han comenzado a dividir la historia de blockchain en varias etapas importantes.

Blockchain 1.0

Fue el desarrollador u organización con seudónimo, Satoshi Nakamoto, quien delineó la primera cadena de bloques tal como la conocemos en el libro blanco de Bitcoin. Las primeras etapas, se estableció la premisa básica de un libro público compartido, uso de bloques de información en transacciones. Los bloques se unen mediante un complejo proceso de verificación criptográfica que forma una cadena inmutable. Se estableció un conceso de prueba de trabajo (POW) para los nodos de la red y Bitcoin obtiene su primer utilidad como recompensa a los mineros por resolver problemas matemáticos para crear bloques en la red.

GENERALIDADES DE LA BLOCKCHAIN

Conceptos importantes que caracterizan Blockchain 1.0:

-Moneda Digital: Es un medio de intercambio disponible en forma digital que posee propiedades similares a las monedas físicas, permite transacciones instantáneas y transferencia de propiedad sin fronteras. Así como el dinero tradicional, estas monedas pueden utilizarse para comprar todo tipo de cosas.

-Merkle tree: Los árboles hash se pueden usar para verificar cualquier tipo de datos almacenados, manejados y transferidos entre computadoras. Pueden ayudar a garantizar que los bloques de datos recibidos de otros pares en una red de igual a igual se reciban sin daños ni alteraciones, e incluso para verificar que los otros pares no mientan y envíen bloques falsos.

-Ledger o libro mayor: Es el registro de todas y cada una de las operaciones y transacciones que se realizan dentro de una blockchain. Con ello, el ledger se convierte en una de las piezas fundamentales de la transparencia, seguridad y privacidad de la tecnología blockchain y las criptomonedas.

-**Blockchain Data**: Registros de datos en donde la información almacenada se alberga en un sistema de bloques. Se trata de un registro único y distribuido en varios nodos de una misma red. La base de datos que genera el blockchain se distribuye entre los usuarios participantes de la red con total transparencia para que tengan libre acceso al contenido.

Blockchain 2.0

A medida que pasó el tiempo, los desarrolladores comenzaron a creer que una cadena de bloques podría hacer más que simplemente documentar las transacciones. Los fundadores de ethereum, por ejemplo, tenían la idea de que los activos y los acuerdos de fideicomiso también podrían beneficiarse de la gestión blockchain. De esta manera, ethereum representa la segunda generación de la tecnología blockchain.

GENERALIDADES DE LA BLOCKCHAIN

Conceptos importantes que caracterizan Blockchain 2.0:

-Contratos Inteligentes: Es un protocolo informático utilizado para facilitar, verificar o hacer cumplir digitalmente la negociación de un contrato. Las transacciones de la red se ejecutan en un contrato inteligente, que la cadena de bloques procesa y ejecuta automáticamente. Entonces, cada vez que ocurre una transacción entre los nodos, se invoca una función que llama al contrato inteligente y comienza el procesamiento. Por lo tanto, la transacción se puede enviar a cualquier nodo de la cadena de bloques, que la transmite a toda la red para que todos los nodos vean la transacción.

-Virtual Machine EVM: La representación física de EVM no se puede describir del mismo modo que una nube o una ola, pero existe como una única entidad sustentada por miles de computadoras conectadas ejecutando un cliente. El protocolo de en sí mismo existe únicamente con el propósito de mantener el funcionamiento continuo, interrumpido e inmutable de esta máquina de estado especial; se trata del entorno que alberga todas las cuentas y los contratos inteligentes. La EVM es la que define las reglas de cálculo de un nuevo estado válido de bloque a bloque.

-Aplicaciones descentralizadas (Dapp): Son herramientas o apps que no están gestionadas por empresas y donde los usuarios se relacionan directamente sin intermediarios entre ellos, generalmente a través de una blockchain. Los datos generados por esta aplicación están alojados en una red de ordenadores que permite que esta información se mantenga segura y accesible. Podríamos imaginar a una DApp como una aplicación conocida como Facebook, You tube pero que en vez de ejecutarse sobre un servidor central (suelen ser varios) se ejecuta en una red formada por miles de nodos u ordenadores.

Blockchain 3.0

Es la etapa de desarrollo de la tecnología blockchain, que permite la adopción global, institucional y empresarial.

GENERALIDADES DE LA BLOCKCHAIN

Conceptos importantes que caracterizan Blockchain 3.0:

-Escalabilidad: Uno de los principales problemas de las cadenas de bloques de primera y segunda generación es el la Escalabilidad. Las Blockchain se miden por capacidad de procesamiento de transacciones por segundo, en las blockchain de primera y segunda generación en el caso de Bitcoin es de 5 transacciones por segundo y en Ethereum 20 transacciones por segundo, lo que al día de hoy son muy lentas por la alta demanda de usuarios y dapps, lo cual también ha provocado que las tarifas por transaccionar sean muy altas.

Las Cadenas de Bloques de tercera generación son nuevas redes blockchain programables, capaces de soportar aplicaciones descentralizadas, pero con mucha mayor capacidad que las redes de primera y segunda generación, ya que pueden llegar a soportar 75,000 transacciones por segundo y bajo costo.

-Inter Operabilidad: El concepto de interoperabilidad de blockchain se refiere a la capacidad de diferentes redes de cadenas de bloques para intercambiar datos entre sí y para mover tipos únicos de activos digitales entre las respectivas cadenas de bloques de las redes. En un sistema interoperable, las redes y activos de blockchain que alguna vez fueron dispares pueden conectarse fácilmente y combinarse entre sí. Esta interoperabilidad de red puede permitir la creación de nuevos productos y servicios que aprovechen los beneficios de múltiples redes Blockchain simultáneamente.

-Industrias: Hace unos años apareció un nuevo concepto, el del internet del valor. Se basa en el descubrimiento de la tecnología blockchain y se contrapone al Internet de la información en que permite compartir el valor, ya que no necesita que una entidad central de confianza. Esta tecnología se aplicará a títulos, certificaciones, archivos, canciones, se trata de una red articulada por las propias personas generando contenido sin intermediarios y donde todo el mundo es emisor y receptor.

GENERALIDADES DE LA BLOCKCHAIN

Cuando se habla de la industria 4.0 se refiere a la digitalización de los procesos productivos en las fábricas a través de sistemas de información y sensores que harán que se produzca mejor y más eficientemente. Se trata de la comunicación entre humanos y máquinas en Sistemas ciberfísicos a través de extensas redes lo que hará que sea posible obtener y examinar diferentes datos a través de las máquinas, lo que permitirá procesos más rápidos, más eficientes y más flexibles para la fabricación de productos de mayor calidad a un costo más reducido.

El concepto parte de la consideración de que esta va a ser la cuarta revolución Industrial. Otras innovaciones técnicas hicieron posible las 3 anteriores: el agua y el vapor permitieron que la energía entrase en las fábricas del siglo XXVIII, la electricidad permitió la fabricación en cadena y un aumento considerable de la productividad en el siglo XX, y la tecnología digital supuso una nueva revolución cuando sustituye a la analógica, a partir de los años 70 del Siglo XX.

-Infraestructura: Blockchain de última generación utilizan soluciones como el mecanismo del consenso prueba de participación (PoS), permite que no se tengan que utilizar dispositivos físicos para brindar poder computacional para la minería, lo que a ayuda a reducir el gasto energético. Además este tipo de blockchain ya tienen un protocolo de interacción que permite un mecanismo de transmisión de datos y activos entre blockchains sin necesidad del uso de un sistema externo descentralizado.

-**Ecosistemas**: Los ecosistemas basados en proyectos en blockchain crecen a mayor velocidad a razón de tantas ventajas que brindan blockchain de última generación, por ejemplo: aquellas criptomonedas que tengan las características de velocidad en sus transacciones y bajas comisiones tienen la capacidad de convertirse en medios de pago"

"BITCOIN ES UNA FORMA DE DINERO QUE ES UNA HERRAMIENTA DE LIBERACIÓN, NO DE OPRESIÓN".

ANDREAS ANTONOPOULOS
(AUTOR Y EDUCADOR EN BITCOIN)

EMPLEOS.NET

CAPÍTULO 5: BITCOIN

Bitcoin (BTC) es conocida como una blockchain de primera generación, utiliza una criptomoneda digital llamada bitcoin y es conocida como el Oro digital, su código es de fuente abierta y peer-to-peer, desarrollada y lanzada por un grupo de programadores independientes llamados Satoshi Nakamoto en el 2008. Bitcoin no tiene ningún servidor centralizado, es totalmente descentralizado, ya que utiliza una tecnología de base de datos pública de red y distribuida en ordenadores llamada blockchain, que requiere una firma electrónica y está respaldada por un protocolo de prueba de trabajo para su consenso y así proporcionar la seguridad y legitimidad de las transacciones monetarias.

