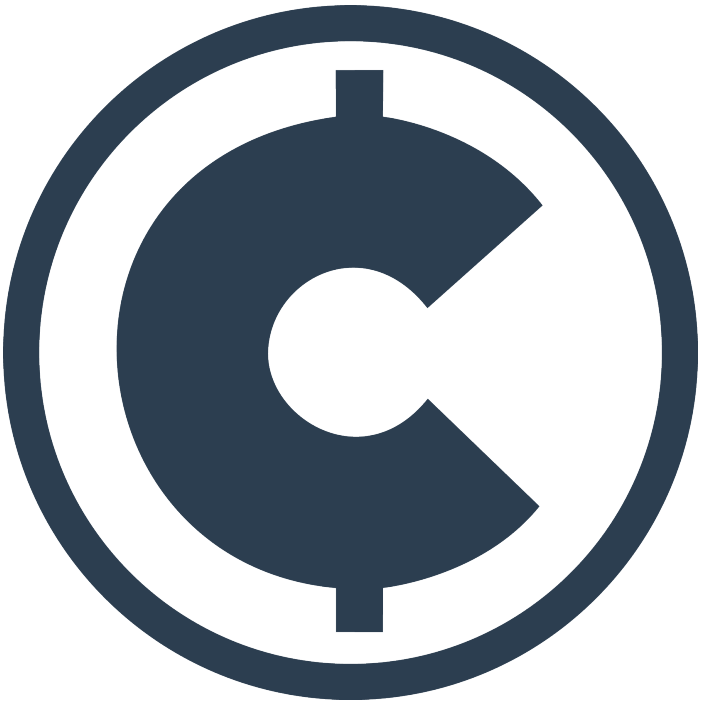
CRIPTOLOG



Glosario de términos Fintech

https://www.criptolog.com/

Índice

A	1
B	8
C	13
D	20
E	23
F	26
G	28
H	31
I	33
K	35
L	35
M	37
N	43
O	45
P	47
Q	52
R	54
S	56
T	60
U	62
V	64
X	65

A

Acortadores de Enlaces Web (Web Link Shorteners): Son aquellos servicio web que reducen la extensión de una URL con el fin de que el usuario lo pueda compartir con facilidad en las redes.

Acuerdos de Bretton Woods (Bretton Woods Agreements): Los acuerdos de Bretton Woods hacen referencia a las decisiones tomadas en la convención que en julio de 1944 reunió a 44 países bajo la Tutela de los Gobiernos de Estados Unidos y otros de Europa con el fin de establecer un nuevo modelo económico mundial de posguerra donde se fijarían las reglas de las relaciones comerciales y financieras entre los países más industrializados. Tuvieron lugar en el Hotel Mount de Bretton Woods, en el estado de New Hampshire (EEUU) durante los días del 1 al 22 de julio de 1944, en plena Guerra Europea, por tanto, no es de extrañar que se celebraran en suelo americano, viendo el panorama que asolaba Europa.

Con estos Acuerdos se logro:

- Sustituir el patrón-oro por un patrón-dólar vinculado al oro.
- La creación del Fondo Monetario Internacional (FMI).
- La creación del Banco Mundial.
- La creación a posterior de la Organización Mundial de Comercio.

A la Luna (To the Moon): Se dice cuando una divisa/criptodivisa va subiendo su valor muy rápidamente.

A la Mitad (Halving): Se refiere a la limitación en el suministro de Bitcoin, fijado en 21 millones, lo que lo convierte en un producto digital escaso. El número de bitcoins generados a través de la minería se reduce en un 50% cada cuatro años y bajo este esquema se calcula que el último de estos criptoactivos será creado en el año 2140. Para el caso de las demás criptodivisas los *halving* son etapas establecidas en el protocolo de cada criptomoneda, en la que se reducen los montos que se recibirán como recompensa por cada bloque resuelto.

A prueba de ASIC (ASIC Proof): Característica de los algoritmos de minado que los hacen ser resistentes al desarrollo de mineros ASIC.

Activo Digital (Digital Asset): Todo lo que existe en un formato binario y viene con el derecho de uso. Los datos que no poseen ese derecho no se consideran activos. Los recursos digitales incluyen, pero no son exclusivos de: documentos digitales, contenido audible, película y otros datos digitales relevantes que están actualmente en circulación o que están almacenados en dispositivos digitales.

Alegría de Quedarse Fuera (Joy Of Missing Out – JOMO): Se refiere al hecho de que, algunas veces, los inversionistas se alegran de no participar de determinada decisión de inversión.

Algoritmo (Algorithm): En el área informática es un conjunto de pasos y métodos lógicos que en una red informática sus participantes deben seguir para ejecutar un comando o resolver un problema.

Algoritmo de encriptación/cifrado (Encryption Algorithm): Es una función que transforma un mensaje en una serie ilegible aparentemente aleatoria, usando una clave de encriptación que puede ser revertida (es decir, obtener el mensaje original) sólo por quienes conocen dicha clave. Por medio de la encriptación, la información privada puede ser enviada públicamente por internet sin mayor riesgo de que otros puedan tener acceso a ella. En el ámbito blockchain se refiere a los métodos empleados por la minería para verificar transacciones. Algunos de ellos son:

- Blake2: Es otra función nueva de *hash*, y ofrece mucha mejor velocidad que SHA-2, lo cual significa menor tiempo de CPU "gastado" en criptografía y que la misma se puede desplegar económicamente en lugares donde antes no se podía. Actualmente BLAKE2 es una función hash criptográfica más rápida que MD5, SHA-1, SHA-2 y SHA-3, pero al menos es tan segura como la última SHA-3 estándar. BLAKE2 ha sido adoptado por muchos proyectos debido a su alta velocidad, seguridad y simplicidad. Está elaborada bajo las especificaciones RFC 7693, y su código y vectores de prueba están disponibles en GitHub, con licencia de CC0 (similar al dominio público). BLAKE2 viene en dos sabores: BLAKE2b (o simplemente BLAKE2) que viene está optimizado para plataformas de 64 bits, incluidos ARM habilitados para NEON, y produce resúmenes de cualquier tamaño entre 1 y 64 bytes y BLAKE2s que está optimizado para plataformas de 8 a 32 bits y produce compendios de cualquier tamaño entre 1 y 32 bytes. BLAKE2 incluye el BLAKE2bp paralelo de 4 vías y el BLAKE2sp paralelo de 8 vías diseñado para un mayor rendimiento en CPU multinúcleo o SIMD. BLAKE2 ofrece estos algoritmos adaptados a sus requisitos específicos, como el hashing con clave (es decir, MAC o PRF), hashing con saltos, hash de árbol incremental o actualizable, o cualquier combinación de los mismos. BLAKE2 también incluye las variantes BLAKE2x, que pueden producir compendios de longitud arbitraria. BLAKE2 brilla en las CPU de 64 bits: en un Intel Core i5-6600 (microarquitectura Skylake, 3310MHz), BLAKE2b puede procesar 1 gibibyte por segundo, o una tasa de velocidad de 3.08 ciclos por byte.

- ECDSA (**Algoritmo de Firma Digitalde Curva Elíptica / Elliptic Curve Digital Signature Algorithm):** es una variante del Digital Signature Algorithm (DSA) que utiliza la criptografía de curva elíptica (Elliptic curve cryptography – ECC) como variante de la criptografía asimétrica o de clave pública. La criptografía de curva elíptica puede ser más rápida y usar claves más cortas que los métodos antiguos como RSA, al tiempo que proporciona un nivel de seguridad superior.

- **CryptoNote y CryptoNight:** *CryptoNote* es un protocolo de capa de aplicación que hace funcionar múltiples monedas descentralizadas. Conceptualmente, es

una evolución de ideas que parten en Bitcoin, con similitudes y muchas diferencias en algunos respectos. La diferencia principal entre las dos tecnologías es que Bitcoin y la mayoría de las monedas digitales son más transparentes que las monedas basadas en el protocolo *CryptoNote* dado que estos *blockchains* son casi anónimos por completo. Las monedas *CryptoNote* utilizan un libro diario distribuido que guarda todos los balances y transacciones de sus monedas, como en Bitcoin. En diferencia, las transacciones *CryptoNote* no pueden ser seguidas por el blockchain de modo de poder revelar quien envía o recibe monedas. La cantidad aproximada de una transacción se puede saber, pero el origen, el destino, o la cantidad real no puede deducirse. La única información disponible es que la cantidad real enviada es menor a la que se muestra. Las únicas personas con acceso a toda la información son el que envia, el que recibe y una persona que pueda tener en su posesión una o ambas claves secretas. Otra diferencia significativa es el algoritmo de hashing para la prueba de trabajo (PoW). Bitcoin utiliza SHA256, el cual es un algoritmo que utiliza el CPU de manera intensiva. Esto quiere decir que los participantes (mineros) están solo limitados por sus velocidades de computo, y es relativamente barato crear circuitos especificos (ASIC) que sobrepasen la velocidad de un CPU de uso general como el que tiene cualquier computadora personal. *CryptoNote* utiliza una función que hace uso intensivo de memoria llamada *CryptoNight*, diseñada para ser usada en CPUs ordinarios de PCs, aun no existen dispositivos especiales para minar. *CryptoNight* depende en accesos aleatorios a memoria lenta y enfatiza la dependencia en la latencia al acceso de la información. Cada bloque depende de TODOS los bloques previos, el algoritmo requiere unos 2Mb por instancia: a) 2Mb pueden almacenarse en el L3 cache de un procesador moderno (o por core) b) 1Mb de memoria interna es inaceptable para los ASICs. c) Los GPUS pudiesen correr cientos de instancias en paralelo, pero están limitados de otros modos. La memoria GDDR5 es mucho más lenta que el L3 Cache de un CPU.

- **Equihash:** Equihash es un algoritmo de Prueba-de-Trabajo ideado por Alex Biryukov y Dmitry Khovratovich. Se basa en un concepto de ciencias de la computación y de criptografía llamado el Problema del Cumpleaños Generalizado. Equihash proporciona una verificación muy eficiente. Esto podría ser importante en el futuro para clientes ligeros en dispositivos restringidos o para implementar un cliente Zcash dentro de Ethereum (como BTC Relay, pero para Zcash). Equihash es una Prueba-de-Trabajo orientada a la memoria, lo que significa que la cantidad de minado que se puede hacer está determinada en gran medida por la cantidad de RAM que se tenga.

- **Ethash:** Es una mezcla de protocolos SHA3 más avanzados que los de Bitcoin (SHA2), y por ello más seguros. Este protocolo resiste el uso de ASIC debido a un aumento del requerimiento de memoria, lo que significa que la minería se hace imposible con dicho hardware. Ethash requiere de potencia de procesamiento y esto se consigue a través del hardware GPU o coloquialmente conocido como tarjetas gráficas. Este protocolo es nativo de la Criptodivisa Ethereum.

- **Groestl:** Es una repetitiva función de hasheo, donde la función de compresión se constituye de dos fijas, largas y diferentes permutaciones. El diseño de Grøstl es transparente y está basado en principios muy diferentes de los que usan la familia SHA. Las dos permutaciones utilizadas están echas usando la estrategia de diseño de rail ancho, que permite ofrecer estamentos fuertes sobre la resistencia de Grøstl ante amplias clases de ataques cryptoanaliticos. Se puede acelerar por el soporte de hardware AES presente en las más modernas CPUs Intel, las cuales ayudan a reducir la brecha entre las CPU y otras implementaciones. Ofrece una amplia gama de soluciones sobre el rendimiento, la latencia y el consumo de energía. Debido a esto, groestl utiliza menos energía por hash que otros debido a que el hasheo es menos complejo, groestl funciona bien en viejas GPU así como en CPUs. Este algoritmo es nativo de la Blockchain de la criptodivisa Groestlcoin.

- **LBRY:** Algoritmo usado por la Blockchain de la Critpdivisa LBC que ofrece La obtención de estas criptomonedas se realiza mediante PoW (Proof-of-Work) y PEW (Protocol Engineering Workbench) y mediante tres niveles de dificultad, determinados por el número de bloque minado.

- **Lyra2Rev2:** Algoritmo que permite la minería mediante su propio protocolo de consenso que emplea Prueba-de-Trabajo(POW), y permite minar eficientemente con GPU.
- **NeoScrypt:** Es un combinado de algoritmos de cifrado (Salsa20/20, ChaCha20/20, Blake2, etc) con un uso altamente intensivo de memoria que lo hace resistente a su descifrado con dispositivos ASIC. Las criptodivisas Phoenixcoin y Feathercoin utilizan NeoScrypt.

- **Quark:** Algoritmo nativo de la Blockchain de la criptodivisa Quark y el primero en implementar 9 rondas de algoritmos hash criptográficos de 6 funciones de hash (blake, bmw, grøstl, JH, keccak,skein) con 3 rondas donde se aplica una hash al azar , esto hace de Quark un protocolo único y seguro frente a la función de un solo hash que emplea Bitcoin (SHA-256). La función de algoritmos múltiples de Quark , además de mantener el blockchain seguro contra ataques de fuerza bruta que podría ser posibles en el futuro con la aparición de los ordenadores cuánticos, también ayuda a prevenir la minería usando hardware especializado que da una ventaja sobre los mineros de que utilizan simplemente CPUs. La minería de Bitcoin se hace actualmente en su mayor parte por empresas mineras dedicadas con grandes maquinas especializadas, negando el propósito de 1 voto por CPU que concibió originalmente el creador de Bitcoin. Empleando Quark todos en el mundo tendrá el mismo poder relativo en la red.

- RIPEMD-160 **(RACE Integrity Primitives Evaluation Message Digest):** Algoritmo usado donde se requiere un hash de menor longitud. Fue creado en 1996 y pertenece a la familia RIPEMD, de la que existen algoritmos con longitudes de salida de 128, 160, 256 y 320 bits. Bitcoin llegó a usar la versión de 160 bits, como SHA-1. La diferencia principal entre SHA y RIPEMD es que este último fue creado bajo los auspicios de una comunidad investigadora abierta en contraposición de SHA-1, que fue diseñado por la NSA.

- **Scrypt:** Algoritmo que tiende a utilizar menos de energía que el algoritmo SHA-256, gracias a eso, durante un tiempo, facilitó su uso por la mayoría de mineros individuales por GPU. En comparación con SHA-256, las tasas de hash de Scrypt para la minería oscilan entre los kilohashes por segundo (KH/s) y los megahashes por segundo (MH/s), que eran fácilmente alcanzables por las GPU's. Algunos argumentan que este sistema más simple es más susceptible a los problemas de seguridad, ya que los tiempos de respuesta de transacciones rápido puede significar que el sistema analiza más superficialmente los datos. Por el momento no existe noticia de que este algoritmo haya sufrido brechas de seguridad por eso. La proliferación de monedas Scrypt se debió en gran parte a que la dificultad de minado del bitcoin llego a unas tasas que no permitía su extracción por los mineros con pocos recursos.

- **SHA (Algoritmo de Hash Seguro / Secure Hash Algorithm):** SHA es una de las muchas funciones hash. Por ejemplo, SHA-256 es un hash de 64 dígitos hexadecimales (Tal como a continuación: bd4526534df7b33772c2f1ee26d97c39ff11379c8848e4e19d74ad849ef66423 (tamaño fijo de 256 bits /32 bytes. La familia es un sistema de funciones hash criptográficas relacionadas de la **Agencia de Seguridad Nacional de los Estados Unidos (NSA)** y publicadas por el **National Institute of Standards and Technology (NIST)**. El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores, SHA-1, SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos). SHA-0 y SHA-1 producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 264 bits. Y entre las aplicaciones de SHA-256 actualmente están: Un gran número de herramientas de seguridad y protocolos. Algunos de ellos son TLS, SSL, PGP, SSH, S/MIME, IPsec y Bitcoin. En el protocolo Bitcoin, SHA-256 se utiliza en la creación de claves o direcciones públicas y en la minería de Bitcoin. Sus defensores dicen que también es mejor para la seguridad de los datos en general. Para minar con éxito, este algoritmo requiere a menudo tasas de hash de de GH/S o incluso ya tasas más altas cómo los TH/S lo que hace más dificil que puedan participar en la minería los mineros individuales. Hoy por hoy, el minado mediante SHA-256 sólo tiene sentido mediante equipos ASIC.

- **X11:** El origen de su nombre son los 11 algoritmos de hash de la sphlib (conjunto de implementaciones de diversas funciones de hash). Fue creado por Evan Duffield, X11 consta de blake, bmw, groestl, jh, keccak, madeja, luffa, cubehash, shavite, SIMD, y el eco. Se utilizó por primera vez en Darkcoin , también creado por Duffield, pero despues ha sido utilizado en muchas otras monedas. Los mineros que extraen la GPU con el algoritmo X11 han visto reducciones drásticas en cuanto al consumo de energía de otros algoritmos (hasta un 50%) y la reducción de las temperaturas en comparación con el algoritmo scrypt. X11 se inspiró en la aproximación de encadenamiento de hashes de Quark, añadiendo una mayor "profundidad" y complejidad al número de hashes. Se diferencia de Quark en que la determinación de las rondas de hashes se realiza a priori en

lugar de elegir los hashes de forma aleatoria. El algoritmo X11 utiliza múltiples rondas de 11 hashes distintos, de ahí proviene su nombre, convirtiéndolo así en uno de los hashes criptográficos más sofisticados actualmente en uso de las divisas criptográficas modernas. Aunque compartan el mismo nombre, el servidor de la interfaz gráfica para sistemas Unix/Linux no tiene relación alguna con este algoritmo.

Algoritmo de Consenso (Consensus Algorithm): Es una serie de reglas para determinar que copia de la blockchain es válida y cuál no. Estas reglas se resumen básicamente en dos: La primera es que la cadena más larga que siempre se considerará más correcta y la blockchain con más bloques. Porque un "minero honrado" solo añadiría bloques a una cadena de bloques íntegra (en la que no hay discrepancias). Y la segunda es que se considerará a la cadena de bloques con más apoyo como "válida", es decir, la blockchain que mayor apoyo tenga entre los miembros de la red será la correcta. Precisamente la forma de medir "el apoyo a la red" es el factor de diferenciación básico entre los algoritmos de consenso Proof of Work (POW) y Proof of Stake (POS).

Almacenamiento en Frío (Cold Storage): La forma más segura de almacenar sus claves privadas es manteniéndolas fuera de línea en "almacenamiento en frío". Esto podría ser en forma de billetera de hardware, memoria USB o billetera de papel. Estas billeteras se conocen como "Billeteras frías".

Altura del Bloque (Block Height): Cantidad de bloques que preceden a otro en una plataforma blockchain.

Análisis Fundamental (Fundamental Analysis): Es un método para evaluar la seguridad de determinada inversión a fin de medir su valor intrínseco, a través del examen de factores cualitativos y cuantitativos relacionados.

Apalancamiento (Leverage): Uso de capital prestado, generalmente por casas de cambio, para potenciar las posibles ganancias. En el mercado de criptomonedas se consiguen tasas de apalancamiento de 2 a 5 veces la inversión en casas de cambio como Kraken o Poloniex.

Ataque de 51% (51% Attack): Se trata del uso del 51% de la potencia de cálculo en una red para discriminar cuáles transacciones van a ser procesadas. Es común que estas transacciones privilegien los intereses de un grupo que posee tal poder de procesamiento de la red. En teoría, un ataque informático que pudiera ser perpetrado por una entidad o grupo de minería que posea la mayoría del procesamiento de transacciones de la red blockchain (51% o más) para prevenir que nuevas transacciones se confirmen.

