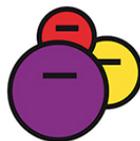


GUÍA DE CONCEPTOS PRÁCTICOS PARA CONSUMIDORES SOBRE CRIPTOMONEDAS



ADICAE CV

Asociación de Usuarios de Bancos, Cajas y Seguros



**GENERALITAT
VALENCIANA**

Conselleria d'Economia
Sostenible, Sectors Productius,
Comerc i Treball



1. ¿Sabemos lo que son las criptomonedas y como es su funcionamiento? p. 2-4
2. Como se ha desarrollado el fenómeno de las criptomonedas. Bitcoin como nuevo paradigma p. 5-6
3. El registro contable compartido o blockchain p. 7-9
4. El valor de las criptomonedas. Para qué sirven p. 9-11
5. Como adquirir criptomonedas p. 12-13
6. Los peligros de la inversión en criptomonedas. Fraudes al ahorro p. 14-17
7. Diccionario elemental de 20 conceptos sobre criptomonedas p. 18-20



1

¿SABEMOS LO QUE SON LAS CRIPTOMONEDAS Y COMO ES SU FUNCIONAMIENTO?

Las criptomonedas o también llamadas criptodivisas fueron pensadas en un inicio como un posible **medio alternativo de pago** que ha generado gran interés por distintos motivos y circunstancias. Su aparición podría entenderse como una evolución más de los sistemas de intercambio que han existido a lo largo de la historia. Son ofrecidas globalmente por Internet como alternativa al dinero de curso legal.

Las más populares son Bitcoin y Ether, pero hay más de 7.000 criptomonedas distintas en el mercado.

Por sus características, que seguidamente veremos, tenemos que tener en cuenta que no están sometidos a ninguna regulación específica. No existe por tanto una protección o garantía similar a la que podría darse en los productos financieros regulados y supervisados.

Tampoco tienen la protección de mecanismos como el Fondo de Garantía de Depósitos o por el Fondo de Garantía de Inversores, lo que las hace, cuando se utilizan a modo de inversión especulativa, un activo poco recomendable para consumidores, ahorradores o inversores no avezados.

El sistema denominado “de papel moneda”

En los últimos años del siglo pasado y principios del actual el sistema predominante ha sido el sistema denominado “*de papel moneda*”, donde los bancos centrales han tenido el monopolio para ampliar o reducir la oferta monetaria que se pone en los mercados, sin estar ligados a un tipo de cambio fijo con ningún valor, basándose, por tanto, en la confianza prestada por las personas en el hecho de que los respectivos bancos centrales no ampliarán en exceso la oferta monetaria con el fin, de esta manera, de mantener su valor y de que no se produzca una depreciación.

Las Tarjetas de Crédito y Débito

Con la aparición de las tarjetas de débito y crédito a partir los años 80 del siglo pasado surgió la posibilidad de pagar por medio de una nueva manera que no requería el intercambio de dinero en efectivo.

Estas formas más sofisticadas de intercambio requerían de unos mayores elementos de control para su seguridad, y donde las entidades financieras, supervisadas por organismos gubernamentales y supra-gubernamentales, se tenían que encargar de actuar como agentes validadores de las transacciones.

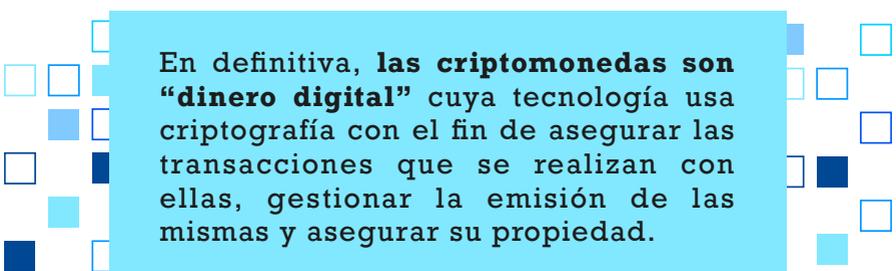
Es importante reseñar que este elemento, el de pago por tarjeta, solo afecta a la forma de pago, ya que se sigue realizando a través de contabilidad de las monedas emitidas por los bancos centrales. **Las criptomonedas pretenden ir más allá.**