El primer bloque minado de Bitcoin fue el 3 de enero del 2009. La emisión de Bitcoin es realizada por usuarios con capacidades mineras y está limitada a 21 millones de monedas y cada unidad es divisible en ocho unidades. Actualmente la red consta de más de 12 mil nodos en todas partes del mundo. El ranking actual de CoinMarketCap es el # 1, con una capitalización de mercado de $ 703,505,238,651 USD. El precio de cada Bitcoin es de $ 37,200, tiene un suministro circulante de 18,940,675 monedas BTC y un máximo. suministro de 21.000.000 de monedas BTC. La compra y venta de Bitcoin está disponible a través de plataformas especiales de bolsas de criptomonedas, cajeros automáticos y con personas de confianza. La velocidad de la red de Bitcoin se mide por transacciones por segundo la cual puede soportar de 5 a 7 transacciones por segundo.

BITCOIN

Halving de Bitcoin

Un halving de Bitcoin se da cuando el beneficio por minar nuevos bloques se reduce a la mitad, lo que implica que los mineros reciben un 50% menos de Bitcoin por verificar las transacciones.

Los halving de Bitcoin tienen lugar cada 210 000 bloques (aproximadamente cada cuatro años), y se producirán hasta que la red haya generado una oferta máxima de 21 millones de Bitcoin.
Los halving de Bitcoin son eventos importantes para los inversores porque reducen el número de Bitcoin nuevos que genera la red. Esto limita la oferta de nuevas monedas, por lo que los precios podrían subir si la demanda se mantiene alta. Aunque esto ha pasado durante los meses previos y posteriores a los halving que han tenido lugar con anterioridad (lo que ha precipitado que el precio del Bitcoin se apreciase rápidamente), las circunstancias en las que tiene lugar cada halving son diferentes y la demanda de Bitcoin puede fluctuar de manera importante.

El halving más reciente de bitcoin tuvo lugar el 11 de mayo de 2020, causando que la recompensa por bloque descendiera de 12,5 a 6,25 bitcoin**.**

Evento	Fecha	Número de bloque	Recompensa por bloque	Total de bitcoins nuevos entre eventos
Lanzamiento de bitcoin	3 enero 2009	0 (bloque génesis)	50 nuevos BTC	10 500 000 BTC
Primer halving	28 noviembre 2012	210 000	25 nuevos BTC	5 250 000 BTC
Segundo halving	9 julio 2016	420 000	12,5 nuevos BTC	2 625 000 BTC
Tercer halving	11 mayo 2020	630 000	6,25 nuevos BTC	1 312 500 BTC
Cuarto halving	Se espera para el año 2024	840 000	3,125 nuevos BTC	656 250 BTC
Quinto halving	Se espera para el año 2028	1 050 000	1,5625 nuevos BTC	328 125 BTC

Bitcoin Script

El Bitcoin Script es un lenguaje de programación simple empleado en Bitcoin para el procesamiento de las transacciones, usados para bloquear y desbloquear las transacciones.

Un script es esencialmente una lista de instrucciones registradas con cada transacción que describen cómo la próxima persona que quiera gastar los Bitcoins que se transfieren puede acceder a ellos.

El lenguaje de Bitcoin no es (Turing Completo) debido a que su funcionalidad es limitada y no puede realizar bucles. Por lo que no es capaz de resolver cualquier tipo de problema como las máquinas Turing.

- La Máquina de Turing es un modelo matemático consistente en un autómata que es capaz de implementar cualquier problema matemático expresado a través de un algoritmo y que además puede adaptarse para que simule la lógica de cualquier algoritmo de computador.

-Bucle informático: Un bucle informático es un fragmento de código que se ejecuta repetidamente hasta que se cumple una condición dada.

Esta limitación en Bitcoin de no ser capaz de realizar bucles y que no sea turing es intencional ya que así se evita la entrada en un bucle infinito o sin fin y la ejecución de errores. Donde las partes maliciosas del programa pueden tener la libertad de crear operaciones complicadas para consumir la tasa de hash y ralentizar el sistema de Bitcoin a través de bucles infinitos.

El código que Bitcoin ejecuta cuando se produce una transacción está hecho usando el Bitcoin Transaction Language. Bitcoin utiliza un sistema de secuencias de comandos para las transacciones, es intencionalmente no Turing-completo, sin bucles.

BITCOIN

Utilidades de Bitcoin

Pagos móviles de forma fácil: Bitcoin le permite pagar con un dispositivo móvil en dos sencillos pasos: escanear y pagar.

No hay necesidad de pasar la tarjeta, teclear un PIN o firmar nada. Todo lo que necesita para recibir pagos con Bitcoin es mostrar el código QR en su aplicación de monedero y dejar que su amigo escanee su móvil o juntar los dos teléfonos (usando la tecnología NFC).

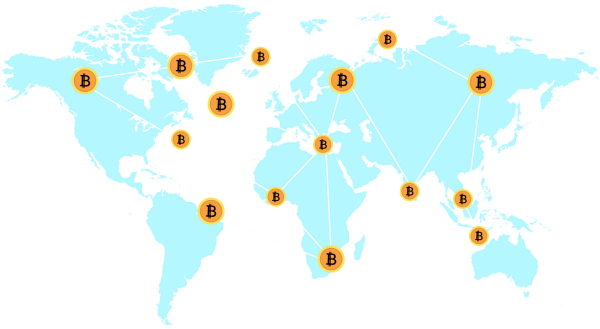
Seguridad y control sobre su dinero: Las transacciones de Bitcoin están aseguradas mediante criptografía militar. Nadie puede cobrarle dinero o hacer un pago en su nombre.

Tan pronto como tome los pasos requeridos para proteger su monedero, Bitcoin podrá darle control sobre su dinero y un fuerte nivel de protección contra muchos tipos de fraude.

BITCOIN

Utilidades de Bitcoin

Funciona en todas partes y en cualquier momento: Al igual que con el correo electrónico, no es necesario pedir a su familia que utilice el mismo software o los mismos proveedores de servicio. Deje que usen sus favoritos. No hay problema; todos ellos son compatibles, ya que utilizan la misma tecnología. La red Bitcoin nunca duerme ni tiene vacaciones.



Pagos internacionales: Bitcoin puede ser transferido de África a Canadá en menos de 10 minutos. No existe un banco que retrase el proceso, honorarios escandalosos o congelar la transferencia. Usted puede pagarle a sus vecinos de la misma manera que usted puede pagarle un miembro de su familia en otro país.

Baja comisión: Bitcoin le permite enviar y recibir pagos a un costo muy bajo en comparación con los bancos sistemas centralizados.

BITCOIN

Proteja su identidad: Con Bitcoin, no existe un número de tarjeta de crédito que alguien pueda usar para hacerse pasar por ti. Es posible hacer un pago sin revelar tu identidad, casi como el dinero físico. Ya que cuando se genera una transacción los datos son almacenados y registrados públicamente a tiempo real pero todos los datos y direcciones están encriptados en algoritmos matemáticos.

Proteja su identidad: Con Bitcoin, no existe un número de tarjeta de crédito que alguien pueda usar para hacerse pasar por ti. Es posible hacer un pago sin revelar tu identidad, casi como el dinero físico. Ya que cuando se genera una transacción los datos son almacenados y registrados públicamente a tiempo real pero todos los datos y direcciones están encriptados en algoritmos matemáticos.

Visibilidad gratis para las empresas: Bitcoin es un mercado emergente con nuevos clientes que están buscando maneras de gastar sus Bitcoin. Aceptar pagos con Bitcoin es una buena forma de conseguir nuevos clientes y de dar a su negocio un poco de visibilidad. Aceptar una nueva forma de pago siempre ha demostrado ser una práctica inteligente para los negocios online.

BITCOIN

Transparencia contable: Muchas organizaciones están obligadas a presentar los documentos de contabilidad sobre sus actividades. Usar Bitcoin ofrece el más alto nivel de transparencia ya que puede proveer toda la información necesaria para que sus miembros verifiquen sus sueldos y transacciones. Las organizaciones sin ánimo de lucro también pueden publicar cuantas donaciones reciben.

"ETHEREUM: EL SUEÑO DE LA DESCENTRALIZACIÓN EN ACCIÓN".

MATTHEW ROSZAK
(COFUNDADOR DE BLOQ)

EMPLEOS.NET

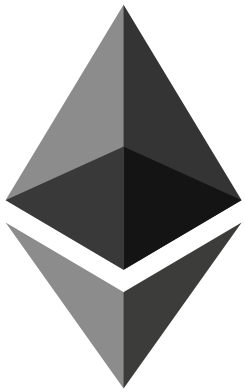
CAPÍTULO 6: ETHEREUM

A finales de 2013, Vitalik Buterin describió su idea en un libro blanco, que envió a algunos de sus amigos, que a su vez lo enviaron más lejos. Como resultado, unas 30 personas contactaron a Vitalik para discutir el concepto. Estaba esperando críticas y gente señalando errores críticos en el concepto, pero nunca sucedió.