Ataque de Denegación de Servicio Distribuido – Ataque DSD (Attack Distributed Denial of Service – Attack DDoS): Ataque informático consistente en realizar peticiones sencillas a un servidor hasta saturarlo y afectar su disponibilidad.

Ave Temprana (Early Bird): se trata de aquellos inversionistas que compraron Bitcoin en los primeros años de su historia y que hoy día gozan de los beneficios de esa decisión.

Muchos de estos inversionistas compraron bitcoins por algunos centavos, y gracias al exponencial aumento del precio de este criptoactivo se han hecho millonarios.

B

Balanza de pagos (Balance of payments): La balanza de pagos es un documento contable en el que se registran operaciones comerciales, de servicios y de movimientos de capitales de un país con el exterior. La balanza de pagos es un indicador macroeconómico que proporciona información sobre la situación económica del país de una manera general. Es decir, permite conocer todos los ingresos que recibe un país procedentes del resto del mundo y los pagos que realiza tal país al resto del mundo debido a las importaciones y exportaciones de bienes, servicios, capital o transferencias en un período de tiempo. Dentro de la balanza de pagos de un país existen cuatro cuentas principales:

- **Balanza por cuenta corriente:** Esta balanza es la más importante ya es las que más se utiliza para conocer el estado de la economía de un país. Aquí se incluyen las importaciones y exportaciones de bienes y servicios, además de las rentas y transferencias. A su vez, se subdivide en cuatro subcuentas: balanza comercial, balanza de servicios, balanza de rentas y balanza de transferencias.
- **Balanza de cuenta de capital:** Se registran el movimiento de capitales, por ejemplo las ayudas que llegan del extranjero o la compra y venta de bienes que no son financieros.
- **Balanza de cuenta financiera:** Se recogen los préstamos que pide un país al extranjero, las inversiones o depósitos que los países extranjeros efectúan a un país.
- **Cuenta de errores y omisiones:** esta cuenta se incluye dada la dificultad de calcular con extrema precisión el total de exportaciones e importaciones de un país.

Cada una de estas balanzas dan un saldo independiente que puede ser positivo o negativo:

- **Superávit:** en el caso de que el saldo de un tipo de balanza sea positivo estaremos hablando de que la balanza está en superávit.
- **Déficit:** en el caso de que sea negativo.

Sin embargo, no se busca el equilibro de cada una de estas balanzas por sí solas, sino el equilibrio global de la balanza de pagos. Por consiguiente, la balanza de pagos siempre estará en equilibro, por ejemplo un déficit en la balanza por cuenta corriente será compensado con un superávit en la balanza por cuenta de capital. Ya que si un país tiene más compras que de ventas, el dinero lo debe obtener por algún lado, bien por medio de inversiones o préstamos extranjeros.

Ballena (Whale): Persona que tiene mucho dinero en una moneda o que tiene mucha cantidad de una moneda y con sus acciones financieras, especulativas o no, puede marcar una tendencia a la baja o alta de la misma u otras, para beneficio propio u ajeno.

Banco Internacional de Pagos de Basilea (Basel International Payment Bank): Fundado el 17 de mayo de 1930, el Banco de Pagos Internacionales (BPI) es la institución financiera internacional más antigua del mundo. Su sede se encuentra en Basilea (Suiza) y cuenta con oficinas de representación en Hong Kong y en Ciudad de México. Los empleados del BPI proceden de 61 países. El BPI cuenta entre sus miembros con 60 bancos centrales, que representan a países de todo el mundo y aproximadamente el 95% del PIB mundial. El BPI se organiza en tres grandes departamentos: dos de ellos realizan las dos actividades principales del BPI (Análisis de políticas y operaciones bancarias), y el tercero presta apoyo interno.

En sus reuniones bimestrales, que suelen celebrarse en Basilea, los Gobernadores y otros altos cargos de bancos centrales examinan los acontecimientos más recientes y las perspectivas para la economía mundial y los mercados financieros. En estas reuniones, se intercambian opiniones y experiencias sobre asuntos de especial interés y de máxima actualidad para los bancos centrales. Además, el Banco organiza otras consultas periódicas a las que asisten, según el caso, representantes de los sectores público y privado y del mundo académico. Estas reuniones permiten comprender mejor la evolución, desafíos y políticas que afectan a los diferentes países y mercados.

Quizá su principal tarea sea la de ser el Banco que está por encima de todos los Bancos Centrales del mundo. En este sentido, el BIP puede considerarse como un árbitro solucionador de conflictos entre Bancos Centrales, mediador entre las autoridades monetarias y políticas, diseñador de políticas monetarias conducentes a la estabilidad monetaria y financiera ó actuar como aval de operaciones financieras entre Bancos Centrales.

Pero cuando se fundó en el año 1930 en la ciudad suiza de Basilea con el objeto de recoger, administrar y distribuir los pagos anuales que el Gobierno de Alemania tenía que hacer a los ganadores de la I Guerra Mundial en concepto de reparaciones de guerra establecidas en el Tratado de Versalles, además de coordinar el dinero del préstamo que los Estados Unidos hicieron a Alemania en el marco del Plan Dawes y Young. por ende, este Banco fue creado por los gobernadores del Banco de Inglaterra y el Reichsbank en 1930 está protegido por un tratado internacional, por lo que el BPI y sus activos están legalmente fuera del alcance de cualquier Gobierno o jurisdicción. Es decir, el BPI es intocable.

Este papel original de gestor de las reparaciones de guerra dio paso al de garante y gestor de los acuerdos de Bretton Woods, diseñando la estrategia que debían seguir los Bancos Centrales para mantener fijos los tipos de cambio, la soberanía monetaria y el control de los flujos de capital. Tras la ruptura de los acuerdos de Bretton Woods (en 1971 Richard Nixon decretó la inconvertibilidad del dólar en oro, base de dichos acuerdos) el BPI se convirtió en el organismo diseñador de la nueva regulación financiera y, especialmente, las reglas para la Banca. Aquí es donde surgen las famosas regulaciones de Basilea.

Baño de sangre (Bloodbath): Hace referencia a cuando una determinada criptomoneda o la mayoría de las criptomonedas del mercado sufren una reducción considerable en su precio, reflejando valores en rojo en Coinmarketcap u otro sitio de estadísticas y gráficos.

Base de moneda (Coinbase): Entrada de las transacciones de generación de criptomonedas en los bloques de la blockchain realizada por el minero creador del último bloque y que puede contener texto arbitrario. La palabra Coinbase también es el nombre de una popular casa de cambio de criptomonedas.

Basura digital / Correo no deseado (Spam): Hace referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Bifurcación (Fork): Esto es, sencillamente, tomar una copia del código original de algo, por ejemplo una criptomoneda u otro programa (aplicación/software) y empezar a desarrollar implementaciones o proyectos propios a partir de allí. criptomonedas son, de hecho, software: programas informáticos. Y como todo software están propensos a sufrir cambios en pro de su mejoramiento; aunque, en su caso, esta propensión es mucho más elevada dado que se trata de software de código abierto. Esto quiere decir que, literalmente, cualquiera puede acceder a su código fuente y utilizarlo de forma libre. Así lo determinó desde un principio su gran creador, Satoshi Nakamoto, y de esa forma es que Bitcoin (y las demás criptomonedas) han logrado crecer hasta convertirse en lo que son hoy. Otros asocian este concepto a una versión alternativa realizada a otra cadena de bloques a la actual, que a veces puede originarse de forma maliciosa si un minero obtiene demasiado poder de cómputo, de forma accidental en caso de un error en el sistema, o de forma intencional si se introduce una modificación del protocolo. En este caso para que una bifurcación tenga éxito es necesario que cuente con el apoyo de suficientes mineros como para obtener la cadena más larga dentro de la cadena de bloques.

Bifurcación Dura (Hardfork): Modalidad de fork en el que el cambio aumenta los límites de código anterior. Crea una bifurcación y los clientes (mineros, nodos, monederos) que no actualicen el software no se podrán comunicar con los clientes que si actualicen.

Bifurcación Suave (Softfork): Modalidad de fork en el que el cambio reduce los límites de código anterior. No crea una bifurcación y los clientes que no actualicen el software aún podrán comunicarse con los clientes que si actualicen.

Bifurcación suave activada por el usuario – BSAU (User Activated Soft Fork – UASF): Es una bifurcación de la red activada por los nodos y sus clientes en lugar de por los mineros.

Billetera (Wallet): Dirección de blockchain que almacena, envía y recibe criptoactivos. Se accede a ella a través de interfaces digitales o físicas, desde dispositivos móviles, de escritorio, cajeros automáticos o en línea.

Billetera Caliente (Hot Wallet): Una billetera bitcoin que tiene una conexión activa a internet. Se utilizan para transacciones “cotidianas” y nunca deben contener grandes cantidades de bitcoin, ya que su conectividad reduce su seguridad.

Billetera Fría (Cold Wallet): Dispositivo de hardware diseñado para almacenar criptoactivos de forma segura y aislada de internet.

Bitcoin (con B mayúscula): Se utiliza para describir el concepto de Bitcoin, la totalidad de la red Blockchain que sustenta a la criptomoneda y el protocolo que se ejecuta sobre ella.
bitcoin (con b minúscula): Se refiere a la unidad de la criptomoneda basada en la red blockchain homónima, pudiendo ser usada en singular y en plural (bitcoin y bitcoins). Se abrevia como BTC, y a veces como XBT, aunque esta última ha entrado en desuso progresivamente. Es una moneda descentralizada, que no depende de la supervisión de ninguna autoridad central o institución. No la controla nadie en concreto, por eso se dice que la controlan todos los que participan en el sistema y nadie, a la vez. Es de código abierto y se identifica mediante códigos cifrados y anónimos (en vez de billetes y monedas). Permite registrar todo tipo de transacciones financieras con facilidad, en un entorno seguro y entre iguales, ya que usa tecnología “peer-to-peer” (P2P).

Bloque (Block): Cada una de las divisiones de la blockchain o cadena de bloques. Colección de transacciones (u otros datos) en un intervalo de tiempo determinado. En el bitcoin cada bloque contiene las transacciones realizadas durante 10 minutos.

Bloque Obsoleto (Obsolete Block): Bloque de información que no es parte de la red distribuida. Se crea cuando dos o más mineros producen bloques casi al mismo momento pero uno de ellos es propagado por la red con mayor rapidez y aceptado por los nodos, dejando fuera de la cadena a los demás.

Bloque Génesis (Genesis Block): Nombre dado al primer bloque creado y verificado de la blockchain de una criptomoneda.

Bloque huérfano (Orphan Block): Bloque que señala como bloque anterior a una dirección desconocida, siendo imposible validarlo.

Bloque recompensa (Reward Block): Beneficio que obtiene un minero por resolver con éxito un acertijo hash y crear un bloque. La red Bitcoin actualmente otorga 12,5 bitcoins por cada bloque minado. Esta recompensa se reduce a la mitad cuando se ha extraído un cierto número de bloques. En el caso de Bitcoin, el cambio se produce cada 210.000 bloques.

Bomba / Bombear (Pump): Realizar acciones financieras (especulativas o no) con el fin de subir el precio de una divisa / criptodivisa para obtener ganancias rápidas y fuera de lo normal o predecible.

Bombear y Vaciar (Pump & Dump): Realizar acciones financieras (especulativas o no) con el fin de subir y luego bajar el precio de una divisa / criptodivisa para obtener ganancias rápidas y fuera de lo normal o predecible.

BTC: Abreviatura para referirse a las unidades de bitcoins.

Bulla / Bullicio (Bull / Bullish): Señales de que una divisa / criptodivisa va a subir de precio.

Botón de madera (Buttonwood): Movimiento online fundado por el entusiasta Josh Rossi, que promueve el intercambio público y libre de bitcoins por dólares. Lleva el nombre del

acuerdo de Buttonwood, que fue un acuerdo fundamental para la Bolsa de Nueva York en 1792.

C

Cabecera de Bloque (Block Header): Componente de un bloque donde se incluye la siguiente información: versión del software de Bitcoin, Dirección Hash del bloque anterior, Árbol Merkle, hora o marca de tiempo, Objetivo de Dificultad, Número Nonce.

Cadena de Bloques (Blockchain): Nombre que recibe actualmente la tecnología Bitcoin y sus bifurcaciones, pero que se refiere específicamente a la secuencia de bloques que almacenan información y que han sido verificados por los usuarios de la red desde sus inicios. El término blockchain (cuya traducción literal es “cadena de bloques”) proviene del hecho de que cada bloque contiene un apuntador hash hacia su bloque predecesor, creando una red interconectada. Es importante destacar que existe una empresa de nombre Blockchain y cuyo principal producto es un explorador de bloques que posee el mismo nombre.

Cadena Lateral (Sidechain): Es una cadena de bloques que valida datos desde otra cadena de bloques a la que se llama principal. Su utilidad principal es poder aportar funcionalidades nuevas, las cuales pueden estar en periodo de pruebas, apoyándose en la confianza ofrecida por la cadena de bloques principal. Las cadenas laterales funcionan de forma similar a como hacían las monedas tradicionales con el patrón oro. Un ejemplo de cadena de bloques que usa cadenas laterales es Lisk. Debido a la popularidad de Bitcoin y la enorme fuerza de su red para dar confianza mediante su algoritmo de consenso por prueba de trabajo, se quiere aprovechar como cadena de bloques principal y construir cadenas laterales vinculadas que se apoyen en ella. Una cadena lateral vinculada es una cadena lateral cuyos activos pueden ser importados desde y hacia la otra cadena. Este tipo de cadenas se puede conseguir de las siguiente formas: Vinculación federada (Federated Peg) y Vinculación SPV (Simplified Payment Verification “SPV” Peg).

Cajero de criptomonedas (Cashier of cryptocurrencies): Cajero automático de criptomonedas. Es un dispositivo que permite canjear criptomonedas por dinero fiduciario en efectivo y viceversa.

Canal de pago (Payment Channel): Es un medio de transacción fuera de la cadena de bloques, en el que dos personas comprometen fondos en una dirección y se pagan entre ellas emitiendo compromisos de pagos firmados por las partes, evitando tener que esperar por confirmaciones de la blockchain subyacente. Las partes abren un canal de pago entre ellas enviando fondos en una transacción inicial (Transacción de fondeo) a una dirección multifirma 2 de 2, la cual es manejada por ambos involucrados y requiere las firmas de los dos para generar nuevas transacciones. Esta primera transacción es entonces propagada a la blockchain, quedando el canal efectivamente abierto. Para pagarse, las partes crean transacciones (Transacción de compromiso) desde la dirección multifirma, que no son difundidas en la red aún, y cuyos saldos consensuados, resultantes de operaciones fuera de red, son redimibles por las partes con o sin el permiso del otro y, de hacerlo, provoca el cierre del canal y la difusión de la transacción en la red blockchain. Abierto el canal de pago,

las partes pueden realizar transacciones entre ellos en cualquier momento a través del mismo (fuera de cadena). El canal puede permanecer abierto por cualquier cantidad de horas, días, semanas o décadas. La única vez que se vuelve a tocar la blockchain es cuando se cierra el canal, momento en el cual se registra el saldo final de las transacciones que ocurrieron a través del canal en la cadena de bloques.

Capitalización de Mercado / Capitalización Bursátil (Market Capitalization / MarketCap): Es una medida de una empresa o su dimensión económica, y es igual al precio por acción en un momento dado multiplicado por el número de acciones en circulación de una empresa de capital abierto, e indica el patrimonio disponible para la compra y venta activa en la bolsa. Al propietario de las existencias se representa como propietario de la empresa, incluidos todos sus activos. La capitalización puede representar a la opinión pública de una empresa y el patrimonio neto es un factor determinante en la valoración de existencias. Del mismo modo, la capitalización de los mercados de valores o regiones económicas pueden ser comparados con otros indicadores económicos. Cuanto mayor sea la capitalización, más capital con que trabajar tiene la empresa. En el ámbito de las Criptodivisa se refiere al monto total en unidades o valor de venta de una criptodivisa X disponible en el Mercado. Es decir, una capitalización de mercado significa lo grande que es el mercado de una criptomoneda en términos de dólares, euros, libras, etc. Se calcula tomando el número de monedas en circulación y multiplicándolo por el tipo de cambio del dólar, euro o libra.

Casa de cambio (Exchanger): Operadora cambiaria de monedas fiduciarias de curso legal y emisión oficial, y/o criptomonedas. Es decir, se trata de aquellas plataformas en donde se puede comprar o vender bitcoin o altcoins desde o hacia su banco de monedas fiat. Cada uno de estas casas de cambio cuenta con carteras internas, pero son los responsables de estas bolsas quienes tienen las llaves privadas de estas carteras, por lo que nunca es seguro utilizar estas carteras para almacenar las criptomonedas durante un período de tiempo prologado.

Casper: Protocolo consensuado en el que los nodos depositan una cantidad de criptoactivos garantes de su participación en el consenso y el procesamiento de bloques de una red. Si un nodo validador intenta aprobar algún bloque no aceptado por Casper, el depósito y la autorización para participar le son retirados al nodo.

Ciencia (Science): Es el conjunto de conocimientos que se organizan de forma sistemática obtenidos a partir de la observación, experimentaciones y razonamientos dentro de áreas específicas. Es por medio de esta acumulación de conocimientos que se generan hipótesis, cuestionamientos, esquemas, leyes y principios. La ciencia se encuentra regida por determinados métodos que comprenden una serie de normas y pasos. Gracias a un riguroso y estricto uso de éstos métodos, son validados los razonamientos que se desprenden de los procesos de investigación, dando rigor científico a las conclusiones obtenidas. Es por esto que las conclusiones derivadas de la observación y experimentación científica son verificables y objetivas.

Circuito Integrado de Aplicación Específica – CIAE (Application Specific Integrated Circuit Chips – ASIC): Es un chip diseñado para cumplir una tarea determinada. En el mundo de Bitcoin y las criptomonedas, es utilizado para resolver problemas de hashing y

así generar nuevas criptomonedas, es decir, procesar los algoritmos de la respectiva blockchain y confirmar las transacciones, lo que se conoce como "minería de criptomonedas. En el caso de Bitcoin, procesan el algoritmos SHA-256 resolviendo el hash de las transacciones para minar nuevas monedas.

Clave (Key): Conjunto de reglas y correspondencias que explican y descifran un mensaje cifrado.

Clave Criptográfica (Cryptographic Key): En la criptografía asimétrica el proceso de encriptación y desencriptación se hace con claves distintas. Con la clave pública se encripta y con la clave privada se desencripta.

Clave de Alerta (Alert Key): El software Bitcoin a partir de la versión 0.3.1 cuenta con un sistema de alerta que permite emitir mensajes críticos a todos los clientes bitcoin (nodos, monederos y mineros). Solo el dueño de la Clave de Alerta puede enviar estos mensajes.

Clave Privada (Private Key): Es un texto alfanumérico asociado matemáticamente a una dirección y que debe ser conocido sólo por el dueño de esa dirección.10 Para poder acceder a los bitcoins depositados en la dirección y disponer de ellos es necesario conocer la clave privada.

Clave Pública (Public Key): Es un texto alfanumérico del cual se obtiene una dirección conocida por todos los usuarios. Al ser conocida, cualquiera puede enviar bitcoins a la dirección asociada, pero sólo quien tenga la clave privada podrá acceder a ellos.