Las Criptodivisas

Las criptodivisas se presentan en un primer término como una nueva tecnología, un nuevo sistema de pago para **transacciones entre personas**, de individuo a individuo, lo que se ha venido en llamar *peer-to-peer*. Por lo tanto, y ahí estriba la gran diferencia verdaderamente interesante de estas criptomonedas con otras tecnologías anteriores, en que **no necesitan de un sistema centralizado que valide sus operaciones**.

Ese es el motivo y la importancia de tratar el desarrollo y utilización de esta tecnología con cautelas, ya que podría provocar una situación de características especiales, incluso podría dar lugar a una amenaza para las políticas monetarias de los estados y de los bancos centrales, fundamentalmente porque escaparía a su control. Este es el motivo, como reacción a esta posible problemática, por el que se ha abierto la posibilidad de crear criptodivisas controladas por los bancos centrales (*Central Bank Cryptocurrencies*). Se trataría de unas criptomonedas controladas en su oferta pero donde la validación de las transacciones (*componente ledger*) se realizaría de forma descentralizada.



En definitiva, **las criptomonedas son “dinero digital”** cuya tecnología usa criptografía con el fin de asegurar las transacciones que se realizan con ellas, gestionar la emisión de las mismas y asegurar su propiedad.

2

COMO SE HA DESARROLLADO EL FENÓMENO DE LAS CRIPTOMONEDAS. BITCOIN COMO NUEVO PARADIGMA

Un sistema descentralizado

Las criptomonedas nacen con una **naturaleza descentralizada y prescindente de todo intermediario**. Se trata de un sistema libre que no conoce de fronteras ni jurisdicciones.

Aunque el fenómeno verdaderamente tiene su punto esencial con la aparición del *Bitcoin*, ahora mismo ya existen miles de criptomonedas, por lo que sus características varían y serán distintas, pero que tienen como común denominador o su homogeneidad en la utilización de lo que se ha venido a denominar la tecnología ***Blockchain***.

Desde que naciera *Bitcoin* en el año 2008 se han ido produciendo desarrollos y proyectos con esta tecnología *Blockchain*. Han aparecido nuevas monedas y *tokens* con distintos usos y aplicaciones.

Bitcoin

Bitcoin es la criptomoneda con una mayor capitalización de mercado y la que dio origen al fenómeno de las criptomonedas. Todo se inició por medio de un usuario (a día de hoy anónimo) conocido como Satoshi Nakamoto que introdujo 50 unidades de *Bitcoin* en circulación en el año 2009 con el fin fundamental de demostrar su método basado en *Blockchain*.



El interés fue tan grande que *Bitcoin* comenzó a cotizar en 2010 en bolsa.

Su funcionamiento de forma esencial lo podemos entender si lo comparamos con las tarjetas de débito o crédito, las cuales tienen que pasar forzosamente por un sistema centralizado para su validación y su efectiva realización con la intervención del propio banco y/o la empresa emisora de la tarjeta (Visa, Mastercard, American Express...).

En el caso de una criptodivisa, de *Bitcoin*, esa validación de la transacción se realiza de forma descentralizada por medio de **un sistema de libro mayor público** fiscalizado por una red de ordenadores, por lo que elimina la intervención de intermediarios financieros o tecnológicos, y son este conjunto de ordenadores los que validan la transacción.

Por ello debemos de tener en cuenta que *Bitcoin* tiene dos acepciones principales, una como **unidad monetaria**, pero también como **protocolo de red**. En la primera acepción es una moneda que sirve para intercambiar bienes y servicios, solo que a diferencia de las monedas tradicionales controladas por los Bancos Centrales, es una divisa virtual descentralizada y producida por personas y empresas de todas partes del mundo sin que exista un emisor central, no siendo controlada por nadie.