El proyecto fue anunciado públicamente en enero de 2014, con el equipo central formado por Vitalik Buterin, Mihai Alisie, Anthony Di Iorio, Charles Hoskinson, Joe Lubin y Gavin Wood. Buterin también presentó Ethereum en el escenario de una conferencia de Bitcoin en Miami, y pocos meses después el equipo decidió realizar una venta al por mayor de Ether, el token nativo de la red, para financiar el desarrollo. En la oferta inicial de la moneda (ICO) Ethereum fue un gran éxito: el equipo consiguió recaudar $15,5 millones, vendiendo 50 millones de tokens a un precio de $ 0,31 por token.

Al día de hoy cada Ether tiene un valor de $2500, el ranking actual de CoinMarketCap es el #2, con una capitalización de mercado de $301,031,479,322 USD. Tiene un suministro en circulación de 119,323,461 monedas ETH y no tiene límite emisión.

Ethereum es una plataforma de software distribuida pública, de código abierto y basada en Blockchain que permite a los desarrolladores crear e implementar aplicaciones descentralizadas. Estas aplicaciones pueden ser ideas completamente nuevas o bien reelaboraciones descentralizadas de conceptos ya existentes. Esto esencialmente elimina al intermediario y todos los gastos asociados con la participación de un tercero.



ETHEREUM

Ethereum tomó la tecnología detrás de Bitcoin y expandió sustancialmente sus capacidades. Es una red completa, con su propio navegador de Internet, lenguaje de codificación y sistema de pago.

La velocidad de la red de Ethereum es de 20 transacciones por segundo.

Ethereum es un sistema descentralizado, lo que significa que utiliza un enfoque de par a par. Cada una de las interacciones tiene lugar entre los usuarios que participan en ella, sin que intervenga ninguna autoridad de control.

Todo el sistema Ethereum está soportado por un sistema global de los llamados nodos. Los nodos son voluntarios que descargan toda la cadena de bloques de Ethereum a sus escritorios y hacen cumplir plenamente todas las reglas de consenso del sistema, manteniendo la red honesta y recibiendo recompensas a cambio.

Todo el sistema Ethereum está soportado por un sistema global de los llamados nodos. Los nodos son voluntarios que descargan toda la cadena de bloques de Ethereum a sus escritorios y hacen cumplir plenamente todas las reglas de consenso del sistema, manteniendo la red honesta y recibiendo recompensas a cambio.

Una de las principales desventajas de la red blockchain de Ethereum, es su alto costo en las tarifas de trazabilidad y la escalabilidad. Son por razones como estas que se siguen desarrollando mejoras en el proyecto.

ETHEREUM

Lenguajes de programación

Los Lenguajes de programación son lenguajes diseñados para realizar tareas que pueden ser llevadas a cabo por maquinas. Para entendernos son el lenguaje de las maquinas.

Ethereum es una blockchain publica con un lenguaje de programación Turing completamente integrado (contiene siete lenguajes de programación diferentes para codificar (Java, Python, JavaScript, Go, Rust, .NET, Delphi).

Máquina de Turing: es un modelo matemático que puede adaptarse para que simule la lógica de cualquier algoritmo de computador, de ahí su enorme potencial y valor.

Existen dos lenguajes de programación ampliamente utilizados para programar en Ethereum: Solidity y Vyper.

Solidity: Es un lenguaje de programación de alto nivel creado específicamente para desarrollar aplicaciones en la cadena de bloques de Ethereum.

Está diseñado para proporcionar seguridad y fiabilidad en las aplicaciones construidas en la cadena de bloques. Solidity ofrece herramientas para crear contratos inteligentes escalables, fiables y flexibles que pueden ser ejecutados sin problemas en los nodo Ethereum.

ETHEREUM

Vyper: es un lenguaje de programación de bajo nivel que proporciona seguridad y claridad a los contratos inteligentes.

vyper

Todos los lenguajes de programación son Turing completos y por eso todo lo que se pueda programar con un lenguaje se puede hacer con otros, sólo cambia el rendimiento y el código. El concepto de Turing completo viene de la informática. Turing completo es que permite que un ordenador pueda llegar a programarse para realizar cualquier tipo de operación como: codificar, calcular y hacer cualquier cosa con el permitiendo que se pueda escribir contratos inteligentes y aplicaciones descentralizadas (DApp).

El protocolo de Ethereum fue concebido originalmente como una versión mejorada de Bitcoin, moviéndose mucho más allá de la funcionabilidad del sistema de pagos descentralizado. Este protocolo está construido para permitir flexibilidad a los usuarios a aumentar la funcionabilidad del sistema conforme vaya avanzando y proporcionándola capacidad de programar muchos tipos de contratos inteligentes.

ETHEREUM

Del libro de contabilidad a la máquina de estado.

La analogía del libro de contabilidad distribuido suele utilizarse para describir blockchain como Bitcoin, que permite la existencia de una moneda descentralizada que utiliza herramientas fundamentales de criptografía. Una criptomoneda se comporta como una moneda norma, debido a las reglas que rigen lo que uno puede o no puede hacer para modificar el libro de contabilidad. Por ejemplo, una dirección de Bitcoin no puede gastar más Bitcoin de los que ha recibido previamente. Estas reglas sustentan todas las transacciones de Bitcoin y muchas otras blockchain.

Aunque Ethereum tenga su propia criptomoneda nativa (Ether), que sigue casi exactamente las mismas reglas intuitivas, también permite el uso de una función mucho más poderosa: los contratos inteligentes. Para explicar esta característica más compleja se requiere una analogía más sofisticada. En lugar de un libro mayor distribuido, Ethereum es una máquina de estado distribuida. El estado de Ethereum es una gran estructura de datos, que no solo sostiene todas las cuentas y saldos, sino que también alberga el estado de la máquina.

ETHEREUM

Contratos Inteligentes

Un contrato inteligente es básicamente un programa que se ejecuta en una blockchain. Se trata de un grupo de código (sus funciones) y datos (su estado) que existe en una dirección específica en la blockchain.

Los contratos inteligentes son un tipo de cuenta. Esto significa que tienen un saldo y pueden enviar transacciones por la red. Sin embargo, no están controlados por un usuario, sino que están implementados en la red y se ejecutan como se hayan programado.

Las cuentas de usuario pueden interactuar con un contrato inteligente enviando transacciones que ejecuten una función definida en el contrato inteligente. Los contratos inteligentes pueden definir reglas, como un contrato normal y automáticamente se ejecutan a través del código.

Un contrato inteligente es un acuerdo entre dos personas o entidades en forma de código informático programado para ejecutarse automáticamente.

Son capaces de facilitar el intercambio de dinero, bienes y cualquier otra cosa de valor, asegurando la total transparencia, evitando los servicios y los cargos de acompañamiento de un intermediario y erradicando la cuestión de la confianza entre las partes. El código de un contrato inteligente en particular incluye todos los términos y condiciones acordados por las partes, y la información sobre la transacción en sí se registra en una cadena de bloques, un libro mayor público descentralizado y distribuido.

ETHEREUM

Contratos Inteligentes

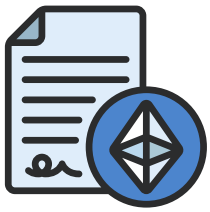
Beneficios de los contratos inteligentes

Independencia: Los participantes realizan las gestiones por sí mismos, es decir, se puede prescindir de la participación de los intermediarios.

Fiabilidad: El contrato se almacena de forma segura en una red distribuida y es virtualmente imposible de alterar o falsificar.

Seguridad: Al estar en una red distribuida, el contrato se encuentra duplicado en todos los nodos de la red y no puede perderse.

Ahorro: Al prescindir de intermediarios y de comisiones, se produce una reducción de los costes para todos los implicados.



Precisión: Este tipo de contratos reducen a cero la posibilidad de que se produzcan errores en los términos o en la tramitación.

Sostenibilidad: Los contratos eliminan el uso de papel en oficinas, notarios y registros y al minimizar los desplazamientos se reduce la contaminación.

ETHEREUM

DApps

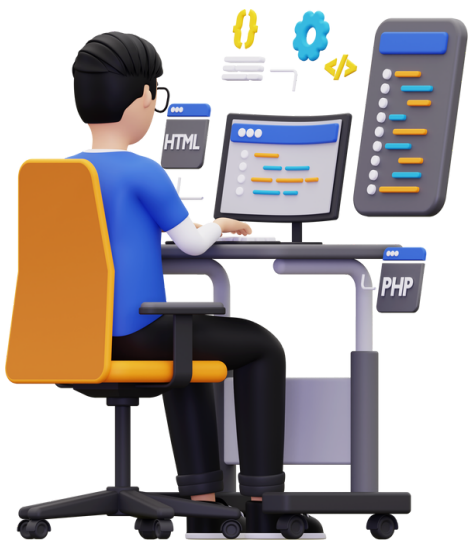
Las Aplicaciones Descentralizadas (DApps) son aplicaciones que funcionan en una red descentralizada de nodos, generalmente en blockchain. Dapp es el término abreviado para una aplicación descentralizada. La lógica de la aplicación principal y el almacenamiento de datos de las dApps se ejecutan en una red peer-to-peer descentralizada y distribuida. Las dApps permiten la interacción directa entre usuarios sin necesidad de una autoridad central o intermediario.