Cliente (Client): Aplicación de software que permite acceder a un nodo blockchain por medio de una interfaz y realizar transacciones, minería o almacenar información. Se dice que un Cliente es "ligero" cuando solamente descarga una pequeña porción de una blockchain, permitiendo ejecutar sus tareas sin consumir tanto espacio de memoria en su dispositivo.

Código o Fuente Abierta (Open Source): Se refiere al software distribuido y desarrollado libremente. Para muchos se reduce a software compartido gratuitamente, pero es mucho más que eso. Es libertad para modificar el código fuente sin restricciones de licencias.

Código Fuente (Source Code): El Código Fuente de un software son las "líneas de texto" que establecen los pasos que debe seguir un ordenador para ejecutar el programa.

Columpiarse / Balancearse (Swing Trading): Realizar muchas operaciones financieras (Trading) concretas en segundos o minutos con el fin de ganar dinero, sin importar lo poco que pueda hacerse en un periodo corto de días.

Colisión de Hash (Collision of Hash): Es cuando dos valores de entrada diferentes generan el mismo resumen. Una función hash debe ser resistente a la colisión. El mismo Hash siempre será el resultado de los mismos datos (funciones deterministas), pero la modificación de la información, aunque sea un solo bit dará como resultado un hash totalmente distinto. La idea básica de un valor Hash es que sirva como una representación compacta de la cadena de entrada para así demostrar la importancia de que todos los datos

de entradas sean iguales para llegar al mismo valor Hash y que esto de un efecto determinista.

Colusión (Collusion): Confabulación, complot. Termino referido a cuando una cantidad de participantes de la red actúan coordinadamente o conspiran para cambiar las normas de la blockchain a su beneficio propio. Guarda similitud con un ataque de 51% por ciento.

Comerciante (Trader): Persona o entidad que invierte en diferentes instrumentos financieros a corto plazo para conseguir un beneficio de forma rápida.

Comerciar (Trading): Inversión en diferentes instrumentos financieros a corto plazo para conseguir un beneficio de forma rápida.

Comisión / Tarifa (Fee): Monto que cobran las Casas de cambio (Exchanger) y los Mineros por efectuar o verificar una transacción.

Compatibilidad de Incentivo (Incentive Compatibility): Es un protocolo compatible con los incentivos si sus participantes se ocupan de seguir sus normas en lugar de intentar engañar a la red, a menos que se pongan de acuerdo para hacerlo.

Cómplice (Shill): Se trata de un aval público sobre los beneficios de cierta criptomoneda, generalmente realizado por comerciantes que compraron esa moneda y que tienen interés en posicionarla ante la opinión pública, a fin de despertar interés en torno a ella.

Compra en la jodida caída (Buy The Fucking Dip – BTFD): Resume uno de los principios básicos de la inversión en criptomonedas: cuando hay una baja importante y la mayoría de las personas decide vender por pánico a las pérdidas, es momento de comprar.

Computación (Computing): Se refiere al estudio científico que se desarrolla sobre sistemas automatizados de manejo de informaciones, lo cual se lleva a cabo a través de herramientas pensadas para tal propósito. La computación está referida a la tecnología en sí que permita el manejo y movilidad de información en cuanto a esta ciencia o conocimiento se refiere y también a los fundamentos teóricos de la información que procesan las computadoras, y las distintas implementaciones en forma de sistemas computacionales. El término computación tiene su origen en el vocablo en latín computatio. Esta palabra permite abordar la noción de cómputo como cuenta o cálculo, pero se usa por lo general como sinónimo de informática (del francés informatique). De esta manera, puede decirse que la computación nuclea a los saberes científicos y a los métodos.

Computador (Computer): También llamado Computador Personal (Personal Computer / PC) u Ordenador, se refiere a una máquina que está diseñada para facilitarnos la vida, mediante el uso de las tecnologías de la información y la comunicación (TIC). En muchos países se le conoce como “Computadora” u “Ordenador”, pero todas estas palabras se refieren a lo mismo. Pueden ser de “Escritorio”, “Portátiles” o “Portables”, tales como las Tabletas y los Celulares Inteligentes. Hay tres elementos básicos sin los cuales no podríamos tener un computador. Estos son: El o los discos que almacenan la información, la Unidad o Unidades que resuelvan y analicen cada una de las órdenes dadas, y los

elementos periféricos, que son los que completan las funciones más importantes de una computadora.

Comunicación (Comunication): Es la acción de comunicar o comunicarse, se entiende como el proceso por el que se trasmite y recibe una información. Todo ser humano y animal tiene la capacidad de comunicarse con los demás. Para que un proceso de comunicación se lleve a cabo, es indispensable la presencia de seis elementos: que exista un emisor; es decir, alguien que trasmita la información; un receptor, alguien a quien vaya dirigida la información y que la reciba; un contacto por medio de un canal de comunicación, que puede ser muy variado: el aire por el que circulan la sondas sonoras, el papel que sirve de soporte a la comunicación escrita, la voz, etc. El término comunicación procede del latín "communicare" que significa "hacer a otro partícipe de lo que uno tiene".

Confirmación (Confirmation): Confirmación de una transacción. Inclusión de una transacción en un bloque. Literalmente es la confirmación de la veracidad de una transacción de un minero, es decir, es la verificación por parte de los nodos de la red de que un bloque contiene únicamente transacciones válidas realizadas con criptomonedas que nunca antes habían sido usadas.

Confirmante (Confirming): Entidad o persona que es parcialmente propietaria de una cartera de criptoactivos.

Congelar (Freeze): Cambiar una criptodivisa a divisa (moneda) fiduciaria (fiat), como por ejemplo el Dólar o el Euro, para guardar el valor que tiene en ese momento y no perderlo si baja su valor. Entonces cuando "descongelas" puedes comprar mas. Otros hablan de congelar como dejar de Mercadear / Comerciar (Trading) y meter la moneda en una Billetera Fría (Cold Wallet).

Consenso (Consensus): Acuerdo alcanzado por la mayoría de nodos participantes de una red en cuanto al estado de esta y su protocolo.

Contraparte (Counterparty): Es otra capa de protocolo implementado sobre Bitcoin u otra criptodivisa. Permite crear y gestionar monedas de usuario, tokens negociables, instrumentos financieros, intercambios descentralizados de activos y otras características. Utiliza el token XCP para la realización de transacciones. Counterparty se implementa principalmente mediante el operador OP_RETURN. En otras palabras, Counterparty es una Metacoins. Específicamente, se trata de un protocolo basado en Bitcoin que ofrece distintos instrumentos financieros (o inclusive lúdicos) de forma totalmente descentralizada. Para ello utiliza el XCP, token combustible de la plataforma, que sirve como punto de partida a los usuarios, que también pueden crear su propia moneda digital en tan sólo unos momentos.

También se conoce como contraparte a la «otra» parte de la operación financiera. Por tanto, se denomina contraparte a cada uno de los participantes involucrados en la operación. Establecer un contrato con una contraparte entraña un riesgo de impago, que se conoce como "riesgo de contrapartida" que define el índice de probabilidades de que la contraparte no pueda cumplir con sus obligaciones contractuales en la fecha indicada, lo que imposibilitaría completar la transacción. Este riesgo a menudo puede evitarse mediante una cámara de compensación, que asume el riesgo de crédito de ambas partes implicadas en la

operación e identifica los requisitos de cada parte para asegurar la transacción y, en caso necesario, cubre el riesgo de impago de las partes.

Contrato directo o seguro de cambio (Contract Forward): es un acuerdo que asegura el tipo de cambio actual para una operación en una fecha futura determinada. Se trata de un instrumento simple pero efectivo para contrarrestar el riesgo de volatilidad del tipo de cambio. En efecto, se "fija" el tipo de cambio de hoy para una operación futura.

Contrato directo flexible o seguro de cambio flexible (Contract Forward Flexible): es un tipo de contrato directo o seguro de cambio cuya función es proteger a la empresa o particular que lo contrata de la volatilidad del tipo de cambio entre dos divisas durante un tiempo determinado. El contrato directo flexible se diferencia de un contrato directo estándar en que el comprador puede liquidar la operación en cualquier momento antes de la fecha de vencimiento del contrato.

Contrato de Garantía (Guarantee Contract): Contrato en el que dos partes colocan los fondos en una transacción de salida multifirma para evitar que ninguno gaste los fondos sin un previo acuerdo.

Contrato Inteligente (Smart Contract): Dirección de blockchain programada para ejecutar una tarea de acuerdo a las instrucciones previamente introducidas. Se trata de contratos cuyos términos se registran por medio de un lenguaje informático y pueden ser ejecutados automáticamente por un software determinado, registrando su ejecución en una blockchain. El cumplimiento de un contrato inteligente no está sujeto a la interpretación de las partes firmantes: si el evento A sucede, se pondrá en marcha un procedimiento B de manera automática.

Conozca a su cliente – CSC (Know Your Costumer – KYC): Se trata de un proceso mediante el cual las empresas o entidades que hacen un negocio o transacción deben identificar a la contraparte con la que realizan la misma. La finalidad es verificar la legitimidad y existencia del cliente.

Cripto Fondo de Inversión (Cripto Investment Trust): Fondo de inversión financiera cuyos activos capitales están basados en la criptomoneda, por lo general de Bitcoin.

Criptoactivo (Cryptoactive / Cryptoassets): Ficha criptográfica que es emitida y comercializada en una plataforma blockchain. El término se acuña y populariza ante la expansión de las rondas de financiamiento y venta inicial de monedas (ICO) y el establecimiento de las nuevas dinámicas financieras en las casas de cambio. Los criptoactivos son la forma en que se denomina al conjunto de las criptodivisas y otras formas de bienes y servicios que utilizan la criptografía (y por extensión la tecnología blockchain) para funcionar. Los más conocidos son las criptomonedas o criptodivisas, pero hay otros como contratos inteligentes, tokens o sistemas de gobernanza que entran en dicha categoría.

Criptodivisa (Cryptocurrency): Token digital que usa la criptografía como medio para identificar y asegurar datos. Estos tokens en su mayoría pretenden funcionar como moneda (divisa) u otra forma de almacenar valor. Se caracterizan y diferencian de las monedas

convencionales en la falta de organismo central (gobierno/banco) que la controle, y que se generan con la resolución de problemas matemáticos basados en criptografía. Su valor, no obstante, está sujeto a variación de precios dependiendo de la oferta y demanda en los mercados.

En resumen, las criptomonedas, como Bitcoin, son un tipo de moneda virtual que no tienen un emisor concreto, que están protegidas por criptografía y que en principio su coherencia puede estar protegida por una comprobación de sus usuarios masiva y distribuida. Por tanto, las criptomonedas son dinero virtual y digital. Pero al contrario que otras monedas virtuales, no tienen un control centralizado, sino que está distribuido y basado en criptografía para evitar la manipulación de alguno de sus miembros. Se puede concluir con que todas criptomonedas son moneda virtual y dinero digital, pero no viceversa. Cuando se habla de dinero digital se puede estar hablando de cualquier divisa del mundo (el euro y el dólar también), y cuando se habla de moneda virtual puede que no se trate de una criptomoneda, sino una moneda con un emisor concreto. Esperamos que los términos se usen correctamente en el futuro y no haya equívocos.

Por ultimo, toda criptodivisa (criptomoneda) es un token y/o un criptoactivo, pero no todo token y/o criptoactivo es una criptodivisa (criptomoneda).

Criptografía (Cryptography): Conjunto de técnicas y métodos matemáticos que protegen la información de los datos registrados en la blockchain, dotándolos de seguridad y garantizando su inmutabilidad. La Criptografía puede ser de 2 Tipos:

- **La criptografía de clave privada (simétrica)** que es donde el emisor puede generar un texto cifrado a partir de un texto en claro porque conoce la clave de cifrado, mientras que un atacante no puede invertir el proceso fácilmente y recuperar el texto en claro o la clave partiendo sólo del texto cifrado.

- **La criptografía de clave pública (asimétrica)** que es donde se generan un par de claves, pública y privada, pero dada la clave pública resulta computacionalmente muy costoso obtener la clave privada sin más o trampa. Del mismo modo, en la firma digital es muy fácil verificar una firma, pero resulta computacionalmente complejo falsificarla sin conocer la clave privada del firmante.

Este paradigma de “fácil de calcular, difícil de invertir” es tan común en criptografía que las funciones que tienen esta propiedad son denominadas funciones unidireccionales o de una sola dirección. La criptografía simétrica o de clave secreta y la criptografía asimétrica o de clave pública son funciones unidireccionales.

D

Dar la vuelta (Flipping): Es una estrategia para rotar la inversión en altcoins en una plataforma de trading, tratando de maximizar ganancias. El objetivo es estudiar los porcentajes de aumento de esas monedas, cambiándolas por aquellas que empiecen a mostrar picos de precio más atractivos.

Decred: Es un proyecto y plataforma criptomoneda construida desde cero para aprovechar la voluntad de sus constituyentes para impulsar el cambio. Este enfoque elimina los conflictos que surgen cuando entidades poderosas intentan ejercer control sobre una criptomoneda. Decred se adapta para satisfacer continuamente las necesidades de las personas a las que sirve.

Se dice que Decred es “La primera criptomoneda mundial del pueblo, para el pueblo y por el pueblo”. La mayoría de las criptomonedas se distinguen por la forma en que aseguran las transacciones en su red. Por ejemplo, Bitcoin es famoso por usar un algoritmo de prueba de trabajo que recompensa a los mineros por encontrar soluciones a un enigma de hash criptográfico. Otros proyectos de criptomonedas se basan en algoritmos de prueba de participación que premian a los usuarios que tienen la moneda en una cartera “participante” con interés sobre los saldos que llevan. Ambos enfoques tienen fortalezas y limitaciones; Decred aprovecha lo mejor de ambos mundos con un sistema de consenso híbrido de prueba de trabajo y de participación. Esto permite que la plataforma encuentre un equilibrio entre los beneficios tanto para los mineros como para las partes interesadas, dando lugar a una noción más sólida de consenso.

Deflación (Deflation): Reducción de los precios en una economía durante un período de tiempo determinado.

Delfín (Dolphin): Esta palabra hace referencia a determinado pequeño inversionista que ya ha alcanzado cierto renombre en la comunidad y que además tiene alguna influencia sobre el movimiento del precio de una criptomoneda determinada, aunque aún no puede ser considerado como Whale o Ballena.

Descentralización (Decentralization): Característica de los Sistemas que no dependen de un punto central o punto único para funcionar. Favorece la independencia y complica la censura y el control.

Desorden Obsesivo de Criptomonedas – DOC (Obsessive Cryptocurrency Disorder – OCD: Se trata de una “enfermedad” sufrida por aquellos que no pueden dejar de verificar el valor de sus monedas.

Dificultad (Difficulty): Número (Factor) que determina la complejidad del acertijo hash a resolver en cada bloque. Varía en función de la potencia de cálculo de los mineros en la red

y se ajusta automáticamente cada cierta cantidad de bloques minados. En el caso de Bitcoin, se ajusta cada 2016 bloques.

Dinero Digital (Digital Money): Es cualquier medio de intercambio monetario que se haga por un medio electrónico. Cuando se hace una transferencia de dinero desde una cuenta de un banco a otra, se está usando dinero digital. Cuando se paga con tarjeta en un comercio, también. Es decir, cuando se realiza un pago o envío de dinero sin intercambiar físicamente monedas o billetes, se está usando dinero digital. Prácticamente todo el dinero del mundo es digital, ya que el efectivo solo representa aproximadamente el 8% del dinero en circulación. Por tanto cuando alguien se refiere a dinero digital debería estar hablando, simplemente, de dinero. El dinero del día a día es digital. La gran mayoría de los asalariados del mundo cobra y paga en dinero digital. El dinero digital es dinero.

Dinero Efectivo (Cash): Se llama dinero efectivo al dinero en forma de monedas o papel moneda (billetes). Es la representación más líquida del valor económico. También es la forma (o una de ellas) más privada de valor económico.

Dinero Virtual (Virtual Money): Es aquel que no existe más que en su formato digital. Por ejemplo, en muchos videojuegos existe internamente una divisa con la que se pueden comprar objetos. Este dinero que se usa dentro del juego es virtual. También puede existir dinero virtual que no sea protagonista de un videojuego, por ejemplo alguna divisa creada por empresas o aficionados que pretendía sustituir el dinero físico actual por una nueva moneda alejada del control de los bancos centrales. Un ejemplo podría ser E-gold, que acabo cerrando por problemas legales. Por definición, las monedas virtuales son todas digitales. Como no existen físicamente, no hay papel moneda de las mismas, tienen que ser 100% digitales. Por tanto todas las monedas virtuales son digitales, pero no todas las digitales son virtuales (un ejemplo es una cuenta bancaria en euros, es digital pero no virtual).

Dirección de Billetera (Address Wallet): Secuencia de caracteres alfanuméricos que señala la ubicación de una Billetera a la que pueden enviarse la cantidad deseada de criptomonedas.

Divisa (Currency): Dinero. “Vale por” emitido por un gobierno y usado como medio de intercambio en cierta economía. Algunos ejemplos: Dólar, Euro, Yuan, Rublo, entre otros.

Divisa exótica (Exotic currency): Es una divisa exótica es aquella cuya liquidez y comercialización son escasas. La etiqueta de “exótica” no guarda relación con el país del que procede. La comercialización de una divisa exótica es un proceso a menudo costoso, puesto que su falta de liquidez se traduce en la aplicación de mayores spreads en el tipo de cambio. Las divisas exóticas pueden ser convertibles y no convertibles. Entre las divisas no convertibles se encuentran, por ejemplo, el real brasileño y el peso chileno. Una moneda exótica convertible es el peso mexicano. Las divisas exóticas más comercializadas son el peso mexicano (MXN); el rublo ruso (RUB); el dólar de Hong Kong (HKD); el dólar de Singapur (SGD); la lira turca (TRY); el won surcoreano (KRW); el rand surafricano (ZAR); el real brasileño (BRL); y la rupia india (INR).

Divisa parcialmente convertible (Partially convertible currency): Es la moneda de curso legal de un país que se comercializa en volúmenes limitados, debido a que las autoridades monetarias que la emiten restringen el comercio internacional de la divisa en el mercado mundial de divisas, a partir de un determinado volumen. Las divisas parcialmente convertibles forman parte, sin excepción, del grupo de divisas exóticas, aunque no todas las divisas exóticas tengan su convertibilidad limitada. La rupia india es un ejemplo de divisa parcialmente convertible. En función de la divisa, se aplican diferentes controles y niveles de restricción. Las divisas parcialmente convertibles normalmente pertenecen a países con economías débiles, cuyos gobiernos restringen su convertibilidad con el objetivo de proteger la estabilidad económica. En estos casos, las limitaciones del gobierno suelen incidir particularmente en lo relativo al volumen de transferencias al extranjero que se permiten.

Sin estas restricciones y con una economía frágil y fuertemente dependiente de un determinado sector, una potencial crisis económica podría provocar una mayor inestabilidad. La fuga de capitales, por miedo a una devaluación obligada provocaría la extinción de las reservas de divisa extranjera. Si la devaluación tiene lugar, se produciría un encarecimiento de las importaciones, lo que causaría un grave impacto en la inflación, y un deterioro general en la economía.

Divisa plenamente convertible (Fully convertible currency): También conocida como “divisa flotante” o “divisa flexible” es aquella que puede intercambiarse sin ningún tipo de limitación gubernamental. Las divisas convertibles son propias de países con economías estables, aunque hay algunas excepciones. Las principales divisas mundiales, tales como el dólar estadounidense, la libra esterlina, el franco suizo, el yen, el yuan y el euro, forman parte del grupo de divisas plenamente convertibles.

Dragado de Cenizas (Ashdraked): Se refiere a una situación en donde un poseedor de tokens pierde todo su dinero por un suceso en el ecosistema, bien sea un hackeo, una falla en el protocolo de su moneda o cartera, etc.

Doble Gasto (Double Expense): Acto de realizar dos pagos con una misma criptomoneda. Supone una operación fraudulenta y, aunque no resulta fácil de hacer en la red Bitcoin, se evita esperando al menos una confirmación de la red antes de dar por finalizada la transacción.

E

Edad (Age): Hace referencia al tiempo transcurrido en el que una cantidad determinada de criptomonedas se encuentran almacenadas en una dirección.

Empresa de servicios monetarios (Money Services Business): Es una organización que transfiere dinero o convierte divisas. El término abarca a instituciones financieras bancarias y no bancarias, tales como las sociedades de inversión, las empresas de cambio de divisas y de seguros. Su definición de puede variar en función de la jurisdicción. Una empresa puede considerarse como tal si se encuentra en alguna de las siguientes categorías: Actúa como casa de cambio (incluso si se trata de un barco que no se encuentra en aguas territoriales del Reino Unido), Transfiere dinero, o cualquier representación del mismo, de cualquier modo (la recogida y entrega de dinero como un “mensajero” no se considera transferencia de dinero) y Cobra cheques que son pagaderos a los clientes de una empresa.

En el sitio (On the spot): Se denominan así porque a las operaciones entre dos partes (comprador y vendedor) que se completan al instante, en el valor de mercado en el momento de la operación. En el mercado de divisas, la fecha de liquidación para operaciones spot en el par de divisas comerciado es normalmente de 2 días hábiles después de la fecha de la transacción (T+2). Normalmente, en las operaciones de divisas, una de las dos partes escoge entre una operación spot o forward. Si una empresa tiene una necesidad periódica de cambiar cantidades similares de una divisa extranjera, las operaciones spot son la opción más común, pues las operaciones forward tendrían prácticamente el mismo resultado, pero retrasarían la transacción durante el periodo de tiempo acordado en la operación.

Encriptación (Encryption): En el ámbito de la informática, encriptar información consiste en ocultarla, de forma que solo pueda interpretarse si se dispone de una clave o un código. En el de la criptografía, cifrar tiene el mismo fin. Es una técnica que permite proteger el intercambio de los datos y que los procesos en los que se utilicen sean más seguros.

Entidad de Contraparte Central o Cámara de Compensación (Central Counterparty Entity or Compensation Chamber): Son organismos, normalmente pertenecientes a grandes bancos, cuya función es facilitar el comercio de acciones y derivados en los mercados internacionales. Las Entidades de Contraparte Central tienen dos funciones principales en su papel de intermediarias: la compensación y la liquidación. En el proceso de compensación, la entidad media entre el comprador y el vendedor ofreciéndose como contrapartida a las contrapartes y definiendo los requisitos de cada parte para llevar a cabo la operación. En la liquidación, comprueba que la transferencia de valores y capital para completar la transacción se ha realizado correctamente y a tiempo y en caso necesario garantiza la transacción, cubriendo el riesgo de insolvencia de las partes.

Entrada (Input): se refiere al origen de una transacción. Suele tratarse de la dirección perteneciente al emisor del pago, excepto en el caso de una transacción por recompensa a la minería.
Entrega por paracaídas (Airdrop): Es cuando un proyecto de blockchain decide distribuir la totalidad o parte sus tokens o un criptoactivo de manera gratuita, que se lleva a cabo con fines publicitarios, normalmente durante una fase temprana de un determinado proyecto.

ERC20: Es una interfaz estándar que garantiza la interoperabilidad entre tokens. Por ende, los Tokens ERC20 son fichas, o Tokens que tienen compatibilidad con la plataforma Ethereum. Se podría decir que ERC20 es un estándar para que todos los Tokens que operen bajo él, puedan ser fácilmente intercambiables. Lo que hace un token "estandarizado" es utilizar un cierto conjunto de funciones. Si los desarrolladores saben de antemano cómo funcionará un símbolo, pueden integrar fácilmente esa ficha en sus proyectos con menor temor a errores. Si varios tokens se comportan de manera similar, llamando a las mismas funciones de la misma manera, entonces un Dapp (modelo para desarrollar aplicaciones exitosas y masivamente escalables) puede interactuar más fácilmente con diferentes subdivisas.

Los tokens aparte de trasmitir valor, pueden representar muchas otras cosas, tales como derecho a voto, cupones de descuento, etc. La mayoría de las monedas principales que corren en la Blockchain de Ethereum, se adhieren al ERC20, incluyendo aquellas que están emergiendo en las recientes ICO (Initial Coin Offerings). Para decirlo de una manera más sencilla, una ficha no es más que un contrato inteligente que opera sobre el Blockchain de Ethereum. Como tal, es un conjunto de códigos (funciones) con una base de datos asociada. El código describe el comportamiento de la ficha, y la base de datos es básicamente una tabla con filas y columnas que describen quién tiene cuántas fichas. Si un usuario, o un contrato inteligente dentro de Ethereum, envía un mensaje al contrato de esa moneda en forma de una transacción, el código actualizará la base de datos.

Escalabilidad (Scalability): Propiedad de la tecnología blockchain en su conjunto que señala su habilidad para adaptarse a los nuevos retos y evolucionar de manera fluida.

Escalpar / Especular (Scalping): Realizar muchas operaciones financieras (Trading) concretas en segundos o minutos con el fin de ganar dinero, sin importar lo poco que pueda hacerse en un día.

Esquema Ponzi (Ponzi Scheme): Es uno de los esquemas fraudulentos que más se repiten en el ecosistema de las Finanzas. En este tipo de operaciones, el responsable del esquema genera ganancias a partir del aporte de los inversionistas más viejos, garantizando a los más nuevos que gozarán de los mismos beneficios y exigiéndoles un pago determinado para ingresar y mantener el fraude operando. Debe su nombre a Carlos Ponzi, el primero en operar un esquema como este.

Estafa (Scam): Delito que se ejecuta contra el patrimonio o la propiedad y que se perpetra por medio de un engaño. El estafador se encarga de que la víctima crea en algo que no tiene existencia real o comprobable. Otra opción es engañar al estafado respecto a las condiciones de una operación comercial.

Estrategia de cobertura del riesgo (Hedging): En intercambio de divisas, la estrategia de cobertura del riesgo consiste en gestionar la exposición a la volatilidad a la hora de realizar un cambio de divisas. El principal método de cobertura del riesgo consiste en la adquisición de productos para tal fin, como los swap de divisas, los contratos forward y las opciones. De distinta manera, estos productos compensan la fluctuación de los tipos de cambio, de modo que protegen la inversión de la empresa del riesgo de devaluación de la divisa. En un entorno cada vez más competitivo e internacionalizado, hacer negocios fuera de las propias fronteras es cada vez más importante, por lo que resulta imprescindible contar con una estrategia cobertura del riesgo óptima para maximizar los beneficios.

Ethereum: Es una plataforma descentralizada que permite la creación de Contratos Inteligentes (Smart Contracts), a la que algunos han denominado un Superordenador Descentralizado. También opera sobre su propia cadena de bloques y fue concebido originalmente como una versión mejorada para superar las limitaciones de programación de la 'blockchain' de bitcoin. Codifica los datos de la misma forma, pero una de las principales diferencias es que sirve para ejecutar contratos inteligentes (piezas de software que sirven para automatizar y blindar la ejecución de órdenes previamente programadas) y tiene una gran variedad de aplicaciones más allá de las relacionadas con el ámbito financiero. El Ether es su criptomoneda, la segunda más utilizada después de bitcoin y de mayor capitalización del mercado.

Ethereum Maquina Virtual (Etherem Virtual Machine): Es una máquina virtual donde se pueden ejecutar de manera segura los contratos inteligentes y protocolos de Ethereum.

Expansión (Spread): Valor resultante entre las marcas (montos) de Ofertar (Bid) y Pedir (Ask). Mientras mas spread es mas fácil hacer trading sobre todo en scalping.

Explorador de Bloques (Block Explorer): es una herramienta en línea para ver todas las transacciones, pasadas y actuales, en la cadena de bloques. Proporcionan información útil, como la tasa de hash de la red y el crecimiento de las transacciones.

F

Ficha ó Pieza (Token): Tradicionalmente, 'token' es el nombre con el que se llama a las piezas que, adquiridas a cambio de dinero, sirven para recibir un bien o servicio. Ya sean, por ejemplo, las fichas para jugar en un casino, o para comprar comida en un festival. En el mundo de la cadena de bloques, esta palabra sirve para designar unidades de valor que pueden adquirirse a través de 'blockchain' y que se usan para obtener bienes y servicios. Al igual que bitcoin, estas unidades se transmiten a través de los mensajes de la red de 'blockchain', pero a diferencia de la moneda, sirven para intercambiarse por todo tipo de servicios. Dentro de una red privada 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. Incluso pueden usarse como 'garantía' de la recepción de futuros servicios que una compañía promete ofrecer, cuando se usan en las ICOs como forma de financiación de 'startups'.

Ficha ERC20 (Token ERC20): Los tokens ERC20 son simplemente un subconjunto de tokens Ethereum que se ajustan a determinados parámetros. Para cumplir plenamente con los estándares de ERC20, el desarrollador debe incorporar un conjunto específico de funciones en su contrato inteligente que, a un alto nivel, le permitirá realizar las siguientes acciones: 1. Obtener el suministro total de tokens, 2. Obtener el saldo de la cuenta, 3. Transferir el token y 4. Aprobar gastar el token. ERC20 permite una interacción perfecta con otros contratos inteligentes y aplicaciones descentralizadas en la cadena de bloques Ethereum. Los tokens que con algunas (pero no todas) de las funciones estándar, se consideran parcialmente compatibles con ERC20 y todavía podrían interactuar dependiendo de qué funciones faltan. En general, un token ERC20 no es diferente de cualquier otro token, sino que además se ajusta al token estándar de Ethereum.

Firma Digital (Digital Signature): Proceso matemático que permite verificar la autenticidad del remitente de bitcoins. Hasheando en conjunto la clave pública y la clave privada del remitente, el receptor puede comprobar que el pago fue realizado por ese remitente y que, además, no fue alterado por nadie más.

Firma de Círculo (Ring-Signature): Es un tipo de firma digital que puede ser realizada por cualquier miembro de un grupo de usuarios que tengan claves.

Foro Hablemos Bitcoin (Bitcointalk Forum): Foro para usuarios bitcoin y de otras blockchain. Primera comunidad bitcoin y referente en el mundo blockchain. Fue fundado por el mismo Satoshi Nakamoto en Noviembre de 2009.

Fraguador o Apartador (Forger): Elemento del ecosistema de una blockchain PoS que "bloquea" tokens ("dinero") durante cierto tiempo a cambio de una rentabilidad. Cumple el papel de un minero, pero resuelve algoritmos Proof of Stake, donde es recompensado en función de la cantidad de tokens "apartados" y el tiempo que van a estar bloqueados.

Fraguar o Apartar (Forge): Resolver hashes con un algoritmo Proof of Stake para verificar transacciones (u otro tipo de registros) y añadir bloques a la blockchain.

Función unidireccional (Unidirectional function): es una función matemática en la cual se conoce un procedimiento de cálculo eficiente y rápido para computar esa función, mientras que no se conoce un procedimiento eficiente para realizar ese mismo cálculo pero a la inversa.

Existen muchos ejemplos de funciones unidireccionales. Uno famoso es el problema de la factorización de números enteros: multiplicar dos primos grandes de centenas o miles de bits es viable y fácil para los ordenadores actuales como explicamos en nuestro ejemplo del algoritmo RSA de clave pública; sin embargo, no se conoce un algoritmo eficiente para invertir esta multiplicación, es decir, recuperar los dos primos partiendo exclusivamente de su producto.

El tema de las funciones unidireccionales es una de las preguntas abiertas más importantes en computación teórica y una ciencia muy práctica en el campo de la criptografía. De momento, no se tienen pruebas matemáticas de la existencia de funciones de una dirección, pero los criptógrafos “entienden” que tales funciones existen y usan algunos candidatos razonables en la construcción de algoritmos criptográficos.

Funciones deterministas (Deterministic functions): Son aquellas funciones donde siempre se crea el mismo resumen con la misma entrada aunque el resumen parezca aleatorio.

G

Gabinete (Case): Es una pieza en cuya construcción se emplean materiales como el plástico y metales como el aluminio y el acero, y básicamente es una caja preparada para colocar en su interior todos los componentes que conforman una PC, es decir Discos rígidos, Unidades ópticas, Tarjetas madres, Procesadores, Memorias, Placas de vídeo y audio y demás, y se diferencian entre si por su tamaño y al tipo de computadora a la que está destinada.

Generaciones Humanas actuales de acuerdo a la Edad:

Baby Boomers (1945 y 1964):

✓ Nacidos post Segunda Guerra Mundial. El nombre de esta generación refiere al repunte en la tasa de natalidad (Baby Boom) de esos años.

✓ El trabajo como modo de ser y de existir: estable, a largo plazo, adictivo, no necesariamente de lo que aman hacer.

✓ No le dedican mucho tiempo al ocio y a la actividad recreativa.

✓ Las mujeres de esta generación aún se están incorporando al mercado laboral. Si bien persiste el ideal de familia tradicional, se empiezan a romper estructuras.

Generación X (1965 y 1981):

✓ Hombres y Mujeres que trabajan mucho pero logran un equilibrio, siendo felices con sus propias vidas.

✓ Son los que vieron el nacimiento de Internet y los avances tecnológicos. Están marcados por grandes cambios sociales.

✓ Como son una generación en transición (se les llamó Generación Perdida e incluso Generación Peter Pan) pueden hacer convivir equilibradamente la relación entre tecnología y vida social activa “presencial”: tienen participación dentro de los eventos de su comunidad.

✓ Son más propensos a estar empleados (aceptan los órdenes de jerarquía institucional) y equilibran la energía entre el trabajo, los hijos y el tiempo de ocio.

✓ Son los padres de los Millennials, hacen esfuerzos adaptativos a la vertiginosidad de la generación que sigue.

Generación Y o Millennials (1982 y 1994):

✓ Muy adaptados a la tecnología. La vida virtual es una extensión de la vida real. Aunque conservan algunos códigos de privacidad en relación a lo que exponen o no en Internet (a diferencia de los Centennials, que comparten todo).

✓ Son multitareas (multitasking).

✓ No dejan la vida en el trabajo, no son adictos al trabajo (workaholic), porque quizá observaron que sus padres sí lo fueron, y lo hacen distinto.

✓ Son emprendedores y creativos, intentan vivir de lo que aman hacer. Son idealistas.

✓ Aficionados a la tecnología del entretenimiento: usuarios de las salas de chat en los ’90 y ahora de redes de citas. Pasaron por todo: SMS, Reproductor de CD, MP3, MP4, DVD.

✓ Aman viajar, conocer el mundo, ¡y subir las fotos a las redes!

✓ Según estudios, duran en sus trabajos un promedio de dos años, a diferencia de la Generación X y los “Baby Boomers” (más estables). Es por eso que las empresas enloquecen armando políticas de “fidelización”.

✓ La mayoría trata de reemplazar el viejo orden mundial y el obsoleto y centralizado sistema financiero de los “Baby Boomers” imponiendo nuevos esquemas y formas de riqueza y negocios, mediante las nuevas Tecnologías de Información y Comunicación disponibles, tales como las FinTech y el uso del Criptocomercio (Blockchain y Criptodivisas).

Generación Z o Centennials (1995 hasta el presente):

✓ Son verdaderamente “nativos digitales” (desde su niñez usan Internet).

✓ Autodidactas (aprenden por tutoriales), creativos (incorporan rápido nuevos conocimientos y relacionan bien) y sobreinformados (alta propensión al consumo de información y entretenimiento).

✓ Visitan redes que sus padres no: un ejemplo es Snapchat. Comparten contenido de su vida privada, aspiran a ser YouTubers. Su vida social pasa en un alto porcentaje por las redes.

✓ A la mayoría les encantan o ven positivamente las FinTech y el uso del Criptocomercio (Blockchain y Criptodivisas), independientemente del buen uso de las Comunidades, Empresas o Gobiernos que las implementen.

Gigahashes/seg: El número de intentos de hash posible en un segundo dado, medido en miles de millones de hashes (miles de Megahashes).
GitHub: Plataforma destinada al desarrollo de software colaborativo. Se usa para alojar proyectos y utiliza el sistema de control de versiones Git.

Grifo (Faucet): Una técnica que se utiliza cuando se inicia por primera vez un altcoin. Un número determinado de monedas son preminadas, y entregadas de forma gratuita, para animar a la gente a tomar interés en la moneda y comenzar su extracción a sí mismos.

Grupo minero (Minning Pool): Un grupo de mineros que han decidido combinar su poder de computación para la minería. Esto permite que las recompensas se distribuyan de manera más consistente entre los participantes en el grupo.

H

Hardware: Partes físicas de un sistema informático. Por ejemplo: Teclado, ratón, tarjeta gráfica, entre otros. El hardware suele distinguirse entre básico (los dispositivos necesarios para iniciar el funcionamiento de un ordenador) y complementario (realizan ciertas funciones específicas). En cuanto a los tipos de hardware, pueden mencionarse a los periféricos de entrada (permiten ingresar información al sistema) y salida (muestran al usuario el resultado de distintas operaciones realizadas en la computadora).

Hash, Función Hash o Resumen Criptográfico: Es una función algorítmica que emite una dirección alfanumérica que resume y protege la información insertada a través de una entrada. Sirven también para garantizar la inmutabilidad de una unidad de información, ocultar una contraseña o servir como firma digital. En otras palabras, es una función matemática que permite convertir una entrada de tamaño aleatorio en una salida de tamaño fijo. Puede comprenderse como la función criptográfica que dota de seguridad determinados procesos de procesamiento de datos. En el caso de las blockchains, el proceso de confirmar transacciones.

Un Hash se utiliza lo que se llama **funciones hash criptográficas o funciones unidireccionales** en el área de la criptografía. Este tipo de funciones se caracterizan por cumplir propiedades que las hacen idóneas para su uso en sistemas que confían en la criptografía para dotarse de seguridad. Al igual que todos los datos informáticos, los hashes no son números grandes, y se escriben normalmente en sistema hexadecimal (números entre 0 y 9 y letras entre A y F.

Un algoritmo de Hash convierte una cantidad arbitrariamente grande de datos en un Hash de longitud fija. Por ejemplo el Hash de la clave pública de la palabra “proyectotictac” pudiera llegar a ser algo parecido a 8Fgdd9ur6wqtr2uciLFNxvgm1GBuS5kaej .