Características importantes de las DApps:

Descentralización:
Las DApps operan en una red descentralizada de nodos, eliminando la necesidad de una autoridad central. Esto proporciona resistencia a la censura y aumenta la seguridad al evitar puntos únicos de falla.

Contratos Inteligentes:
Las DApps a menudo utilizan contratos inteligentes, que son programas autoejecutables basados en código en la cadena de bloques. Estos contratos definen las reglas y lógica de la aplicación, garantizando la transparencia y la ejecución automática.

Transparencia:
Todas las transacciones y acciones realizadas en una DApp son transparentes y verificables en la cadena de bloques. La información sobre la actividad de la aplicación está disponible para todos los participantes de la red.



ETHEREUM

Seguridad:
La seguridad se mejora debido a la descentralización y al uso de criptografía. La información sensible y las transacciones están protegidas, y la resistencia a la censura contribuye a la seguridad general de la aplicación.

Interoperabilidad:
Algunas DApps están diseñadas para ser interoperables, lo que significa que pueden interactuar y compartir datos con otras DApps o servicios en la cadena de bloques. Esto facilita la creación de ecosistemas más amplios y colaborativos.

Incentivos Tokenizados:
Muchas DApps utilizan tokens criptográficos nativos de la plataforma para incentivar la participación y recompensar a los usuarios por contribuir al ecosistema. Estos tokens pueden tener diversos usos dentro de la aplicación.

Acceso Público:
Las DApps son generalmente de acceso público y no requieren aprobación central para participar. Cualquier persona con acceso a la red puede utilizar la DApp y contribuir a su desarrollo.

Resiliencia a la Censura:
La arquitectura descentralizada de las DApps proporciona resistencia a la censura gubernamental o corporativa. Las transacciones y datos no pueden ser fácilmente controlados o bloqueados por terceros.

Propiedad de Datos:
Los usuarios de las DApps a menudo tienen más control sobre sus datos personales. La propiedad y el control de los datos pueden residir en manos de los usuarios, reduciendo el riesgo de explotación y pérdida de privacidad.

ETHEREUM

Las Dapps se pueden clasificar en base sí disponen de su propia blockchain o si utilizan la cadena de bloques de otra dapp.

Dapp tipo 1: Disponen de su propia cadena de bloques independientemente. Bitcoin y Ethereum serían ejemplos de este tipo de aplicación descentralizada.

Dapp tipo 2: Emplean la blockchain de una Dapp tipo 1 en vez de tener ellas su propia. Este tipo de aplicación descentralizada son protocolos que funcionan ya sea con sus propios tokens o con los tokens de la cadena de bloques en la que operan.

Dapp tipo 3: Utilizan el protocolo de una descentralizada de tipo 2. Estas aplicaciones también funcionan con sus propios tokens digitales o bien con los de las aplicaciones descentralizadas en las que se basan, al igual que pasaba con las dapps de tipo 2.

Ethereum 2.0

Ethereum 2.0 "Serenity", una nueva iteración de esta plataforma cuyo token es Ether que renace con una cadena de bloques o blockchain renovado en el que se mejora la eficiencia, la escalabilidad y el número de transacciones por segundo (para habilitar pagos) y en el que desaparece uno de los encantos con los que nació: se acabó minar ETH con GPUs. Hasta ahora Ethereum usaba un mecanismo de consenso (POW) prueba de trabajo en la que los mineros usaban hardware como GPUs para procesar complejos problemas matemáticos que permitían verificar nuevas transacciones pero ese proceso suele consumir una gran cantidad de energía y el registro en los bloques es muy lento y alto comisión. Ethereum lo que implemento es una versión (POS) Prueba de participación, no hay mineros, sino validadores de transacciones que deben tener cierta participación (actualmente, 32 ETH, unos $102 mil dólares al valor actual) en este sistema para poder verificarlas


“WEB3 SE TRATA DE LIBRE ELECCIÓN Y DEMOCRACIA.”
GUN GUN FEBRIANZA.
EMPLEOS.NET

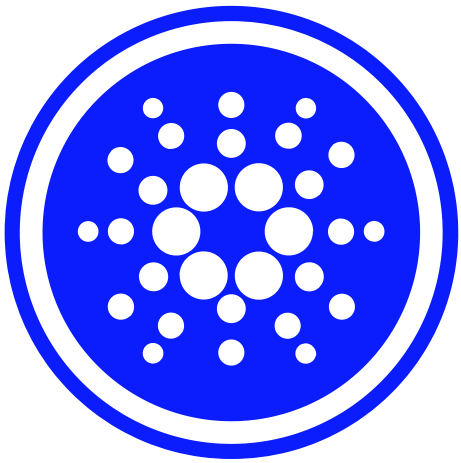
CAPÍTULO 7: CARDANO, SOLANA Y BINANCE

Cardano

Cardano es uno de los proyectos de más rápido crecimiento en el espacio de las criptomonedas. El equipo detrás de su cadena de bloques de código abierto realiza una investigación exhaustiva y publica regularmente sus resultados en artículos académicos revisados por pares. Su investigación se centra en la construcción de una red descentralizada escalable, segura y eficiente mediante la adopción de un enfoque sistemático para la investigación y el desarrollo de blockchain.

Tomando su nombre del erudito italiano del siglo XVI Gerolamo Cardano, la plataforma ha crecido significativamente en los últimos años, con su token ADA nativo actualmente clasificado como el sexto activo digital más grande por capitalización de mercado en todo el mundo. ADA lleva el nombre de la matemática del siglo XIX Ada Lovelace, a quien a menudo se la considera la primera programadora de computadoras del mundo.

El proyecto Cardano comenzó en 2015 cuando uno de los cofundadores de Ethereum, Charles Hoskinson , y su antiguo colega Jerry Wood abandonaron la Fundación Ethereum tras desacuerdos internos. Establecieron una nueva empresa, Input Output (IOHK), que luego lanzó la red Cardano y el token ADA en 2017.



CARDANO

Cardano utiliza una arquitectura única que emplea un sistema de doble capa, que es distinto de la mayoría de las demás plataformas de cadena de bloques. Su capa de liquidación (CSL) permite a los titulares de tokens ADA enviar y recibir transacciones casi instantáneamente a tarifas bajas, mientras que su capa computacional (CCL) sirve como base para el resto de la funcionalidad de Cardano.

Esta capa flexible se compone de muchos protocolos y opera por separado del CSL. Admite el buen funcionamiento de los contratos inteligentes y, al mismo tiempo, garantiza la seguridad y el rendimiento de la red.

La cadena de bloques de Cardano se escribió utilizando un lenguaje de programación seguro y universalmente reconocido conocido como Haskell. Utiliza el mecanismo de consenso de prueba de participación (PoS) pero con un ligero giro. Usando una versión autorizada de la familia Ouroboros de protocolos de consenso PoS (Ouroboros- BFT), Cardano tiene como objetivo ofrecer un mayor nivel de seguridad que las cadenas PoW a una fracción de sus costos de energía.

El precio de Cardano (ADA) a hoy es de $ 1.37 USD con un volumen de operaciones de 24 horas de $ 1,547,980,032 USD. El ranking actual de CoinMarketCap es el número 6, con una capitalización de mercado de $ 45 mil millones de dólares. Tiene un suministro en circulación de 33,539,974,392 monedas ADA y un máx. suministro de 45.000.000.000 monedas ADA.

El 57,6 % del suministro total de 45 000 millones de tokens se distribuyó a los inversores a través de una Oferta inicial de monedas (ICO), a través de la cual el ecosistema obtuvo una financiación de 62,2 millones de dólares en el año 2017. Además de la transferencia y el comercio de valor, los participantes de la red también pueden usar el token para participar en los sistemas de gobierno de la p plataforma. Los participantes de ADA también se consideran validadores, ya que funcionan como nodos que registran el estado actual de la red.

SOLANA

Solana

Un flujo aparentemente interminable de redes ha implementado soluciones al problema de escalado, pero ninguna ha tenido un éxito total en sus objetivos. El llamado trilema blockchain ha perseguido durante mucho tiempo a las redes distribuidas, ya que los nuevos proyectos intentan crear una red descentralizada que sea tanto escalable como segura.

El desafío radica en lograr los tres aspectos del trilema: descentralización, seguridad y escalabilidad. Si bien algunos proyectos han construido con éxito redes que resuelven una o dos facetas del problema, pocos han estado cerca de implementar las tres. Solana es una cadena de bloques de tercera generación que admite una variedad de soluciones DeFi , incluido el desarrollo de aplicaciones descentralizadas (DApps) y contratos inteligentes . A diferencia de otras cadenas de bloques, Solana utiliza un algoritmo de consenso híbrido que combina prueba de historial (PoH) con prueba de participación (PoS), lo que permite que la red realice hasta 50 000 transacciones por segundo.