Las características principales de una **función de hash criptográfica** ideal son las siguientes:

- Eficiencia en la computación. Debe proporcionar un cálculo rápido del hash a partir de cualquier mensaje de entrada.
- Resistencia a preimagen. Debe ser computacionalmente muy difícil generar el mensaje a partir del cual se ha derivado el resumen.
- Resistencia a segunda preimagen. Debe ser computacionalmente muy difícil, dado un mensaje, conseguir un segundo mensaje que genere el mismo hash.
- Resistencia a colisión. Debe ser computacionalmente muy difícil generar dos mensajes diferentes y que el hash de ellos sea el mismo.

Hash de Firma (Hash Firm): Un hash que indica cuáles partes de la transacción son firmadas y por tanto, inmodificables. Por defecto, se etiqueta una transacción con la señal SIGHASH ALL.

Hashes/seg: El número de intentos de hash posible en un segundo dado.

Haz tu propia investigación – HTPI (Do Your Own Research – DYOR): Frase u Acrónimo usado para resaltar que siempre es bueno recomendarle a los demás que deben realizar su propia investigación antes de realizar cualquier acción u operación explicada o recomendada o cuando viene de fuentes no conocidas, no confiables o no fidedignas.

Hashgraph: Es esencialmente un grafo, un objeto matemático que se mantiene unido por hashes simples y regulares, sin implementaciones criptográficas de alto nivel, como pruebas de conocimiento cero, por ejemplo. Una red de hashgraph logra consenso (lo que significa que los nodos llegan a un acuerdo sobre el estado de la red, incluidos los registros de quién posee qué activos) usando lo que Leemon Baird, quien originalmente concibió el hashgraph, llama “chismes sobre chismes”. Veamos entonces cómo funciona este concepto en la red.

Los nodos de hashgraph están constantemente “chismoseando” o compartiendo entre ellos cada información que conocen sobre el estado actual de la red y su historia. En lugar de tener toda la red de acuerdo, al unísono, sobre que se produjo una determinada transacción, como ocurre en entornos de blockchain, un nodo involucrado en una transacción hashgraph selecciona aleatoriamente otro nodo para informar sobre la misma (y todo lo demás que sepa), luego otro, y otro, indefinidamente. Todos los nodos que reciben esta información también la comparten con nodos seleccionados aleatoriamente una y otra vez, añadiendo a sus informes cualquier información nueva que hayan recibido desde la última vez que transmitieron la suma de sus conocimientos. Este intercambio constante evita que los actores malintencionados retengan información sobre las transacciones, un acto que puede constituir la base de un ataque a una red DLT.

Hashgraph funciona sin necesidad de utilizar los sistemas PoW, y también puede ofrecer niveles de bajo costo y alto rendimiento sin un solo punto de falla. Hashgraph elimina la necesidad de cálculos extensos y consumo de energía, y mejora las estadísticas de rendimiento de la red Bitcoin.

Hoja de ruta (Roadmap): Documento y/o proceso que contiene una planificación minuciosa a corto y largo plazo de un software en la que frecuentemente se marcan pequeños objetivos llamados “Milestones”.

I

Identidad Digital (Digital Identity): En blockchain, la identidad digital se forma firmando transacciones criptográficamente verificadas con la misma llave pública.

Índice de Potencial del Mercado Bitcoin – IPMB (Bitcoin Market Potential Index – BMPI): Indicador estadístico de más de 40 variables que clasifica a 178 países según su respectivo potencial de adopción de Bitcoin como criptomoneda.

Índice de Precios de Bitcoin – IPB (Bitcoin Price Index – BPI): El Índice de Precios de Bitcoin es un promedio de precios del bitcoin en las principales bolsas del mundo. Es publicado por CoinDesk.

Inflación (Inflation): Aumento de los precios por una depreciación de la divisa. Suele ser una respuesta natural a la impresión de moneda descontrolada (que no está respaldada por un aumento de riqueza real). Reduce el poder adquisitivo de los ahorradores.

Información (Information): La información está definida como una serie de datos con significado, que organiza el pensamiento de los seres vivos, en especial el de los seres humanos. En sentido general, la información es un grupo organizado de datos procesados que integran un mensaje sobre un determinado ente o fenómeno; permitiendo que el hombre adquiera el conocimiento necesario para la toma de decisiones en su vida cotidiana. La información se caracteriza por: Los datos: se refiere a toda la información recopilada y codificada, para poder ser archivada y guardada. El orden: para que la información tenga sentido es necesario que este ordenada. La veracidad: para que la información sea válida, es necesario que provengan de fuentes veraces. Valor: se refiere a la utilidad de la información para el destinatario.

Informática (Computing): En el Diccionario de la Real Academia Española se define informática como el Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.” Disciplina científica que se concentra en el estudio del tratamiento automático y racional de la información mediante el uso y aplicación de dispositivos electrónicos y sistemas computacionales. El vocablo informática proviene del francés automatique d’informations, acuñado por el ingeniero Philippe Dreyfus para su empresa «Société d’Informatique Appliquée» en 1962. Es un acrónimo de las palabras information y automatique (información automática).

Intercambio Atómico (Atomic Swap): Se refiere al protocolo transaccional que permite cambiar una moneda por otra sin usar un servicio centralizado como una casa de cambio.

Intercambio de Divisas (Foreign Exchange – Forex): Es el intercambio de una moneda por otra. El intercambio de divisas es una parte esencial del comercio internacional. Si una compañía china quiere efectuar un intercambio comercial con una francesa, las dos empresas están obligadas a ir al mercado de divisas para completar la transacción, que

implica a la moneda china, el yuan o renminbi y a la divisa francesa, el euro. A pesar de la importancia del comercio internacional, éste solo supone el 2% del total del volumen de actividad del mercado mercado de divisas. El 98% restante de las operaciones del mercado Forex son de carácter puramente especulativo.

Intercambio Sobre La Cuenta – Intercambio ISC (Exchange Over The Counter – Exchange OTC): Es un intercambio bilateral, en el que dos individuos o usuarios se realizan propuestas directamente, sin ningún tipo de mediador, es decir, un intercambio en el que los comerciantes hacen tratos entre sí directamente, en lugar de depender de un intercambio central para mediar entre ellos.

Internet: El nombre Internet procede de las palabras en inglés Interconnected Networks, que significa “redes interconectadas”. Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo, por lo que se podría definir como una red global en la que se conjuntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí. En esta “red de redes” como también es conocida, participan computadores de todo tipo, desde grandes sistemas hasta modelos personales. En la red se dan citas instituciones oficiales, gubernamentales, educativas, científicas y empresariales que ponen a disposición de millones de personas su información.

Internet Profunda (Deep Web): Aquellas páginas que no pueden ser indexadas por un buscador. En la Deep Web es donde tienen lugar la gran mayoría de las actividades delictivas de la red.

K

Kilohashes/seg: Es el número de intentos de hash posible en un segundo dado, medido en miles de hashes.

L

Lambo: Frase que se usa cuando vas ganando mucho. Se trata de la abreviatura de la reconocida marca de automóviles deportivos Lamborghini, una de las primeras firmas en aceptar pagos en criptoactivos. Además, es una de las inversiones preferidas por los millonarios del ecosistema. Lambo también se refiere a grandes ganancias que permiten comprar un Lamborghini de un millón de dólares. Por ejemplo si tu divisa / criptodivisa sube 2000% rápidamente te preguntan: ¿Cuando te vas a comprar un Lamborghini? (¿When the Lambo?) .

Liquidez (Liquidity): Es la capacidad de comprar y vender un activo fácilmente. También se refiere a la cualidad de una inversión, por la cual es posible su transformación inmediata en efectivo. Para los valores cotizados, un buen grado de liquidez significa en general elevados volúmenes y frecuencias de contratación, y escasa diferencia entre los precios de compra y venta. Eso significa que se pueden comprar y vender valores, de forma instantánea, sin que el precio de la operación se vea afectado por ausencia de contrapartidas. Para medir la liquidez de una empresa se utiliza el ratio de liquidez, con el que se calcula la capacidad que tiene ésta para hacer frente a sus obligaciones a corto plazo. Así pues, se puede averiguar la solvencia en efectivo de una empresa y su capacidad para seguir siendo solvente ante cualquier imprevisto.

Luneando (Mooning): Se usa como verbo de la palabra Luna (Moon) para describir el ascenso rápido de una divisa / criptodivisa.

M

Mano débil (Weak hand): Persona que vende rápido sus activos en divisas / criptodivisas tan pronto ve que la tendencia de las mismas baja, aunque sea un poco, porque se asusta rápidamente.

Mantener (Hold): Acción de guardar en nuestro poder las divisas / criptodivisas para que independientemente de la tendencia de la misma en el mercado, no venderlas. Se usa el termino Hodl como una parodia de la palabra hold y se refiere a un individuo que no hace el comercio del día con sus divisas / criptodivisas.

Maraña / Enredo (Tangle): Protocolo y propuesta descentralizada alternativa a blockchain conocida como Gráfico Directo Acíclico (DAG) en el que una transacción requiere de otras dos transacciones para ser confirmada. Fue introducido y explicado por el proyecto IOTA en su papel blanco. En este protocolo, los nodos no requieren conocer la cantidad total de la red para procesar transacciones, sino una pequeña parte de ella.

Máximo Histórico de Precios – MHP (All Time High – ATH): Índice que denota que el precio de un criptoactivo alcanzó su precio máximo jamás logrado.

Medidas Anti-lavado de dinero – ALD (Anti-Money Laundering – AML): Se refiere al marco legal creado por los gobiernos de cada país para combatir el lavado de dinero. Durante los últimos años las autoridades han intentado adaptar estas políticas a la actividad comercial de criptomonedas.

Megahashes/seg: El número de intentos de hash posible en un segundo dado, medido en millones de hashes (miles de Kilohashes).

Mercado de divisas (Mercado Forex): Es el mayor mercado del mundo. Se trata de un intercambio descentralizado en el que las principales divisas del mundo pasan de una mano a otra. El mercado está en constante movimiento y los tipos de cambio varían cada segundo. En el mercado mundial de divisas, la mayor parte del dinero se intercambia con fines especulativos, es decir, la mayor parte del volumen global de divisas se compra y se vende en función de las expectativas de su precio futuro. Solo un pequeño porcentaje se atribuye a transacciones de la economía real, es decir, para el intercambio internacional de bienes y servicios.

El mercado de divisas es esencial para el funcionamiento del comercio internacional, ya que es el que permite, por ejemplo, que una empresa en EEUU compre productos a proveedores europeos. Una operación de intercambio de divisas típica implica el intercambio de una divisa por otra para realizar un pago. Sin el mercado de divisas, no podría existir el comercio internacional.

Mercado de divisas P2P (P2P Forex): Es un sector en alza dentro del mercado de divisas, que elimina intermediarios (bancos y brókeres) y los costes relacionados, al conectar directamente a las dos partes para realizar el intercambio. La ventaja para el usuario es que el mercado peer-to-peer, permite reducir de forma drástica los spreads que los bancos y brókeres aplican normalmente en el tipo de cambio. El tipo de cambio ofrecido en el mercado P2P es, por tanto, el tipo de cambio mid-market (tipo de cambio intermedio entre precio de compra y precio de venta) y al que se puede acceder a tiempo real en cualquier hora del día, lo que se traduce en una reducción de los costes de las operaciones y el tiempo de gestión y una mayor garantía de transparencia.

Meta / Hito (Milestone): Cada uno de los pequeños objetivos marcados en el Documento oficializado como Hoja de Ruta o Roadmap.

Metrópolis: Tercera fase del desarrollo de Ethereum activada en octubre de 2017. Metrópolis añade a Ethereum nuevas interfaces de usuario y una tienda de aplicaciones descentralizadas. Está formada por la fase Byzantium y la fase Constantinople, próxima a activarse.

Mezclador (Mixer): Es un servicio que mezcla los bitcoins de dos o más individuos haciendo múltiples envíos de dinero en forma de dicha criptomoneda, a través de varias entradas y salidas. Es una operación que dificulta el rastreo de capitales en bitcoin.

Micromecenazgo (Crowdfunding): Financiación en masa. Modelo de financiación de startups y otros proyectos que se apoya en micro inversiones de pequeños inversores.

Microtransacción (Microtransaction): Es el pago de una pequeña cantidad de bitcoins a cambio de un bien o servicio en línea.

Miedo, Incertidumbre y Duda – MID (Fear Uncertainly Doubt – FUD): Acrónimo que expresa tres reacciones que algunas entidades buscan generar en los inversionistas para influenciar los mercados de criptoactivos.

Miedo a Perderse Algo – MaPA (Fear of Missing Out – FoMO): Se trata de un concepto relativamente nuevo que podría afectar a casi dos tercios de la población: sentir que te estás perdiendo demasiadas cosas mientras los demás se divierten o algo en las redes sociales o a quedar excluido de un evento, y provoca la dependencia de Internet y su inmediatez comunicacional.

Milibitcoin: 1 milésima de participación Bitcoin (BTC 0,001).

Minar (Mine): Se refiere al acto de ejecutar acciones de Minería Digital. Aunque por lo general se usa muy específicamente al hecho de Resolver hashes con un algoritmo Proof of Work para verificar la veracidad de una transacción (u otro tipo de registro) y crear bloques que se añaden a la cadena de bloques. Minar es, en grosso modo, comprobar que una transacción es líquida (que el emisor tiene mayor cantidad de tokens que la que quiere enviar) o en otras palabras, es el proceso mediante el cual se verifican y añaden transacciones a la blockchain. Este proceso implica la resolución de problemas criptográficos utilizando un Hardware Informático (Equipo) llamado Minero. También implica

la creación o recolección (acumulación) de criptomonedas. La minería asegura que la blockchain esté respaldada y distribuida a través del mundo.
Minería Digital de Criptodivisas (Digital Mining of Cryptocurrency): Por lo general se usa para referirse al acto de resolver un bloque, validando todas las transacciones que contiene, es decir, la minería es el proceso mediante el cual se lanzan (crean) nuevas criptodivisas (bitcoins o altcoins) al mercado al ritmo marcado por los algoritmos y especificaciones técnicas especificadas en su creación. Pero en un amplio sentido se refiere a cada uno de los métodos o acciones mediante los cuales se pueden crear y/o conseguir criptodivisas. Entre los más comunes o conocidos están:

1) **Minería mediante el uso de Equipos Informáticos especializados y/o dedicados:** Esto abarca el uso de Equipos ASIC o Computadores de Alta Gama mediante el uso de Tarjetas de vídeo, GPU o CPU por medio de un **Programa (Software) local instalado (Local Mining)**, o con el uso de **Sitios (paginas web) especiales en los Navegadores (Web Mining),** o la **contratación (compra) de Maquinas Virtuales (Contratos de Poder de Computo) en la Nube (Cloud Mining), o el Uso de aplicaciones especiales en dispositivos móviles (Movil Mining).**
2) **Minería mediante el uso de Acortadores de Enlaces Web (URLs):** Esto solo incluye a los servicios de acortadores que pagan con criptodivisas por el uso de los mismos.
3) **Minería mediante la ejecución de Tareas o Servicios Profesionales:** Esto incluye entre muchas otras actividades, las siguientes: **Realizar trabajos de transcripción, Traducción de textos, Publicación de artículos (Post) en Redes Sociales, Blog o Sitios Web, Audios o Vídeos, Asesorías y Trabajos en área especificas en línea por encargos, realización de encuestas, lecturas o envíos de correos, u otros tales como la Asesoría u Entrenamiento en la Minería Digital o cualquier otra actividad relacionada o no.**
4) **Minería mediante la inversión con divisas:** Esto incluye las **Ofertas Iniciales de Monedas (ICO), la compra/venta directa en las Casas de Cambio y/o Bolsas de Criptomonedas (Exchange) nacionales e internacionales por medio del Mercadeo (Trading) y acciones asociadas.**
5) **Minería mediante recompensas:** Esto incluye el **uso (realización) de actividades lúdicas (Juegos), la utilización de Grifos (Faucets) de Visualización de Publicidad o Resolución de Captchas y Recaptchas, y la obtención y/o acumulación de referidos en Grifos u otros servicios web relacionados con la Minería Digital.**
6) **Minería mediante la Compra/Venta de Bienes y Productos:** Esto incluye a aquellas **operaciones comerciales** que tengan como fin negociar los mismos en **Criptodivisas.**

Minero (Miner): Algunas veces se refiere a las personas encargadas de las labores de Minería Digital, personas que trabajan con potentes ordenadores conectados las 24 horas vigilando que todas las transacciones de la red se realizan correctamente. Para validar cada transacción y crear los bloques los mineros deben encontrar el 'hash', o clave digital, de cada bloque para enlazarlo con el siguiente. Cada vez que los mineros encuentran una de estas claves criptográficas se 'mina' una criptodivisa y ellos reciben una retribución en esta

misma moneda. Otras veces se utiliza para referirse al Hardware Informático (Equipo) especializado utilizado para las labores de la Minería Digital.

MinerOS GNU/Linux: Es una Distro diseñada con Ubuntu y MX Linux 17 (DEBIAN) e inspirada en la Filosofía de Endless OS + Lakka + LibreELEC con la orientación especifica para el aprendizaje y uso de la Minería Digital y el Criptocomercio, en cualquier computador (antiguo o moderno) con un procesador (CPU) de 64 Bit de pocos o muchos recursos de hardware si fuese necesario.

La Versión 1.0 de MinerOS GNU/Linux puede ser usada como Distro de uso diario, ya que trae todo el Software Básico y Esencial para el Hogar y la Oficina (LibreOffice + WPS Office), en una configuración basada Ubuntu 18.04 (Modernidad y alta Compatibilidad) y MX Linux 17 basado en DEBIAN (Estabilidad, Portabilidad y Personalización) en una fusión del Entorno XFCE (Ligero y Funcional) + Plasma (Hermoso y Robusto), por lo que se adapta perfectamente a cualquier PC (Computador Personal) de bajas medianas o altas prestaciones sin ningún problema. Además de Iniciar con el Entorno de Escritorio XFCE y Plasma puede iniciar directamente con el Centro Multimedia de Kodi para una experiencia de usuario multimedia mucho más cómoda y agradable cuando se desee solo usar para ver contenido multimedia (Películas, Música, Imágenes, Sonidos descargadas o en Linea, y hasta Juegos de Videoconsolas Retro). Y ya viene lista para usar Redes Virtuales Privadas VPNs, trayendo 1 ya instalada, y Navegación segura con el Navegador TOR. Y trae JDK 9.0.4 y Firefox 51.0.1 (Congelado) para ejecutar aplicaciones Java de Escritorio y Web. MinerOS GNU/Linux al igual que MX Linux tiene una alta capacidad y facilidad de personalización y empaquetamiento en formato ISO para producir nuevas Distros personalizadas y fáciles de instalar.

MinerOS GNU/Linux 1.0 trae los programas mineros Minergate, CGMiner, CPUMiner (Versión: Multi y Opt), Claymore y XMR-STAK-CPU, más las Billeteras de Armory, Bolivarcoin, Exodus, Jaxx, Magi, Onixcoin y el complemento de detección de Billeteras de Hardware Trezor instalada por defecto.
Moneda de Nombre (Namecoin): Es una altcoin diseñado para funcionar como una alternativa al tradicional Sistema de Nombre del Dominio (DNS por sus siglas en inglés). Con Namecoin, un usuario puede registrar un dominio a través de un servidor proxy.

Moneda Alternativa (Altcoin): Término empleado para referirse a las criptomonedas o fichas de blockchain alternativas a Bitcoin; como Litecoin, Ethereum, Dash, Monero, Zcash, Feathercoin y PPcoin, entre otros.

Moneda Anónima (Anoncoin): Término referido a criptomonedas cuyas transacciones son privadas y no pueden rastrearse, como Zcash y Monero.

Moneda Base (Base currency): En una cotización de un par de divisas, la moneda base o divisa base, también conocida como moneda principal, es la primera divisa que aparece en un par de divisas concreto, mientras que la segunda se conoce como moneda cotizada. La cotización de una divisa se muestra siempre en comparación con otra. Por ejemplo, en el par de divisas EUR/USD, el euro es la moneda base y siempre tiene el valor 1, pues la divisa base es la referencia que fija el tipo de cambio entre las dos divisas. Algunas cotizaciones aparecen de la siguiente forma: EUR/USD: 1,30; es decir, se necesitan 1,30

dólares para comprar 1 euro. En el mercado de divisas, normalmente la divisa más líquida es la que se utiliza como moneda base. Así pues, la mayor parte de las veces el dólar de EEUU es la moneda base en la mayor parte de los cruces, excepto en el caso de los cruces contra el euro, la libra, el dólar australiano y el dólar neozelandés.

Moneda Cotizada o Divisa Secundaria (Quoted Currency or Secondary Currency): Es la segunda divisa que encontramos en un par de cotización y cuyo valor es el que se muestra en la cotización, en relación a una unidad de la divisa base. En el par de cotización EUR/USD, el dólar estadounidense (USD), es la moneda cotizada, mientras que el euro (EUR) es la moneda base. En la cotización "EUR/USD: 1,30", se requieren 1,30 USD para comprar 1 euro. En este caso el euro, que es la divisa base, siempre tendrá valor 1, mientras que la divisa cotizada tiene un valor variable dependiendo de la fluctuación del tipo de cambio. En la gran mayoría de los casos, la divisa con más presencia internacional es la divisa base, es decir, el dólar, que es la que aparece como base en todos sus cruces, con la excepción de los cruces con el euro, la libra esterlina, el dólar australiano y el dólar canadiense.

Moneda de Colores (Colored Coin): Es un metaprotocolo que superpone información sobre pequeñas unidades de Bitcoin. Una moneda coloreada es una cantidad de bitcoin, reutilizada para expresar otro activo. Para entenderlo mejor, podríamos pensar en un billete de un dólar al que ponemos un sello que indica "Esto es el certificado de una acción de Acme Inc". Ahora ese billete de un dólar tiene dos propósitos: es un billete y también un certificado de una acción. Y debido a que es más valioso como certificado, no quieres utilizarlo para comprar algo, por lo que efectivamente ya no es útil como moneda. Colored Coins funciona de la misma manera, solo que convierte una cantidad específica muy pequeña de bitcoin, en un certificado de negocio que representa otro activo.

Moneda de Metadatos (Metacoin / Metachain / Blockchain App): Son implementaciones de monedas (criptodivisas) que utilizan la cadena de bloques (blockchain) de otras criptodivisas en sí, pero codifican sus propios metadatos con nueva semántica de transacción. Por tanto, su principal característica es que comparten la cadena de bloques de otras criptodivisas. Es decir, añaden nuevas capas de protocolo implementado en la parte superior de la cadena de bloques de alguna criptodivisa. Lo hacen creando una moneda (criptodivisas) dentro de otra, o crean una superposición de plataforma o protocolo dentro de la Blockchain. Estas capas añadidas de funciones extienden el código del Protocolo nativo y añaden características y capacidades mediante la codificación de datos adicionales dentro de las transacciones y de las direcciones de dicha criptodivisa nativa.

Moneda Escremento (Shitcoin): Criptodivisa que no es seria, es decir, no tiene o cuenta con un respaldo serio o credibilidad comprobada.

Moneda Fraudulenta (Scamcoin): Criptodivisa generalmente no sustentada en blockchain cuyo esquema financiero es fraudulento y tiende a robar los fondos de los inversionistas y participantes.

Moneda Lenta (Slow Currency): Divisa o Criptodivisa que no tiene muchas operaciones financieras sobre ella en el Mercado de Capitalización.

Moneda Maestra (Mastercoin): Es una capa de protocolo superpuesta en el protocolo Bitcoin u otra criptodivisa, que crea una plataforma para diversas aplicaciones que se extienden al sistema Bitcoin o de otra criptodivisa. Se trata de una plataforma para la construcción de otras cosas, tales como, monedas, tokens de propiedad inteligente (Smart Property) intercambios descentralizados de activos, contratos, etc. Mastercoin utiliza la moneda MSC como token para realizar transacciones, pero Mastercoin no es principalmente una moneda.

Moneda Madre (Mothercoin): Criptodivisa cuya tecnología permite o ha permitido la creación de otras nuevas derivadas de si misma o soportadas por su plataforma. Por ejemplo: Bitcoin (BTC) es Moneda Madre de Bitcoin Cash (BCH) y Bitcoin Gold (BCG) y Ethereum (ETH) es Moneda Madre de Ethereum Classic (ETC).

Monitor: También llamado Pantalla o Display, es el dispositivo de salida para la visualización de imágenes y vídeos que deben ser mostrados al usuario.

Mount Gox: conocido comúnmente como Mt. Gox, es uno de los primeros exchange de bitcoins, al igual que uno de los más utilizados. Tiene su sede en Japón y fue creado en 2010 por Jed McCaleb.

Movimiento de la Nueva Economía (New Economy Movement – NEM): Es una plataforma tecnológica que aspira traer novedosas características al mundo de la criptografía, este sistema se encuentra catalogado como un software de código abierto escrito en Java. La plataforma de NEM ha sufrido un asombroso crecimiento, lo que le permitió estar dentro del top de las primeras 10 criptomonedas junto al Bitcoin y Ethereum. El sistema de NEM opera realizando transacciones de una manera muy parecida a otras plataformas, las cuales trabajan bajo la tecnología blockchain con código abierto, por lo que permite que se hagan operaciones con la criptomoneda XEM, pero a diferencia de Bitcoin y Ethereum, esta plataforma incluye el registro de varios nombres de dominios, crear cuentas con varios titulares y hasta enviar mensajes.

Lo que más llama la atención de todo, es el sistema de activos inteligentes de NEM, la cual tiene la ventaja de que la blockchain pueda modificarse en su totalidad a conveniencia de quien la use, de esta forma así se puede registrar casi cualquier activo inteligente. El objetivo es ofrecer una plataforma a nivel mundial, en el que se gestionen cualquier tipo de activos, por lo que a través de ella podrás registrar documentos notariados, derechos de autor, títulos de propiedad, entre otros, y una vez que todo esto esté dentro de la plataforma de NEM, podrás transferirlos o registrarlos sin necesidad de que un notario o registro de propiedad intervenga.

El algoritmo de Bitcoin exige una enorme potencia en el hardware cuando se trata de la minería de esta criptodivisa, en cambio la plataforma de NEM utiliza un algoritmo basado en el sistema POI (prueba de importancia). Este algoritmo le permite a NEM, marcar el tiempo en que las transacciones son realizadas, para así medir el uso que se le da a la plataforma, el objetivo es motivar a que los usuarios no solo retengan XEM, sino que también la tengan en constante movimiento a través de las diferentes transacciones.

Multifirma (Multisignature): Se refiere a las direcciones de firma múltiple que proporcionan un nivel extra de seguridad, ya que requieren más de una clave para autorizar determinada transacción. Este tipo de direcciones de múltiples firmas tienen una resistencia mayor al robo y a ataques cibernéticos que las tradicionales.

Mundo Financiero (Financial World): Este termino se refiere y/o incluye a todas aquellas actividades que tengan que ver con el intercambio y manejo de capital (bien sea dinero o activos). No se debe confundir a las finanzas con la economía, ya que a pesar de estar relacionados, no son lo mismo, ya que las finanzas están más orientadas a la administración del dinero como tal, dependiendo de la situación por la cual se atraviese.

En este mundo, se pueden escuchar muchos términos, los cuales son necesarios entender, para comprender totalmente cada definición. Entre los términos que más se utilizan, destacan los siguientes:

- Activos: Es cualquier cosa que generen ingresos, sin invertir tiempo, pero si dinero.
- Pasivos: Son todas aquellas cosas que generen perdidas. Normalmente suelen ser deudas o gastos.
- Capital: Es el dinero con el que se cuenta para realizar movimientos en el mundo financiero.
- Ingresos pasivos: Es cuando se obtiene dinero sin realizar ninguna actividad.

Básicamente se puede considerar por activos a cualquier cosa que genere ingresos, sin tener que realizar ninguna actividad (como se ha explicado anteriormente). En todos los casos, los activos si requieren algo y es la inversión de un capital, dicho capital puede variar, dependiendo del activo en el cual se quiera invertir.

Teniendo en cuenta lo anteriormente mencionado, se puede decir que los activos más rentables actualmente, son los siguientes:

1. Las criptomonedas: Uno de los activos más rentables y populares durante los últimos años, han sido las criptomonedas, las cuales han hecho que muchas personas ganen dinero, sin embargo, debido a su inestabilidad y a la gran bajada que tuvo a principios del 2018, muchas otras personas perdieron dinero.
2. Bienes raíces: Es uno de los activos más seguros en la actualidad, ya que trata de adquirir un inmueble y alquilarlo, para que este genere ingresos pasivos, sin embargo, se debe tener en cuenta que no siempre se puede considerar a un inmueble como un activo, ya que no siempre genera ingresos, ya que si se tiene una casa, pero esta no se tiene alquilada, si no que se está utilizando para vivir, dicha casa no estará generando ingresos, estará generando pérdidas.
3. Las acciones: Las acciones son los activos más populares y utilizados en la actualidad, ya que le permiten a una persona adquirir un porcentaje de una entidad y generar ingresos anuales, ya que, no solamente el valor de las acciones son las que generan las ganancias, estas también se obtienen anualmente, dicho monto se paga, básicamente por obtener las acciones durante todo el año. Cabe mencionar que las acciones pueden llegar a ser muy inestables, sin embargo, son mucho más seguras que las criptomonedas, pero en muchas ocasiones, menos rentables.

N

Naufragado / Naufrago / Naufragio (Rekt): Rekt al igual que Hodl se trata de un error ortográfico de la palabra “wrecked”, que significa naufragio. El término se refiere a un inversionistas que está completamente arruinado y destruido con pérdidas por la caída actual del precio de determinado criptoactivo.

Niños pagan por el Padre (Child pays for Parent): Criterio de selección de transacciones del protocolo Bitcoin para su procesamiento empleado por los mineros, en el que se toman en cuenta las comisiones de las transacciones ‘padre’ para procesarlas junto a una transacción ‘hijo’, generando una mayor rentabilidad y rapidez.

Nodo (Node): Es un ordenador conectado a la red Bitcoin que transmite transacciones a otros. En otras palabras, elemento de una blockchain que replica las transacciones o registros emitidos por los usuarios. Comprueban que el usuario que publica la transacción es el dueño legítimo del monedero implicado. Una vez comprobado envían la transacción a los mineros para que comprueben la liquidez de la transacción. En otras palabras, un nodo son los equipos que forman parte de la red ‘blockchain’, encargados de almacenar y distribuir en tiempo real copias actualizadas de las operaciones que se realizan. Cada vez que se genera un nuevo bloque y se añade al gran libro de cuentas, se añade también una copia en todos los nodos de la red. Todos los mineros son nodos, pero no todos los nodos son mineros.

Nodo Federado (Federated Node): Son nodos que crean una especie de estado o comunidad política dentro de la red, en la que ejercen el consenso para validar la información y protegerse contra cualquier nodo que individualmente quiera tomar decisiones contrarias a las que piensa la mayoría. Los otros servidores, los de auditoría, garantizan la veracidad del consenso alcanzado por los servidores federados. Todos estos nodos son elegidos democráticamente por los usuarios de la criptodivisa, quienes evalúan el desempeño de cada nodo en base a su eficiencia, honestidad e intereses en la red. Es conocido que este protocolo de prueba de participación por nodos federados es mucho menos costoso, ecológico y escalable, pues prescinde de tener equipos físicos haciendo minería (lo que consume demasiada electricidad) debido a que el poder de procesamiento de un nodo se basa en la cantidad de criptomonedas depositadas en la cartera especial y la antigüedad de estas monedas. Ya que no se trata de un asunto de control de la red en cuanto al poder de procesamiento sino de posesión y antigüedad como participante tenedor de monedas, es extremadamente difícil que existan ataques de 51% en esta red, que es uno de las posibles amenazas a Bitcoin, ya que es teóricamente posible que un solo cliente acapare la mayoría de la red y tenga mayor poder.

Novato (Noob): Termino que proviene de la parte de la jerga de los videojuegos y del entorno digital en general. En el ecosistema hace referencia a una persona que no tiene experiencia en criptomonedas.

O

Objetivo (Target): Número de 256 bits incluido en la cabecera del bloque que establece la dificultad criptográfica actual para que el bloque sea procesado por los mineros y aceptado en la red.

Ofertar (Bid): Precio al que los compradores están dispuestos a comprar.

Ofertas Iniciales de Moneda – OIM (Initial Coin Offerings – ICO): Son una forma de financiación empresarial. Su particularidad reside en que lo que ofrecen las empresas son 'tokens' en vez de acciones y que sus accionistas pagan con monedas digitales, a través de 'blockchain'. Estos tokens también pueden ser la 'moneda de cambio' para tener acceso a futuros servicios o plataformas. Sin embargo, dada la falta de regulación de este tipo de financiación, en ocasiones estos 'tokens' no representan acciones o derechos económicos reales sobre la empresa que emite la ICO.

Ofertas Iniciales de Bifurcación – OIB (Initial Fork Offerings – IFO): Es el medio por el cual los mineros bifurcan una blockchain para extraer nuevas altcoins, que son equivalentes a la cantidad de altcoins circulantes que tenía la blockchain original. Los motivos para realizar una IFO son varios: ideológicos, políticos y, principalmente, económicos. Por ejemplo, las más recientes bifurcaciones de la red Bitcoin podrían considerarse IFOs: Bitcoin Platinum, Súper Bitcoin Lightning Bitcoin, Bitcoin Gold y otros.

Ofertas Iniciales de Estafa – OIE (Initial Scam Offerings – ISO): Se refiere a un juego de palabras asociado al hecho de que muchas ICO son estafas.

Onixcoin: Criptomoneda venezolana del sector privado de la República Venezolana de Venezuela.

OP_Return: Comando insertado en la salida de una transacción en los protocolos Bitcoin Core 0.9.0 en adelante que añade metadata a la transacción y evita gastarla nuevamente. Este comando puede ser utilizado para quemar bitcoins.

Oráculo (Oracle): Dispositivo computacional que puede tomar datos fidedignos e inalterables del mundo real, fuera de un entorno informático, para ejecutar algún protocolo interno de blockchain. Son sumamente útiles para la ejecución de contratos inteligentes en dispositivos de Internet de las Cosas, por lo que algunas empresas ya comienzan a utilizarlos.

Orden de mercado (Market Order): Es la instrucción de un inversor de vender o comprar una divisa de forma inmediata. Debido a la volatilidad del mercado de divisas, las órdenes de mercado se ejecutan en el precio disponible en el momento en que se ejecuta la operación. Las órdenes de mercado pueden fijarse al tipo de cambio seleccionado por el comprador para garantizar que la compra o la venta se realiza en el momento más

oportuno, minimizando los efectos adversos de la volatilidad. Cuando un cliente solicita una orden de mercado, el proveedor de divisas supervisa los movimientos en los tipos de cambio y ejecuta la operación cuando el tipo seleccionado por el cliente es alcanzado. Esto es posible en gran medida gracias a la automatización a través de plataformas en línea a través de las cuales se pueden comprar y vender de forma inmediata.

Oso / Osuno (Bear / Bearish): Señales de que una divisa / criptodivisa va a de precio. También es un término tomado de la jerga de Wall Street y se refiere a un inversionista (trader) que considera que el precio de cierta criptomoneda se desplomará y quiere sacar provecho de la caída. Cada vez que el precio de bitcoin o del mercado de criptomonedas en general cae, se puede ver como estos 'osos' salen de sus cuevas.

Oso Ballena (Bear Whale): Se refiere a aquellos poseedores de grandes cantidades de monedas que apuestan a la caída del precio de un criptoactivo. Son los grandes inversionistas que tienen un visión negativa del mercado y colocan grandes ordenes de venta en las casas de cambio.

Output (salida): es el destino de una transacción. Lo más habitual es que se trate de una dirección, pero también puede haber transacciones con más de una dirección de destino y, por tanto, varias salidas.

P

P2P: Concepto que hace referencia a una red de igual a igual (Peer-To-Peer), es decir, una red descentralizada donde todas las partes interactúan entre sí. Son las interacciones descentralizadas entre dos partes o más en una red altamente interconectada. No es sinónimo de blockchain. Los participantes de una red con estas características se tratan directamente entre sí a través de un único punto de mediación, eliminando la influencia de las terceras partes. Es una de las características más resaltantes de tecnologías como blockchain y ciertas plataformas de intercambio de criptoactivos.

P2SH² (P2SH^2): Propuesta para que la información adicional registrada en un bloque de la red sea difícil de cambiar.

Pago en moneda local (Payment in local currency): Es una transacción en la que un comprador paga a su proveedor extranjero en la divisa local del proveedor. Las empresas que tradicionalmente han realizado pagos internacionales a proveedores de bienes y servicios en su propia moneda están optando cada vez más por pagar a sus proveedores en moneda local. Esto incluye a fabricantes, proveedores de servicios a empresas y también colaboradores externos individuales que proporcionan servicios subcontratados o que trabajan como autónomos para una empresa extranjera. A medida que la creciente globalización y el aumento de la competitividad llevan a las empresas a acceder a mercados extranjeros, las PYMES confían cada vez más en ofrecer sus productos y servicios en el exterior. Por este motivo y de forma inevitable, la moneda en la cual se realizan los pagos ha pasado a ser una cuestión fundamental en el comercio internacional.

Papel Amarillo (Yellow Paper): Documento Técnico escrito por Gavin Wood, cofundador de Ethereum, donde se incluyen especificaciones técnicas sobre la blockchain de Ethereum además de las expuestas en el papel blanco de esta plataforma. Es el documento técnico que está destinado a proporcionar las reglas definitivas para todos los equipos que ejecutan el software de Etereum.

Papel Blanco (White Paper): Es un documento en forma de guía cuya función es tratar de explicar a los usuarios cómo resolver un problema o ayudarlos a entender un tema determinado. En el caso de la Minería Digital es un documento que describe la tecnología subyacente en detalle de cualquier Criptomoneda y con el que quedan establecidos los fundamentos de la misma a nivel tecnológico y comercial.

Par (Pair): Cotización de una moneda contra otra. Ejemplo: Par btc/eth, btc/usd.

Parar de Perder – PP (Stop Loss – SL): Es una cantidad que se indica en una Casa de Cambio (Exchanger) para vender automáticamente cierta cantidad de X divisa / criptodivisa si el mercado toca ese valor mínimo.

Paridad (Parity): Cliente de Ethereum implementado en el lenguaje de programación Rust. Es uno de los principales clientes de Ethereum, utilizado tanto por servicios de cartera como por aplicaciones descentralizadas.