Esta iniciativa de código abierto también permite una eficiencia mucho mayor que los modelos actuales como Ethereum.

El fundador de Solana, es Anatoly Yakovenko fue gerente senior de ingeniería de personal en la corporación multinacional estadounidense Qualcomm. Poco después, Yakovenko saltó a Dropbox para trabajar como ingeniero de software, antes de dejar la empresa para comenzar a construir Solana en 2017.

SOLANA

La primer tarea de Yakovenko fue abordar el tiempo que tardaron redes como Bitcoin y Ethereum en llegar a un consenso, lo que condujo a la incorporación de PoH en su algoritmo de consenso, en contraste con los mecanismos de consenso establecidos más conocidos.

Solana se lanzó durante el auge de las ICO de 2017 y recaudó $25 millones en rondas de financiación pública y privada.

El precio de Solana a hoy es de $ 124 USD. El ranking actual de Solana en CoinMarketCap es de número 7, con una capitalización de mercado de $39 mil millones de dolares. Tiene un suministro circulante de 314,520,183 monedas SOL y el suministro máximo de SOL está cerca de los 500 millones de tokens, Alrededor del 60% de estos tokens están controlados por los fundadores del proyecto y la Fundación Solana, con solo el 38% reservado para la comunidad.

Proof-of-History (PoH):

Es un algoritmo blockchain complementario al método de consenso Proof-of-Stake (PoS), que pretende acelerar el proceso de consenso al proporcionar un medio para codificar el tiempo en sí mismo en la cadena de bloques.

Permite a los nodos de la red no sólo confiar en las marcas temporales (timestamps) de los bloques, sino también verificar criptográficamente el momento y orden de ocurrencia de los mensajes o eventos que tienen lugar en la red. De esta manera, se evita que los validadores tengan que comunicarse entre sí para acordar qué ha pasado en la red en el tiempo, evitando los cuellos de botella del método Proof-of-Work (PoW) y reduciendo notablemente el tiempo de consenso.

Un año más tarde, Anatoly contrató a su ex colega de Qualcomm, Greg Fitzgerald, como ingeniero principal de Solana para codificar la red blockchain en el lenguaje de programación Rust. El documento técnico oficial y la red de prueba interna del proyecto se publicaron en febrero de 2018, seguidos de múltiples fases de red de prueba que llevaron al lanzamiento final de su red de prueba incentivada en 2020.

La versión beta de la red principal de Solana se lanzó en marzo de 2020, después de lo cual el proyecto (entonces llamado Loom) abrió sus puertas a varios otros ex empleados de Qualcomm, incluido Stephen Akridge como cofundador.

El algoritmo PoH de Solana utiliza criptografía para establecer una fuente de tiempo confiable para el sistema mientras mantiene el grado de descentralización de la red. Ofrece un registro inmutable de eventos anteriores en la cadena de bloques, lo que facilita el almacenamiento cronológico de datos históricos. Sin embargo, esto no se limita solo al seguimiento de marcas de tiempo y zonas horarias locales.

Sin duda, Solana es rápida e increíblemente segura, pero su grado de descentralización aún está en debate. Los comentaristas han destacado repetidamente el hecho de que el costo de ejecutar un nodo Solana es mucho más alto que otros. Para convertirse en validador en Solana, una persona necesitaría desembolsar miles de dólares en hardware, a diferencia de otras cadenas de bloques en las que cualquiera puede convertirse en validador por mucho menos.

Sin lugar a dudas, el token SOL y su apreciación salvaje en valor probablemente desempeñaron un papel importante para atraer inversores a la red. En el frente del desarrollo, Solana está viendo una adopción mucho más amplia que muchos otros proyectos de blockchain en etapas similares de su evolución.

BINANCE

Binance

Binance es la plataforma número uno de intercambio centralizados de criptomonedas en el mundo famosa por ofrecer transacciones rápidas y bajas tarifas de comisión. La plataforma de cambio es propiedad de la compañía Binance LTD, con sede en Malta. Binance ofrece el intercambio de más de 150 monedas digitales diferentes.

Binance fue desarrollado por Changpeng Zhao, un programador informático chino- canadiense, en 2017.

Changpeng Zhao, conocido como CZ, es un emprendedor que ha triunfado en impresionante número de start-ups. En julio de 2017 lanzó Binance y en 180 días, consiguió que se convirtiera en el mayor Exchange de criptomonedas del mundo. CZ, un experto en la blockchain y los sistemas de trading, ha logrado que Binance sea el ecosistema de blockchain líder, compuesto por Binance Exchange, Labs, Launchpad, Info, Academy, Research, Trust Wallet, Charity y NFT, entre otros. CZ pasó su juventud trabajando en restaurantes de comida rápida antes de estudiar en la McGill University de Montreal. En 2005, CZ dejó su puesto al frente del equipo de desarrollo e investigación de futuros en Bloomberg Tradebook y se mudó a Shanghái para fundar Fusion Systems. Poco después, descubrió Bitcoin y se unió a Blockchain.com como director de tecnología. En 2020, CZ apareció en la lista Bloomberg 50 como una de las personas más influyentes del año

BINANCE

Ecosistema Binance

Binance Exchange:
Es el mayor exchange de criptomonedas en términos de volumen de trading de activos de digitales Actualmente, cuenta con más de 13 millones de usuarios en todo el mundo. Esto significa que hay un gran número de personas que confían y usan Binance para sus transacciones criptográficas.Binance calcula su volumen de capital promedio diario usando la información disponible en su sitio web. Esto muestra un promedio de más de $6 mil millones de dólares en capital disponible cada 24 horas. La plataforma de Binance se puede utilizar desde el sitio web de Binance.com o por medio de la App que está disponible desde playstore o appstore.

-**BNB Chain:**
BNB Chain es un sistema de software de blockchain impulsado por la comunidad que cuenta con desarrolladores y colaboradores de todo el mundo. BNB Chain es una blockchain de código abierto desarrollada por la compañía Binance. Está diseñada para proporcionar una plataforma escalable para los contratos inteligentes, aplicaciones descentralizadas (dApps) y soluciones de intercambio de criptomonedas con alta disponibilidad y rendimiento. Binance Chain, la red de Binance, tiene actualmente más de 20 nodos principales distribuidos alrededor del mundo. Estos nodos se conocen como Binance Nodes y son responsables de validar y autorizar transacciones en la red Binance Chain.

BNB Chain, es una de las cadenas de bloques más populares del mundo, se dedica a brindar su infraestructura central para la futura adopción pública y siempre se mantiene como un ecosistema de código abierto y de comunidad primero construido en un entorno descentralizado y sin permisos.

BINANCE

BNB Chain se compone de dos cadenas de bloques: BNB Beacon Chain (BC) y BNB Smart Chain (BSC).

La cadena BNB Beacon chain es el componente de la cadena de bloques, responsable de la gobernanza de la cadena BNB y gestiona la apuesta y la votación en la cadena BNB. Mientras que BNB Smart Chain es el componente de blokchain que es compatible con EVM, capas de consenso y con centros para cadenas múltiples en BNB Chain.

Características Beacon Chain:

-Envío y recepción de BNB y activos digitales.
-Emisión de nuevos activos digitales (un estándar llamado BEP-2 y BEP-8)
-Mint/quemar, congelar/descongelar, bloquear/desbloquear activos digitales.
-Gobernanza para Beacon Chain y Side Chains
-Replanteo de cadenas laterales
-Transferencias y comunicaciones entre cadenas
-Beacon Chain también incluye esfuerzos para implementar listados de activos de otras cadenas.

BNB Smart Chain es una solución innovadora para brindar programabilidad e interoperabilidad a Beacon Chain. Se basa en un sistema de con consenso de Prueba de autoridad estacada (PoSA) que puede admitir un tiempo de bloque corto y tarifas más bajas. Con candidatos validadores de staking más vinculados se convertirán en validadores y producirán bloques.

También admite contratos y protocolos inteligentes compatibles con EVM. La transferencia entre cadenas y otras comunicaciones son posibles gracias al soporte nativo de interoperabilidad.

BINANCE

BNB Smart Chain es una solución innovadora para brindar programabilidad e interoperabilidad a Beacon Chain. Se basa en un sistema de con consenso de Prueba de autoridad estacada (PoSA) que puede admitir un tiempo de bloque corto y tarifas más bajas. Con candidatos validadores de staking más vinculados se convertirán en validadores y producirán bloques. BNB Smart Chain también admite contratos y protocolos inteligentes compatibles con EVM. La transferencia entre cadenas y otras comunicaciones son posibles gracias al soporte nativo de interoperabilidad.

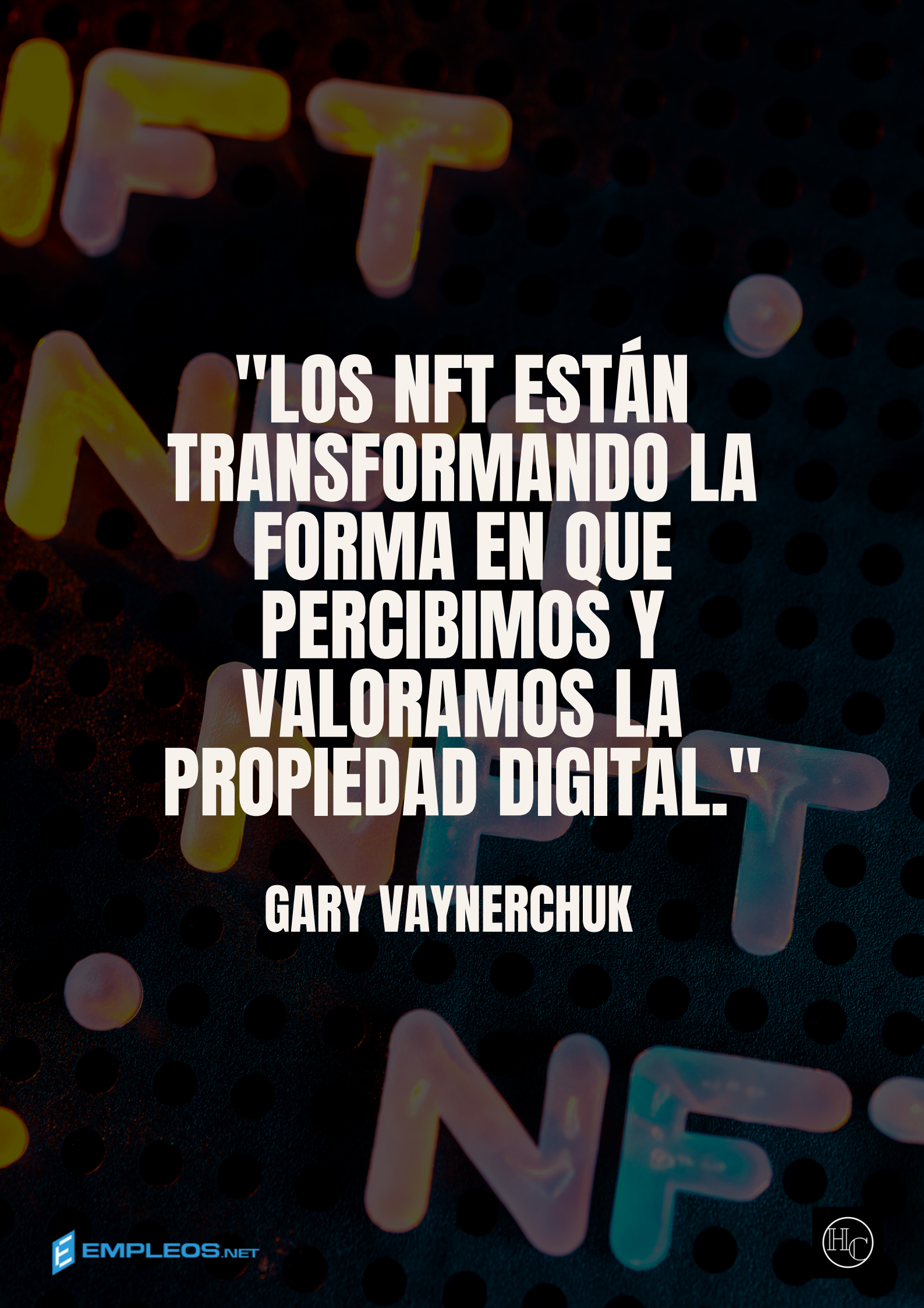
La Cadena Inteligente BNB

-**Una cadena de bloques autónoma**: brinda seguridad y protección con validadores elegidos.

-**Compatible con EVM**: admite todas las herramientas de Ethereum existentes junto con una finalización más rápida y tarifas de transacción más económicas.

-**Interoperable**: Viene con una eficiente comunicación nativa de doble cadena; Optimizado para escalar dApps de alto rendimiento que requieren una experiencia de usuario rápida y fluida.

-Distribuido con gobernanza en cadena: Prueba de autoridad estacada (PoSA) trae descentralización y participantes de la comunidad. Como token nativo, BNB servirá tanto como gas de ejecución de contratos inteligentes como tokens para staking


"LOS NFT ESTÁN TRANSFORMANDO LA FORMA EN QUE PERCIBIMOS Y VALORAMOS LA PROPIEDAD DIGITAL."
GARY VAYNERCHUK

EMPLEOS.NET

CAPÍTULO 8: TOKENS Y NFT

Los tokens

Los tokens o fichas son abstracciones basadas en blockchain que funcionan como la representación de una variedad o derechos cuya propiedad puede ser gestionada y transferida.

Un token puede servir para otorgar un derecho, para pagar por un trabajo o por ceder unos datos, como incentivo, como puerta de entrada a unos servicios extra o a una mejor experiencia de usuario, servirá para aquello que la persona u organización que lo diseñe y desarrolle decida.

La tokenización es el proceso de definir y crear fichas virtuales junto con la posibilidad de poder operar con ellas digitalmente. Es tomar cualquier activo, tangible o intangible fragmentarlo virtualmente en pedacitos, asignar esos pedacitos virtuales de manera irreversible a transacciones en una cadena de bloques y vincularlos con contrato inteligentes que describen el activo y los derechos que otorga su posesión.

Los tokens empresariales pueden ser la una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas.

El token permite al usuario de la plataforma llevar a cabo acciones que benefician al negocio directa o indirectamente. El token puede representar cualquier tipo de valor, ya sea un activo, un servicio u otro.

TOKENS

Características de los tokens

-Carecen de valor alguno: Los tokens no tienen ningún valor, puesto que son creaciones sin ningún tipo de valor. Si hay que considerar que algunos tokens según su tipo, características y cualidades pueden tomar valor a través del tiempo según el mismo uso y valor que los usuarios le van dando y también el desarrollo del proyecto del cual está basado el token.

-Son emitidos por privados: La emisión de los tokens es generalmente realizada por una persona o empresa. El respaldo y aceptación de estos tokens para realizar intercambios está supeditado a quienes emiten el token.

-Son creados usando materiales de muy poco valor: Desde el origen de los mismos, los tokens fueron acuñados en materiales de muy poco valor. Después de todo, nadie querría usar oro o plata para emitir un token de limitado uso. En el caso de los tokens digitales criptográficos, emitir un token es tan sencillo y barato como ejecutar un programa.

-Siguen una reglamentación del emisor: Quienes emiten un token crean una serie de reglas que permiten realizar operaciones e intercambios de los tokens por bienes, servicios o dinero de curso legal. En el caso de los tokens digitales criptográficos, estas reglas y funcionamiento están controladas por la blockchain donde se ejecutan. Así como el contrato o programación que da origen al token mismo.

-Son seguros y no falsificables: Esta característica aplica solo al caso de los tokens digitales criptográficos y es una característica que heredan de la blockchain.

TOKENS

Tipos de tokens

-Security token: Es un tipo de token digital criptográficos que está vinculado a los valores financieros tradicionales. Entendiendo por valor tradicional, cualquier activo financiero intercambiable como lo son los bonos, los swaps o los futuros. un security token representa estos activos dentro de una blockchain. El fin de esto es permitirles a las empresas un control descentralizado de los mismos, además de una mayor seguridad, reducción de costos y un manejo más sencillo

-Utility token: Es un tipo de token utilitario que le permite a todo aquel que tenga uno en su poder, acceder a productos y servicios que son prestados por un privado.

-Equity token: Es un tipo de token similar a los security token pero las regulaciones para estos son más flexibles, funcionan como una representación digital de un activo de acciones tradicional.

Plataformas famosas de tokens

Bitcoin

La blockchain y criptomoneda que empezó la revolución, es también una de las plataformas más usadas para crear tokens. Las conocidas colored coins, son el ejemplo más claro de la implementación de tokens sobre Bitcoin.
Una colored coins es un token especial que funciona sobre la blockchain de Bitcoin. Dicho token basa su funcionamiento y control a una programación especial realiza en lenguaje Bitcoin Script. Dicha programación es controlada por una serie de nodos y monederos diseñados para mantener a la colored coin. Como resultado, se es capaz de generar un nuevo token cuyo funcionamiento y contabilidad están sobre la blockchain de Bitcoin, pero es distinto a la criptomoneda bitcoin

TOKENS

Ethereum

La blockchain Ethereum es la blockchain con el mayor número de tokens ejecutándose sobre ella. Ethereum fue creado con el fin de convertirse en una plataforma para desarrollar tokens. Esto lo vemos claramente en la creación de estándares como el token ERC-20, el cual facilita enormemente la tarea de crear y desplegar un token criptográfico.