Patrón Oro (Gold Pattern): Es un sistema monetario que, básicamente, consiste en establecer el valor de la moneda de un país en relación a la cantidad de oro que este posea. Al nivel más elemental, el poseedor de un billete de cierto valor contaría con el derecho a intercambiar ese billete por una cantidad de oro proporcional según el tipo de cambio que su nación estableciera. A nivel nacional, cada país basa o basaba su cantidad de dinero en circulación directamente con la cantidad de oro que poseía custodiado en sus reservas. El modo de funcionar, por lo tanto, consistía en la libre importación y exportación de oro para equilibrar su balanza de pagos, haciendo del oro la base monetaria por naturaleza.

El patrón oro constituyó el sistema monetario que se utilizó de forma más o menos constante desde Waterloo hasta la Primera Guerra Mundial. Era muy simple: los billetes podían intercambiarse por oro, y el oro a su vez en billetes, a una tasa de cambio fija e inviolable. La tarea diaria de un banco central consistía en facilitar este intercambio. Casi todo el activo del Banco Central era oro y casi todo su pasivo eran los billetes en circulación que en su conjunto valían lo mismo que el oro.

Pececillo (Minnow): Se trata de alguien que tiene una pequeña cantidad de criptomonedas, considerado como un pez pequeño dentro del ecosistema.

Pedir (Ask): Precio al que los ofertantes están dispuestos a vender.

Petro: El PETRO (PTR) es el primer criptoactivo emitido por un Estado. El PETRO (PTR) esta respaldado por la República Bolivariana de Venezuela y la riqueza de sus grandes reservas de petróleo crudo.

Petrodólar (Petrodollar): Es un dólar estadounidense obtenido a través de la venta de petróleo, es decir, es una petrodivisa en dólares. El término fue acuñado por Ibrahim Oweiss, un profesor de economía de la universidad de Georgetown, en 1973. Oweiss pensó que era necesario un término para describir la situación que ocurría en los países de la OPEP, donde la venta de petróleo le permitía a esas naciones prosperar económicamente e invertir en las economías de otras naciones que compraban su petróleo.

Después de la Segunda Guerra Mundial se creó un sistema internacional mediante el cual los dólares se convirtieron en moneda de reserva del mundo. Se acordó que cada dólar fuera respaldado por una cantidad fija de oro. El acuerdo era que cualquier país que tuviera dólares, siempre tenía la opción de canjearlos por oro físico. La idea era crear una mayor confianza y estabilidad en el comercio internacional, lo que se logró durante cerca de veinte años. Este acuerdo puso a los Estados Unidos en una posición particularmente ventajosa; no muy diferente a un banco comercial que opera un sistema de reserva fraccionaria, finalizando la privatización (conversión) del Gobierno de EEUU y luego todo el funcionamiento de su sociedad.
En 1975, todos los miembros de la OPEP acordaron vender su petróleo sólo en dólares estadounidenses. Cada nación importadora de petróleo en el mundo comenzó a ahorrar sus excedentes en dólares estadounidenses con el fin de poder comprar petróleo; con la alta

demanda de dólares se fortaleció la moneda. Además de eso, muchos países exportadores de petróleo como Arabia Saudita pasaron a invertir sus excedentes de dólares en bonos del Tesoro americano, con esto Estados Unidos consiguió una fuente profunda y permanente para financiar sus gastos. El sistema del petrodólar fue un movimiento político y económico brillante. Obligó al dinero del petróleo del mundo a fluir a través de la Reserva Federal de Estados Unidos, creando cada vez una mayor demanda internacional, tanto en dólares como de deuda pública de los Estados Unidos, mientras que en esencia Estados Unidos obtiene el petróleo del mundo prácticamente de forma gratuita, ya que el valor del petróleo está denominado en una moneda que los Estados Unidos controla e imprime. El sistema del petrodólar se extiende más allá del petróleo, la mayor parte del comercio internacional se realiza en dólares estadounidenses.

Pirámide (Pyramid): Se refiere a una organización que se configura aceptando constantemente inversiones con contratos bloqueados, con el fin de apropiarse del dinero de los inversionistas. La constante inversión mantiene la estructuras operando, esto hasta que ya no puedan soportar la demanda de pagos, cuando generalmente colapsan.

Plataforma de Minería (Rig): Equipo de computo (Ordenador) especializado para la minería digital, que principalmente consiste en varias tarjetas gráficas (GPU) unidas para incrementar el nivel de hasheo sobre una Criptomoneda.

Pool de minería (Mining Pool): Es la agrupación de dos o más mineros que juntan su poder de cómputo para elevar las posibilidades de resolver un bloque y obtener una recompensa. En los pools de minería, la recompensa se divide internamente en función de la cantidad de hashes aportados por cada uno de sus integrantes.

Precio de Compra / Venta (Purchase – Bid / Sale Price – Ask): El precio de compra es el que un comprador está dispuesto a pagar para adquirir un determinado activo (como por ejemplo una divisa), mientras que el precio de venta es el precio mínimo que el vendedor está dispuesto a aceptar para vender ese activo. La diferencia entre ambos precios se conoce como separación (spread). En el mercado de divisas, en particular, esta cantidad es a menudo manipulada por algunos operadores con el objetivo de aumentar sus propios beneficios. En efecto, el spread funciona como margen, pues significa un aumento sobre el precio de venta original. La variación entre el precio de compra y precio de venta suele ser un indicador de la liquidez de un mercado. Un mercado muy líquido, como es el Forex, tiene normalmente spreads estrechos, mientras que mercados menos líquidos, como por ejemplo las acciones de empresas no cotizadas, que suelen tener spreads mayores. En todo momento un activo, por ejemplo, las acciones de activo, tiene dos precios: el de compra y el de venta. Estos dos precios son el bid y el ask. El bid es el precio que se ofrece (el precio de compra). El ask es el precio que te piden (el precio de venta).

Preminado o Minado instantáneo (Premine or Instamine): Se refiere a aquellas blockchain que al momento de su inicio ya existía un número de tokens. Estos tokens normalmente se reparten entre los micro-mecenas que financiaron el proyecto o quedan bajo el control de una fundación que se encarga de financiar/recompensar el avance y desarrollo de la plataforma.

Procesador (Processor): Es parte del hardware de muchos dispositivos, no solo de tu computadora. El procesador es el cerebro del sistema, justamente procesa todo lo que ocurre en la PC y ejecuta todas las acciones que existen. Cuanto más rápido sea el procesador que tiene una computadora, más rápidamente se ejecutarán las órdenes que se le den a la máquina. El procesador es una pastilla de silicio que va colocada en el socket sobre la placa madre dentro del gabinete de la computadora de escritorio, la diferencia en una portátil es que está directamente soldado. Entonces, la **CPU** (por sus siglas en inglés, **Central Processor Unit - Unidad Central de Procesamiento**) se conecta a un zócalo especial que se encuentra en la Placa Base de cada ordenador, al que se le debe añadir un sistema de refrigeración consistente en Disipadores y Ventiladores (conocidos como Coolers), además de añadir entre el zócalo y la cápsula una Pasta Térmica que tiende a mejorar la conductividad térmica.

Procesador (Pasarela) de Pagos (Payment Processor): Un procesador de pagos es básicamente un medio, sistema o herramienta a través del cual podemos realizar compras a través de Internet y recibir pagos Online. A través de algunos de ellos podemos disponer de Tarjetas Mastercard o Visa prepagadas virtuales y/o físicas que nos permitirán retirar dinero por cajeros automáticos, realizar pagos a través de puntos de venta e incluso, comprar Online.Los puede haber de Monedas Fiduciarias como Paypal o de Criptomonedas como BitPay que permite a los comerciantes aceptar bitcoins como forma de pago, obteniendo al final de la transacción la criptomoneda o dinero fiduciario según su preferencia, además de ofrecer servicios de Cartera (Billetera / Wallet) de bitcoins.

Propuesta para mejorar bitcoin (Bitcoin Improvement Proposal – BIP): Es un estándar que permite proponer cambios o mejoras potenciales para la blockchain Bitcoin, apostando a que estos cambios afectarán de manera positiva en el protocolo de la red.

Prueba de Capacidad (Proof of Capacity – POC): Es un algoritmo de consenso que recompensa por a los usuarios por *'minar'* usando espacio en un disco vacío, es decir, realmente no se hace nada con ese espacio en disco, solo se tiene que probar que está ahí disponible para ello. Típico en la Blockchain de la Criptodivisa Burst, en la que se exige mantener la computadora encendida 24/7 para poder minar, pero que a su vez hace el proceso de minería muy eficiente en energía y virtualmente a costo cero.

Prueba de Conocimiento Nulo (*Zero Knowledge Proof - ZKP*): También llamado Protocolo de conocimiento cero, es un protocolo criptográfico que establece un método para que una de las partes pruebe a otra que una declaración (generalmente matemática) es cierta, sin revelar nada más que la veracidad de la declaración. Las pruebas de conocimiento cero no son pruebas en el sentido matemático del término, porque hay una probabilidad pequeña, el error de solidez (soundness error), de que un probador engañoso será capaz de convencer al verificador de una declaración falsa. En otras palabras, que son probabilistas y no deterministas. Sin embargo, hay técnicas para disminuir el error de la solidez a valores insignificantes.

Prueba de Importancia (Proof of Importance – POI): Es un algoritmo de consenso en el núcleo del software NEM. Cuanto mayor sea su importancia, mayor será su oportunidad de poder calcular un bloque (y recoger los honorarios dentro de ese bloque). POI ajusta su importancia dependiendo de cuántas transacciones hace un usuario, con quién las hace y

otra serie de factores. Si no realiza ninguna transacción, el POI establecerá su importancia basándose únicamente en su saldo, es decir, un algoritmo POS (Proof Of Stake) tradicional.

Prueba de Participación (Proof of Stake – POS): Algoritmo de consenso que propone validar transacciones no con un poder de cómputo sino con la cantidad de unidades que poseas de una criptomoneda en específico. Es decir, mientras más unidades poseas, más posibilidades tienes de recibir una recompensa. Esto podría tener analogía a depósito a término fijo, en el que dejando tu dinero una cantidad de tiempo recibes una recompensa en intereses. POS se usa en algunas criptomonedas en conjunto con POW para hacer más segura la red.

Prueba de Servicio (Proof of Service – POSe): Es un algoritmo de consenso que recompensa al minero mediante la posibilidad de mejorar sus ingresos por medio del uso y la ejecución de un nodo especial que proporciona servicios a la red, que por lo general, ayuda a proporcionar transacciones anónimas a otros usuarios. Esto es común en la Blockchain de la Criptodivisa Dash.

Prueba de Recursos (Proof of Resources – POR): Es un algoritmo de consenso que recompensa por que recompensan a los mineros de diferentes maneras y por diferentes factores, tales como la cantidad de un tipo de procesamiento matemático en particular que puedan realizar o recursos que puedan poner a disponibilidad de los usuarios de la Blockchain.

Prueba de Trabajo (Proof of Work – PoW): Algoritmo de consenso que consiste en un tipo de trabajo que realiza un cliente, que por lo general es la realización de un cómputo en un ordenador, ese trabajo es verificado en el servidor. Lo común es que estos cómputos deben ser difíciles para el cliente pero debe ser fácil de verificar por el servidor. En Bitcoin se usa POW para verificar transacciones y generar nuevos bloques, este proceso se conoce como minado (mining).

Protocolo (Protocol): Reglas consensuadas y oficiales bajo las que los participantes de una red descentralizada interactúan, se conectan entre sí y comparten diversa información sobre la red, en otras palabras, un protocolo es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información.

Puesta en marcha (Startup): Empresa emergente. Se usa para hacer referencia ideas innovadoras que se apoyan en la tecnología y están empezando o en construcción.

Punto Porcentual (Porcentual Point): Es una medición utilizada en intercambio de divisas para representar los movimientos de los tipos de cambio en porcentajes. Un pip equivale a 1/100 de 1%. Se trata, pues, de la cantidad mínima que puede desplazarse un tipo de cambio. En FX, los tipos de cambio se cotizan en un máximo de 4 puntos decimales, en los que un pip es representado por el cuarto decimal. A menudo, los pips se utilizan para ilustrar las variaciones de un tipo de cambio entre dos divisas. Por ejemplo, si la cotización de EUR/USD 1,3275 se desplaza hasta 1,3300, hay una diferencia de 25 pips. En ese momento se necesitan 25 pips, o 0,0025 dólares menos para comprar un euro que antes de producirse ese desplazamiento.

Punto mas alto (All time high – ATH): Es decir, el tope más alto de todos los tiempos. Esto significa que el precio de cierta criptomoneda a la que se hace referencia con esta expresión ha roto todos los récord pasados, en cuanto a precio y se está comerciando al precio más alto de su historia.

Q

Quemar (Burn): Destrucción de criptodivisas por parte del desarrollador o institución patrocinadora.

R

Ratón (Mouse): Es el dispositivo de entrada para la introducción de ordenes gráficas (por pantalla) al computador.

Red de Ejecución de Delitos Financieros – REDF (FinCEN (Financial Crimes Enforcement Network): Es una agencia dentro del Departamento del Tesoro de Estados Unidos, que se ha destacado en los últimos años por ser el organismo gubernamental que ha empezado a regular los intercambios comerciales con criptomonedas.

Red de Pruebas (Test Network): Entorno de pruebas donde los desarrolladores pueden generar y gastar criptoactivos falsos en una red blockchain similar a la verdadera.

Red de Rayo (Lightning Network): Es una red descentralizada que utiliza la funcionalidad de contrato inteligente en blockchain para permitir pagos instantáneos a través de una red de participantes. Lightning Network permitirá que las transacciones de bitcoin ocurran instantáneamente, sin preocuparse por los tiempos de confirmación de bloque. Este protocolo intenta resolver el problema de escalabilidad de bitcoin, ya que trata de ser un sistema descentralizado para micropagos instantáneos y de alto volumen que elimina el riesgo de delegar la custodia de fondos a terceros de confianza. En la red Lightning, los pagos no necesitan confirmaciones de bloque y son instantáneos y atómicos. La atomicidad implica que los pagos se realizarán o no: no es posible que queden a medias en caso de algún fallo. Además, permite enviar fondos tan pequeños como 1 satoshi, o 0,00000001 BTC, sin riesgo de custodia y comisiones inmateriales. Las transacciones de la red Lightning se llevan a cabo fuera de la blockchain en principio, sin delegación de confianza ni propiedad, lo que permite a los usuarios realizar transacciones casi ilimitadas entre ellos.

Red informática (Computer network): Es el conjunto de técnicas e interconexiones físicas utilizadas para conectar entre sí en un sistema principal a dos o más equipos informáticos, con el objetivo de intercambiar toda clase de información y los periféricos a gran velocidad. La Internet es conocida como la red mas grande. El medio empleado para conectar y transmitir la información puede ser de manera guiada por cables de cobre de dos hilos, cables coaxiales o fibra óptica, y de forma no guiada se encuentra la red por radio, por microondas o infrarrojos. El alcance de conexión de la red informática puede ser local o de forma remota. Desde la red más sencilla, una computadora puede estar conectada con la de su vecino. Y sucesivamente conectándose a más computadoras en un mismo edificio, una ciudad o el mundo.

Reemplazar con la comisión (Replace-By-Fee – RBF): Este término se refiere a las operaciones que los usuarios realizan para retransmitir una transacción anterior pero con una tarifa más alta. Esta operación anula la transacción original, pues es sobrescrita por la nueva.

Reorganización (Reorganization): es la denominación que recibe el proceso mediante el cual la cadena de un bloque que se está trabajando deja de alargarse. Los bloques de la vieja bifurcación se vuelven bloques huérfanos y pierden validez.

Retención a largo plazo (Long term hold): Es la posición que toma un inversionista frente a determinada criptomoneda. Seguir esta estrategia implica que el inversionista asume que su valor aumentará considerablemente en el futuro.

Retorno de Inversión (Return on Investment – ROI): Se refiere a cuánto ganó o perdió un inversionista desde que compró determinada criptomoneda.

Riesgo de transacción (Transaction Risk): Son los efectos negativos potenciales de las variaciones en el tipo de cambio durante el periodo comprendido entre la suscripción de un contrato y su posterior liquidación. Cuando dos empresas que trabajan en divisas diferentes se comprometen a una transacción mediante un contrato, el intervalo entre la suscripción de dicho contrato y la liquidación del pago representa un periodo de riesgo, que viene dado por la volatilidad del tipo de cambio, puesto que los tipos de cambio pueden fluctuar de forma considerable en un breve espacio de tiempo, perjudicando a una de las partes del contrato. Para evitar ese perjuicio, las empresas a menudo recurren a productos de cobertura del riesgo, como son los seguros de cambio o las opciones. Los efectos potencialmente adversos del riesgo de transacción pueden causar verdaderos estragos; la variación repentina de un tipo de cambio puede provocar que una empresa tenga que pagar mucho más para satisfacer el pago de una compra en la divisa de su proveedor. Asimismo, tienen el potencial de que los beneficios disminuyan o se desplomen, e incluso pueden llegar a provocar el impago.

Robot (Bot): Programa que hace operaciones automáticas de X tipo para unos u otros.

Ronda de Financiamiento Inicial – RFI (Initial Financing Round – IFR): Jornada en que las empresas desarrolladoras de plataformas blockchain ofrecen a los inversionistas una cantidad determinada de criptomonedas a cambio de financiamiento capital para ejecutar su proyecto.

Ruta de la Seda (Silk Road): Fue un mercado en línea (ubicado en la Deep web) utilizado para la compra de productos ilícitos y en la cual, la principal forma de pago fue el bitcoin. Fue cerrada a finales del año 2013 luego de que el FBI arrestara a su propietario, Ross Ulbricht.

S

Sabiondo (Poser): Persona que parecer saber mucho pero no sabe tanto de lo que desea demostrar con sus intervenciones y/o declaraciones. Generalmente promociona paginas o servicios fraudulentos (Scam).

Salida de Cambio (Change Output): Dirección blockchain que en su salida puede retornar bitcoins al remitente si el monto estipulado para pagar la comisión de la red era más alto de lo que se necesitaba.

Salida Multi-Firma (Multi-Signature Output): Dirección blockchain que incluye dos llaves públicas necesarias para firmar cualquier transacción saliente.

Satoshi: Es la subdivisión más pequeña que puede obtener de un bitcoin, a saber: 0.00000001 BTC.

Satoshi Nakamoto: Es el seudónimo utilizado por la persona o grupo de personas que desarrollaron el protocolo de Bitcoin. Está retirado desde 2010.

Separación (Spread): También conocido en español como horquilla, es la diferencia en un momento dado entre los precios bid y ask. Es decir, es la diferencia entre el precio de oferta y demanda para un determinado valor. Puede emplearse como indicador de la liquidez de un valor (menores spreads indicarían más liquidez), aunque también es posible que se vea influido por otros factores. El término 'spread' es, en sí mismo, enormemente polisémico en el campo de las finanzas. Puede referirse a: La diferencia existente entre la demanda (bid) y la oferta (ask) de un mercado y también puede referirse al diferencial de rentabilidad entre un producto y otro que le sea comparable (p.e. se habla de spread o diferencial crediticio entre el bono alemán y el español).

Servicio de mezcla (Mixing Service): Un servicio que mezcla tus bitcoins con los de otra persona, devolviéndote bitcoins con diferentes entradas y salidas de las que le enviaste. Un servicio de mezcla (también conocido como Vaso/Glass) conserva su privacidad porque impide que las personas rastreen un bitcoin en particular. También tiene el potencial de ser utilizado para el lavado de dinero.