Protocolo ERC-20

Es un protocolo para la emisión de monedas basadas o respaldas en la plataforma de contratos inteligentes de Ethereum. El ERC-20 fue creado para facilitar a los desarrolladores la creación de nuevos tokens sin tener que empezar de nuevo cada vez.

El protocolo ERC-20 tiene funciones que muestran cómo se pueden transferir los tokens y la forma de acceder a los datos que tienen relación con los tokens. Su nombre significa, Ethereum Request For Comments o dicho en español, Solicitud de Comentarios de Ethereum y el número 20 se establece como una identificación estándar para diferenciarlo del resto de los tokens.

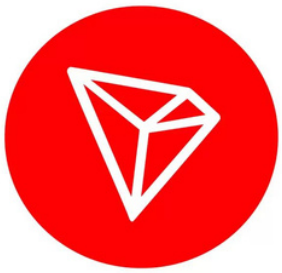
Eos

Un sistema operativo hecho para que las empresas construyan aplicaciones Blockchain como reemplazo de aplicaciones web, al tiempo que conservan principios estructurales similares. primero es la ausencia de tarifas de transacción y la segunda ventaja es la escalabilidad

TOKENS

Tron

Es una fundación que se estableció para proporcionar el desarrollo y mantenimiento de la red distribuida de TRON (TRX) Trom busca convertirse en una plataforma descentralizada para la industria del entretenimiento digital. Sus características principales se centran en la distribución justa
de recompensas y derechos para los desarrolladores de contenido



Waves:

Waves es una plataforma de Blockchain desarrollada para ofrecer a los usuarios la oportunidad de crear su propio token personalizado. Estos tokens se pueden usar para programas de lealtad, creación de moneda en la aplicación y para la fundación de ICO.

NFT

Tokens no fungibles (NFT)

Los tokens no fungibles (NFT) son elementos digitales únicos con propiedad administrada por la tecnología blockchain. Los ejemplos incluyen coleccionables, artículos de juegos, arte digital, boletos para eventos, nombres de dominio e incluso registros de propiedad de activos físicos. Algo fungible es algo que puede ser reemplazado por otro elemento idéntico y alfo no fungible, es algo único y no pueden ser reemplazado.

Tokens no fungibles basados en blockchain

Las cadenas de bloques proporcionan una capa de coordinación para los activos digitales, lo que les otorga a los usuarios permisos de propiedad y administración. Las cadenas de bloques agregan varias propiedades únicas a los activos no fungibles que cambian las relaciones entre el usuario y el desarrollador con estos activos.

Características de los NFT

Interoperabilidad

Los estándares de tokens no fungibles permiten que los tokens no fungibles se muevan fácilmente a través de múltiples ecosistemas. Cuando un desarrollador lanza un nuevo proyecto de NFT, estos NFT se pueden ver inmediatamente dentro de docenas de diferentes proveedores de billeteras, se pueden negociar en los mercados y se pueden visualizar dentro de los mundos virtuales. Esto es posible porque los estándares abiertos proporcionan una API clara, consistente, confiable y autorizada para leer y escribir datos.

Comerciabilidad

Por primera vez, los usuarios pueden mover artículos fuera de sus entornos originales y entrar en un mercado donde pueden aprovechar las capacidades comerciales sofisticadas, como subastas al estilo de eBay, licitación, agrupación y la capacidad de vender en cualquier moneda, como monedas estables y monedas específicas de la aplicación.

NFT

Liquidez

La comerciabilidad instantánea de los tokens no fungibles conducirá a una mayor liquidez. Los mercados de NFT pueden atender a una variedad de audiencias, desde traders incondicionales hasta jugadores más novatos, lo que permite una mayor exposición de los activos a un grupo más amplio de compradores.

Inmutabilidad y escases

Los contratos inteligentes permiten a los desarrolladores poner límites estrictos al suministro de tokens no fungibles y hacer cumplir las propiedades persistentes que no se pueden modificar después de que se emiten las NFT.
Los desarrolladores también pueden exigir que las propiedades específicas no cambien con el tiempo al codificarlas en cadena. Esto es particularmente interesante para el arte, que se basa en gran medida en la escasez demostrable de una pieza original

Programabilidad

Al igual que los activos digitales tradicionales, las NFT son totalmente programables, tienen mecánicas más complejas, como forjar, crear, redimir, generar aleatoriamente, etc. El espacio de diseño está lleno de posibilidades.

NFT

Cómo funcionan los NFT

Los NFT otorgan la capacidad de asignar o reclamar el derecho de propiedad de cualquier pieza única de datos digitales, rastreable mediante el uso de la cadena de bloques como un registro público.

Un NFT se acuña a partir de objetos digitales como una representación de activos digitales o no digitales. Por ejemplo, un NFT puede representar:

Arte digital: Un GIF, Coleccionables, Música, Vídeos

Objetos del mundo real: Títulos de propiedad de automóviles, entradas para un evento en el mundo real, facturas tokenizadas, documentos legales, firmas.

NFT

Plataformas de NFT Open Sea

OpenSea:

Es un mercado en línea para tokens no fungibles es el primer y más grande mercado de NFT del mundo Fue fundado por Devin Finzer y Alex Atallah en Nueva York el 20 de diciembre de 2017.

Los usuarios pueden generar NFT de forma gratuita en OpenSea y ofrecerlos para compra directa o subasta. OpenSea se basa en el estándar Ethereum ERC-721 y Polygon (una solución de escalado de capa 2 para Ethereum).

El sitio oficial es opensea.io y se pueden encontrar NFT´s relacionados al arte, coleccionables, nombres de dominio, música, fotografía, deportes, tarjetas coleccionables, utilidad y mundos virtuales.

También se puede llevar un seguimientos del ranking y volúmenes de todos las categorías.

OpenSea

Actualmente las mejores colecciones y más populares de Open Sea son:

CryptoPunks

CryptoPunks se lanzó en junio de 2017 como uno de los primeros tokens no fungibles en la blockchain de Ethereum. El proyecto fue desarrollado por el estudio estadounidense Larva Labs, un equipo de dos personas formado por los desarrolladores de software canadienses Matt Hall y John Watkinson.

10 000 personajes coleccionables únicos con prueba de propiedad almacenados en la cadena de bloques de Ethereum. El proyecto que inspiró el movimiento CryptoArt moderno.

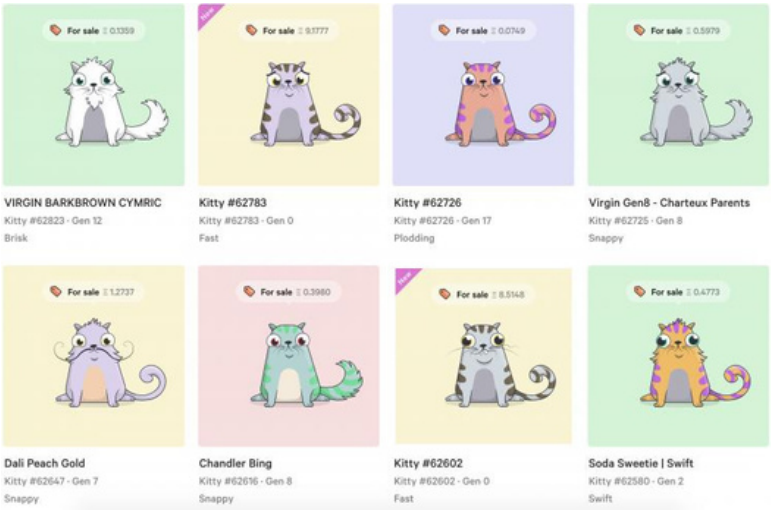
Los Cryptopunks son uno de los primeros ejemplos de un token no fungible en Ethereum, y fueron la inspiración para el estándar ERC-721 que impulsa la mayoría de los coleccionables y el arte digital. Los CryptoPunks son anteriores al estándar ERC-721 y son un contrato personalizado, lo que significa que no cumple con ningún estándar. Son casi un token ERC20 . Admitimos los métodos que proporcionan su saldo para que pueda ver CryptoPunks como un token en su billetera y ver cuántos posee. Su sitio oficial se puede encontrar www.larvalabs.com/cryptopunks Actualmente tienen un volumen negociado de 791.1 K Ether, el precio más bajo es de 68 Ether, y son los numero 6 en el ranking en los últimos 30 días en Open Sea.

OpenSea

CryptoKitties

Es un juego de blockchain en Ethereum desarrollado por Axiom Zen que permite a los jugadores comprar, recolectar, criar y vender gatos virtuales. Es uno de los primeros intentos de implementar la tecnología blockchain para la recreación y el ocio. La popularidad del juego en diciembre de 2017 congestionó la red Ethereum, lo que hizo que alcanzara un máximo histórico en el número de transacciones y lo ralentizó significativamente.

Su sitio web oficial es: www.cryptokitties.com y actualmente tienen un volumen negociado de 70.4 K Ether.

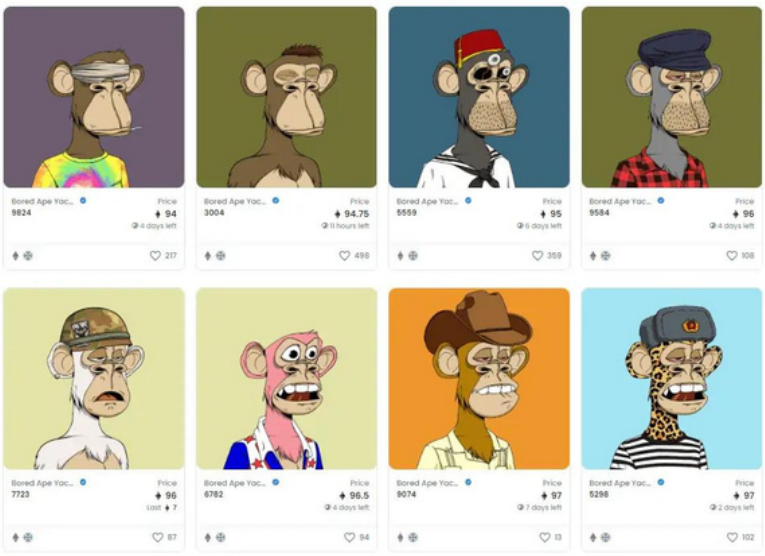


Bored Ape Yacht Club

Bored Ape Yacht Club (el yate de monos aburridos) es una colección de 10 000 NFT únicos de Bored Ape, coleccionables digitales únicos que viven en la cadena de bloques de Ethereum. Su Bored Ape funciona como su tarjeta de membresía del Yacht Club y otorga acceso a beneficios exclusivos para miembros, el primero de los cuales es el acceso a THE BATHROOM, un tablero de grafiti colaborativo. La comunidad puede desbloquear áreas y ventajas futuras a través de la activación de la hoja de ruta. El sitio web es www.BoredApeYachtClub.com

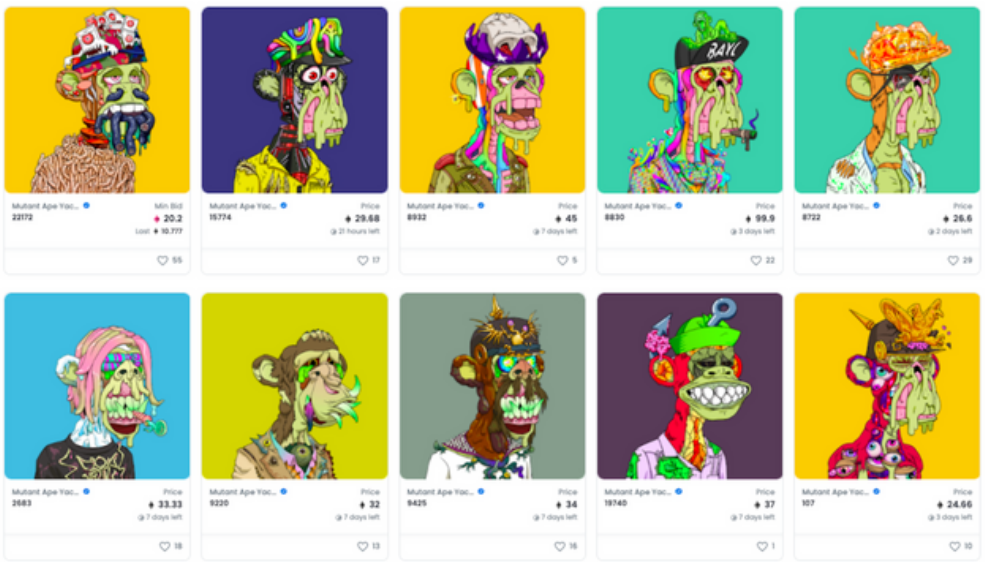
OpenSea

Actualmente tienen un volumen negociado de 337.1 K Ether, el precio más bajo es de Ether, tiene 6.2 k de dueños y son los numero 1 en el ranking en los últimos 30 días en Open Sea.



Mutant Ape Yacht Club

El Mutant Ape Yacht Club es una colección de hasta 20 000 Mutant Ape que solo se pueden crear exponiendo un Bored Ape existente a un vial de mutant serum o acuñando un Mutant Ape en la venta pública. Actualmente tienen un volumen negociado de 201.7 K Ether, el precio más bajo es de 15.99 Ether, y son los numero 2 en el ranking en los últimos 30 días en Open Sea.



OpenSea

The Sandbox

The Sandbox es un videojuego para iOS y Android que se lanzó por primera vez el 15 de mayo de 2012. Fue desarrollado por Pixowl y asumido por Animoca en 2018. Sandbox es miembro de Blockchain Game Alliance.
En agosto de 2018, Animoca se hizo cargo del juego por $ 4,875 millones. Se planea una versión 3D similar a Minecraft para Windows, en la que los usuarios pueden intercambiar productos en el juego con la moneda SAND o LAND en forma de Non-Fungible Tokens, ERC-721) a través de blockchain.

El 5 de diciembre de 2019, todas las unidades virtuales de preventa de LAND se vendieron en 4 horas. Entre el 19 de julio y el 19 de septiembre de 2019, Para junio de 2020, se habían vendido $ 1 millón en tierras virtuales.

Sandbox es una plataforma impulsada por la comunidad donde los creadores pueden monetizar activos y experiencias de juego en la cadena de bloques. El metaverso Sandbox comprende un mapa formado por 166.464 tierras. Los propietarios de LAND pueden organizar concursos y eventos, apostar SAND para ganar y personalizar activos, monetizar activos y experiencias, votar en el gobierno del metaverso, jugar juegos creados por usted u otros.

SAND es el token nativo de The Sandbox y actualmente tiene un valor de $3.13 cada token, El ranking actual de CoinMarketCap es el # 43, con una capitalización de mercado en vivo de $2,896,131,356 USD. Tiene un suministro circulante de 925,054,385 monedas SAND y un máx. suministro de 3.000.000.000 monedas SAND.

SAND es un token ERC-20 que permite realizar transacciones dentro de The Sandbox. ... Por ejemplo, un usuario puede usar los tokens SAND para acceder a mini-juegos dentro de The Sandbox, comprar equipos y mejorar sus personajes.

OpenSea

LAND es una pieza digital de bienes raíces en el metaverso de The Sandbox. Los diseñadores de juegos usan LAND para crear experiencias digitales, como juegos o dioramas, y también lo pueblan con ACTIVOS.

Cada LAND es un token ERC-721 único y no fungible en la cadena de bloques de Ethereum. Habrá un total de 166.464 LAND disponibles.

Se pueden combinar varios terrenos para formar estados un tipo especial de patrimonio propiedad de más de una persona se denomina distrito.
Se puede acceder a land a través de un mapa virtual en el sitio web oficial de the sandbox. La proximidad de los land a grandes socios y otras posiciones clave desempeñará un papel en la jugabilidad, el número de visitantes, la economía y la visibilidad de los juegos creados en esos land. También será posible alquilar land a creadores de juegos. los creadores de juegos también podrán colaborar con otros creadores o artistas de voxel para crear una gran experiencia en ese land. El terreno también se puede combinar en estados o distritos más grandes, siempre que sean adyacentes. alternativamente, los estados se pueden dividir en terrenos más pequeños.
Su sitio web oficial es es www.sandbox.game

Decentraland

Decentraland es una plataforma de realidad virtual descentralizada 3D que consiste en 90601 parcelas de tierra. La propiedad virtual en decentraland son los NFTs que se pueden comprar por medio de la criptomoneda MANA, que está basada en la Blockchain de Ethereum.

OpenSea

Cuando Decentraland se lanzó en versión beta en 2017, los desarrolladores vendieron paquetes de tierra virtual por tan solo $20; por otro lado, a raíz del boom en arte en NFT en 2020-2021, la propiedad más codiciada se estaba vendiendo por más de $100,000.

fue inaugurada de manera pública en febrero de 2020, y se es supervisada por la organización sin ánimo de lucro Decentraland Foundation.

Decentraland cuya finalidad es la creación de un mundo virtual abierto en el que sus usuarios puedan operar tal cual lo hacen en el mundo físico. Esto significa que son capaces de socializar, explorar y comerciar en dicho mundo virtual. Y, todo ello gracias a la tecnología blockchain, con la cual pueden crear avatares únicos de sí mismos, realizar compras y pagos entre pares

Su sitio oficial es decentraland.org

El MANA es el token de oferta limitada que sirve para adquirir estos Non-Fungible Tokens (NFT) de la plataforma, los cuales son parcelas de terrenos para construir y desarrollar dentro de la plataforma de Decentraland.

El precio de MANA es de $ 2.16 USD. El ranking actual de CoinMarketCap # 32, con una capitalización de mercado de $3,948,612,283 USD. Tiene un suministro circulante de 1,824,505,535 monedas MANA