Sistema Internacional de Pagos de China (Cross-Border Interbank Payment System - CIPS): Es un sistema de pago que ofrece servicios de compensación y liquidación para sus participantes en pagos y transferencias transfronterizas en moneda china (Reminmbi RMB, también conocida como Yuan). Es una infraestructura básica para los mercados financieros en China. Se propone el sistema de pagos internacionales como alternativa a los sistemas SWIFT (Estados Unidos) e IBAN (Europa). El CIPS entró en funcionamiento el 8 de octubre de 2015 con 19 bancos tanto chinos como extranjeros que se establecieron en China continental y 176 participantes indirectos que cubrían 6 continentes y 47 países y regiones. El 25 de marzo de 2016, CIPS firmó un memorando de entendimiento con SWIFT con la

comprensión mutua de la implementación de SWIFT como un canal de comunicación seguro, eficiente y fiable para la conexión de CIPS con los miembros de SWIFT, que proporcionaría una red que permite a las instituciones financieras enviar y recibir información financiera. transacciones en un entorno seguro, estandarizado y confiable. CIPS a veces se conoce como el Sistema Interbancario de Pagos de China. Luego de China con el CIPS le ha seguido Rusia con la creación del suyo propio, un servicio bancario lanzado recientemente como respuesta a las amenazas de sacar al país del SWIFT. Bajo el nombre de 'Sistema de transferencia de envíos financieros' o SPFS, el protocolo está diseñado para hacer pagos a nivel nacional.

El potencial de ambos sistemas de funcionar en el exterior es enorme gracias, precisamente, al potencial de las economías rusa y china en el comercio entre Europa y Asia. Se espera que los bancos de la Unión Económica Euroasiática puedan operar a través del SPFS y que China haga lo propio con el suyo aplicándolo a lo largo de toda la Nueva Ruta de la Seda, el proyecto llamado a conectar el intercambio comercial desde el extremo este de Asia hasta Europa.

Las intenciones de Rusia y de China también se dejaron ver en octubre de 2017, cuando el gigante asiático abrió en Moscú la primera sucursal de su Banco de Industria y Comercio, basado en yuanes. La entrada en Rusia del Yuan no es exclusiva. En estos momentos, el país ya ha acordado con Turquía, con Irán y con Azerbaiyán deshacerse de la moneda estadounidense.

Sistema Monetario Internacional (International Monetary System): El Sistema Monetario Internacional (SMI) es el conjunto de instituciones, acuerdos y normas que rigen las transacciones comerciales y financieras entre distintos países. El Sistema Monetario Internacional establece las normas que regulan los flujos monetarios transfronterizos (esto es, entre distintos países). Entre sus principales objetivos se encuentran garantizar la libertad de intercambio internacional y prevenir desequilibrios monetarios que podrían afectar la credibilidad del sistema.

Los objetivos oficiales:

- **Marco común:** proporcionar un sistema de reglas y normas ampliamente aceptado de modo que los países puedan entenderse e intercambiar flujos comerciales y financieros libremente
- **Convertibilidad:** asegurar la convertibilidad de las divisas a través de un sistema de intercambio internacional (en donde el tipo de cambio es el precio relativo de las monedas)
- **Liquidez:** proporcionar y asegurar suficiente liquidez para que los flujos entre países no se vean restringidos artificialmente
- **Ajuste:** corregir, en la medida de lo posible, los desequilibrios en balanza de pagos de los países. Lo anterior puede incluir otorgar facilidades de financiamiento
- **Medios de pago mundiales:** crear y desarrollar medios de pago internacionalmente aceptados.

En el SMI participan un conjunto de instituciones financieras entre las que están:

- Fondo Monetario Internacional (FMI)
- Banco Mundial (BM)
- Banco de Pagos Internacionales (BPI)

Sistema Operativo (Operating System): Es el conjunto de programas informáticos que permite la administración eficaz de los recursos de una computadora es conocido como sistema operativo o software de sistema. Estos programas comienzan a trabajar apenas se enciende el equipo, ya que gestionan el hardware desde los niveles más básicos y permiten además la interacción con el usuario. El sistema operativo cumple con cinco funciones básicas: el suministro de interfaz al usuario, la administración de recursos, la administración de archivos, la administración de tareas y el servicio de soporte y utilidades.

SHA-256: es la función criptográfica utilizada como base para la prueba de trabajo que permite minar bitcoins y otras criptomonedas.

Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales (Society for Worldwide Interbank Financial Telecommunication – SWIFT): Es una organización que tiene a cargo una red internacional de comunicaciones financieras entre bancos y otras entidades financieras. SWIFT es una Sociedad Cooperativa bajo legislación belga, propiedad de sus propios miembros con oficinas alrededor de todo el mundo.

En otras palabras, El Sistema SWIFT es propiedad de una cooperativa internacional y el proveedor más importante del mundo de servicios de mensajería financiera segura. Que le ofrece a la comunidad internacional una plataforma de mensajería, normas de comunicación y productos y servicios que facilitan el acceso y la integración, la identificación, el análisis y el cumplimiento con la regulación. Una plataforma de mensajería, con productos y servicios, que conectan a más de 11.000 organizaciones bancarias y de valores, infraestructuras de mercado y clientes corporativos, en más de 200 países y territorios. Aunque SWIFT no posee fondos ni gestiona cuentas en nombre de sus clientes, le facilita a la comunidad internacional de usuarios una comunicación segura y un intercambio de mensajes financieros estandarizados de una forma fiable, con lo cual posibilita los flujos financieros globales y locales, mientras apoyan las operaciones comerciales en todo el mundo.

Software: A diferencia del Hardware, el Software comprende todas las partes no tangibles de un sistema informático. Es decir, los programas. El software de una computadora es todo aquel desarrollo informático que le permite al usuario de un equipo de computación ordenarle al mismo que realice una tarea. También se deben subdividir en diversas categorías en base a las funciones que realizan en el sistema: Sistemas Operativos y Aplicaciones, es decir, Software de Sistema y Software de Aplicaciones. Software es una secuencia de instrucciones que son interpretadas y/o ejecutadas para la gestión, redireccionamiento o modificación de un dato/información o suceso. Software también es un producto, el cual es desarrollado por la ingeniería de software, e incluye no sólo el programa para la computadora, sino que también manuales y documentación técnica.

Software de Aplicación (Application Software): Se le llama software de aplicación a todos aquellos programas utilizados por los usuarios para la concreción de una tarea, y en este grupo podemos encontrar software del tipo ofimática, de diseño gráfico, de contabilidad

y de electrónica, por solo citar una pequeña fracción de todas las categorías de aplicaciones que podemos encontrar en el mercado. Por ende, un Programa se trata de aplicaciones y recursos que permiten desarrollar diferentes tareas en una computadora (ordenador), un teléfono u otros equipos tecnológicos. Para desarrollar un programa informático, se necesita apelar a los lenguajes de programación que posibilitan el control de las máquinas. A través de diversas reglas semánticas y sintácticas, estos lenguajes especifican los datos que transmite el software y que tendrá que operar la computadora.

Software de Sistema (System Software): Este grupo comprende el sistema operativo, controladores de dispositivos, utilitarios de sistema y toda aquella herramienta que sirva para el control específico de las características de la computadora.

Software privativos y cerrados (Privative and closed Software): Es todo programa amparados bajo licencias que reservan algunos o todos los derechos de uso, copia, modificación y distribución para el fabricante, quien previo pago de una regalía concede el uso de una copia ejecutable del programa al titular de la licencia. El usuario no es dueño del software que está funcionando en su computador, el propietario sigue siendo el fabricante y no faculta al usuario a realizar ninguna modificación en él, ni a tampoco estudiarlo por ninguna vía para determinar como realiza sus funciones.
Software Libres y Abiertos (Free and Open Software): Es todo programa que pueda ser utilizados, copiados, modificados y redistribuidos libremente por sus usuarios con o sin costo previo para adquirirse, es decir, no necesariamente gratis.

Software Web (Webapps): las Aplicaciones y Servicios en linea, también conocidos como **Aplicaciones web (WebApps – Webware) o Software como un Servicio (Software as a Service - SaaS)** están adquiriendo una mayor popularidad, especialmente ahora que el acceso a Internet de banda ancha está más extendido y está disponible para más usuarios. No hay que descargar ni instalar las aplicaciones y servicios online en tu ordenador para empezar a usarlos, solo tienes que abrir un navegador y acceder a ellos online. No se trata únicamente de ahorrar espacio en el disco duro, puesto que no necesitan instalación, sino también de poder trabajar con archivos que están guardados en Internet desde cualquier ordenador y desde cualquier lugar, sin necesidad de llevar contigo un dispositivo de almacenamiento, ni siquiera una memoria USB. Además, no tienes que preocuparte por los diferentes Sistemas Operativos, puesto que estas aplicaciones y servicios son multiplataforma y se ejecutan en tu navegador como un cliente. Tampoco tienes que preocuparte de actualizar las versiones de tu software, ya que vas a recibir cualquier actualización de software o corrección de fallos automáticamente cuando accedas a los programas.

Sostener – Sostenedor (Hold / Hodl – Holder / Hodler): Cada vez que alguien utiliza esta palabra quiere decir que prefiere conserva o quiere conservar su criptoactivo en espera de que adquiera más valor en el futuro. Hodl: originalmente un error ortográfico de la palabra “Hold”. La primera vez que apareció fue en el foro de discusión de Bitcoin en el año 2013, y vino de un usuario identificado como GameKyuubi bajo el hilo “I AM HODLING”. Cada vez que alguien utiliza esta palabra quiere decir que prefiere conservar su criptoactivo en espera de que adquiera más valor en el futuro. El 18 de diciembre del año pasado cumplió 4 años desde la primera vez que se usó. Otro significado de Hodl proviene de la expresión “Hold On for Dear Life”, que significa “espera por la querida vida”.

T

Tasa de Hash (Hash Rate): Es la unidad de potencia de procesamiento de la red Bitcoin, es decir, que se relaciona con el número de valores hash que se pueden realizar en un periodo de tiempo dado. También se conoce como velocidad hash. Es decir, es una medida que denota el número de hashes que un minero puede realizar en un período de tiempo determinado (generalmente en un segundo).

Tarifa de Transacción (Transaction Fee): Una pequeña cuota impuesta a algunas transacciones enviados a través de la red Bitcoin. La tarifa de transacción se otorga a la minera que hashes con éxito el bloque que contiene la transacción correspondiente.

Teclado (Keyboard): Es el dispositivo de entrada para la introducción de ordenes escritas al computador.

Tecnología (Technology): Es la ciencia con la que el hombre estudia, analiza, repara y considera las mejores alternativas para poder tener una vida más plena, segura, tranquila y actual, que va en movimiento, en innovación, en evolución completa y revolucionando las diferentes industrias por todo el mundo, que van desde las mejoras cotidianas de la vida hasta las más complicadas. La tecnología es el conjunto de conocimientos con las que el hombre desarrolla un mejor entorno, más saludable, agradable y sobre todo cómodo para la optimización de la vida. La tecnología combina la técnica de mejoramiento de un espacio con las distintas revoluciones que se han suscitado en los últimos siglos, la agrícola, la industrial, la digital y otras futuras. Palabra que está compuesta por dos palabras griegas que son tekne que significa técnica, arte y logia que da una traducción de destreza, es decir, que es la técnica o destreza de algo o sobre algo.

Tecnología Financiera – TecFin (Financial Technology – FinTech): El término se utiliza tanto para la industria y ecosistema como para denotar Equipos (Hardwares) y Aplicaciones (Softwares) cuyo principal enfoque es el de optimizar las operaciones financieras, monetarias y bancarias a través de la tecnología.

Telemática (Telematic): Se define como todo el proceso mediante el cual se transfiere información digitalizada a larga distancia. La Telemática da cobijo a todo lo referente al contexto científico y tecnológico, abarcando el análisis, diseño, administración y aplicación de las redes y servicios de comunicaciones para el traslado, depósito y procesado de cualquier clase de información englobando todo lo que es el estudio y diseño de tecnologías. Etimológicamente el término Telemática proviene del vocablo griego “tele” que significa “lejos o distancia” y del vocablo de origen latín “matica” que significa información.

Tipo de cambio fijo (Fixed exchange rate): Se trata de una política cambiaria en la que el banco central de un país vincula la divisa nacional a otra más fuerte, a un grupo de divisas o incluso a un valor de referencia como puede ser el oro.

Tipo de cambio intermedio (Mid-market exchange rate): Es el tipo de cambio también conocido como “interbancario” o “spot” y es el punto intermedio entre el tipo de cambio de compra y el de venta en el mercado mundial de divisas. En cualquier par de divisas, el tipo de cambio varía constantemente. El tipo mid-market auténtico es reconocido universalmente como el tipo de cambio más transparente y preciso de un par de divisas, el que realmente refleja los movimientos del mercado de divisas en tiempo real. Los bancos y brókeres normalmente aplican un spread por encima o por debajo del precio mid-market –dependiendo de si el cliente quiere comprar o vender la divisa–, lo que en la práctica es una comisión oculta que se aplica al tipo de cambio real. Las plataformas de gestión de divisas de la genuina industria Fintech, aquellas que tienen la transparencia como objetivo, eliminan a los intermediarios, lo que les facilita proporcionar a sus clientes la posibilidad de ejecutar sus movimientos al tipo de cambio mid-market.

Al pedir la cotización de una divisa a un banco o bróker nos podemos encontrar claros ejemplos de lo que es el mid-market (aunque por su ausencia). En el par EUR/USD, nos pueden ofrecer un precio de compra de 1,1704, y un precio de venta de 1,0824. El precio mid-market , en este caso sería 1,1264. El banco o bróker, en este caso estaría aplicando un spread de casi un 4% en cada movimiento.

Tipo de cambio inmediato (On the spot exchange rate): se refiere al tipo de cambio del momento de un par de divisas determinado, para ser liquidado de forma inmediata. El tipo de cambio entre dos divisas viene determinado por varios factores que influyen en el valor de la divisa, como pueden ser los tipos de interés, los resultados económicos a nivel nacional o la inflación. Otro aspecto que puede afectar es el precio que los compradores de la divisa estén dispuestos a pagar y, a su vez, el que los vendedores estén dispuestos a aceptar, también denominados precios de compra y venta, respectivamente. El tipo de cambio forward difiere del tipo de cambio spot. Está basado en el último, pero en su cálculo también se aplica el diferencial de los tipos de cambio de ambos países, que puede ser positivo o negativo. El tipo de cambio forward no es un pronóstico del tipo de cambio spot futuro.

Titular de la bolsa (Baghodler): Dicesé de un inversionista que compró un criptoactivo a un precio muy alto y ha estado manteniendo dicho activo durante demasiado tiempo para no vender a perdida.

Tomar Ganancias – TG (Take Profit – TP): Es una cantidad que se indica en una Casa de Cambio (Exchanger) para vender automáticamente cierta cantidad de X divisa / criptodivisa si el mercado toca ese valor mínimo.

Toro / Torear (Bull / Bullish): Otro término tomado de la jerga de Wall Street. Se trata de un movimiento de mercado en el que los precios de las monedas están subiendo, fomentando una estampida de compras. Este efecto se notó durante finales del mes de noviembre, cuando bitcoin llegó a su ATH, alcanzando más de 20.000 dólares.

Transacción internacional (International Transaction): Es una operación transfronteriza en la que participan dos divisas diferentes, o tres si se utiliza una moneda de reserva, como el USD. Una excepción a esta norma se produce cuando dos empresas de diferentes países dentro de la zona euro realizan operaciones entre sí, pues utilizan la misma divisa: el

euro. Un ejemplo de transacción internacional en la que participan dos divisas: Una empresa con sede en Alemania compra materiales a un proveedor en EEUU, El proveedor acepta pagos en USD. Por consiguiente, la empresa alemana deberá cambiar euros a dólares para pagar el encargo. Ejemplo de una transacción internacional que implica a una tercera moneda de reserva: La misma empresa alemana también compra maquinaria a un proveedor en China. La divisa de la empresa china es el renminbi, que no es de libre conversión. Para completar la transacción, ambas partes deciden utilizar el USD como moneda de reserva. La empresa alemana cambia euros a USD para pagar a su proveedor en China.

U

Unidad Central de Procesamiento – UCP (Central Processing Unit – CPU): Es el cerebro del Ordenador, es decir, la parte de la computadora en la que se controlan y originan comandos directos que generan las diferentes funciones de la CPU. En el CPU se hacen todos los cálculos del código binario de la computadora. En general, es la parte más importante del sistema. La CPU está formada por varios componentes, entre los que destacan dos como los principales: Unidad Aritmético-Lógica y Unidad de Control.

Unidad Gráfica de Procesamiento – UGP (Graphic Processing Unit – GPU): Chip de silicio diseñado específicamente para realizar cálculos matemáticos complejos necesarios para interpretar los gráficos visuales de juegos de ordenador. Son muy adecuadas para hacer cálculos criptográficos necesarios en la minería criptomoneda ya que es un circuito electrónico especializado, creado con el fin de manipular y modificar rápidamente la memoria de una computadora dispuesta a la minería, para acelerar la creación de imágenes en un búfer de cuadros destinado a la salida a un dispositivo de visualización.

V

Vaciar / Tumbar (Dump): Realizar acciones financieras (especulativas o no) con el fin de bajar el precio de una divisa / criptodivisa para obtener ganancias rápidas y fuera de lo normal o predecible.

Verificación de pago simplificada – VPS (Simplified Payment Verification – SPV): Es un elemento presente en el protocolo Bitcoin el cual dicta que los nodos verifican cada operación haciendo uso de las cabeceras de los bloques. Con esto, los nodos pueden verificar sin descargar toda la cadena de bloques.

Vinculación federada (Federated Peg): Es una cadena lateral en la que el consenso es alcanzado cuando cierto número de partes están de acuerdo (confianza semicentralizada). Por tanto tenemos que tener confianza en ciertas entidades. Este es el tipo de Cadena Lateral Liquid, de código cerrado, propuesta por Blockstream.

Vinculación SPV (Simplified Payment Verification "SPV" Peg): Esencialmente una prueba SPV está compuesta de una lista de cabeceras de bloque que demuestran prueba de trabajo y una prueba criptográfica de que una salida fue creada en uno de los bloques de la lista. Esto permite a los verificadores chequea que cierta cantidad de trabajo ha sido realizada para la existencia de la salida. Tal prueba puede ser invalidada por otra prueba demostrando la existencia de una cadena con más trabajo la cual no ha incluido el bloque que creó la salida. Por tanto no se requiere confianza en terceras partes. Es la forma ideal. Para conseguirla sobre Bitcoin el algoritmo tiene que ser modificado y es difícil alcanzar el consenso para tal modificación. Por ello se usa con bitcoin vinculación federada como medida temporal.

Volteando (Flippening): Es la esperanza de que una altcoin sobrepase a Bitcoin en precio, transacciones, nodos y recompensa de minería. Aunque comúnmente se utiliza cuando cualquier altcoin supera la posición de una criptomoneda que está en el Top del Ranking.

X

XEM: Es el nombre de la criptomoneda que se desarrolla en la plataforma de NEM, esta comenzó a ser construida desde cero bajo la tecnología de blockchain, lo que ha permitido traer nuevas características para optimizar el rendimiento del mundo empresarial a nivel mundial.