3

EL REGISTRO CONTABLE COMPARTIDO O BLOCKCHAIN

Blockchain es un **registro contable compartido**, una base de datos descentralizada y pública conocida como cadena de bloques (*blockchain*) que permite registrar transacciones realizadas a través de una criptomoneda.

El funcionamiento se concreta con la incorporación de una huella de tiempo a cada una de las transacciones, lo que da a la totalidad del registro unas características determinadas, que se concretan en que **la información es inmutable** y no puede modificarse, ni tampoco puede eliminarse.

La validación de las operaciones se realiza por el consenso de los propios **nodos de la red** estableciendo un sistema de gobernanza distribuida por el que cada uno de ellos almacena una copia completa de la cadena de bloques e incorpora las nuevas transacciones a medida que ocurren, dando fe de su validez y evitando que puedan existir duplicaciones o falsificaciones.

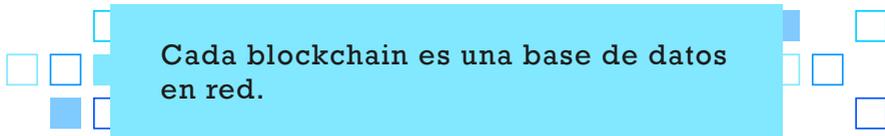
Este sistema de libro mayor público mencionado anteriormente se llama blockchain y su funcionamiento se desarrolla como un libro contable en donde se registran las entradas y salidas de dinero.

Este libro está formado por una cadena de bloques, los cuales



contienen información de una transacción en la red, enlazados, lo que permite transferencias de datos donde no hace falta un tercero que certifique la información, y cuando introduce la información, en el registro global de transacciones aparecen los elementos que han sido modificados o añadidos de manera inmutable, sin posibilidad de borrarlos.

En el caso de Bitcoin, su blockchain es una base de datos distribuida, no centralizada en ningún punto, que se actualiza cada 10 minutos con más datos e inputs.



De esta manera, cualquier bloque o información dentro de la cadena de bloques que se une a la cadena del sistema ha de ser validado, es decir, ha de estar conforme con toda la información previa presente en la blockchain.

Con cada nuevo bloque (transacción, actualización o dato), la cadena se actualiza completamente y es validada de manera descentralizada por todos los usuarios, lo que la convierte en una herramienta de almacenaje muy segura.

Se trata de una tecnología muy eficiente de almacenamiento de datos ordenados en el tiempo sin la posibilidad de poder revisarla o modificarla posteriormente. Su principal ventaja es la posibilidad de validar transacciones entre dos partes, sin que ningún agente pueda actuar de manera oportunista, y sin que éstas tengan que ser validadas por un ente central lo que ofrece un control sobre los datos

previamente desconocido.

La primera blockchain distribuida fue la conceptualizada para dar soporte y como principal estructura de Bitcoin. Más allá de Bitcoin se han creado otras blockchains, en plataformas como Airbnb, en el mercado de la electricidad, en el mercado inmobiliario, etc... todas ellas con el objetivo de registrar y validar transacciones de una forma descentralizada.

4

EL VALOR DE LAS CRIPTOMONEDAS. PARA QUÉ SIRVEN

Cada criptomoneda nace como respuesta a la solución de un problema, por ejemplo *Bitcoin* trataba de resolver la dependencia con intermediarios creando un medio de pago seguro para transferir valor sin intermediarios.

Para ello, y como fortaleza, y a diferencia de las monedas fiduciarias existentes, su emisión está restringida, y nunca crecerá por encima de una magnitud establecida.

Igualmente Ethereum permite ejecutar contratos inteligentes (smart contracts) utilizando la misma tecnología Blockchain.

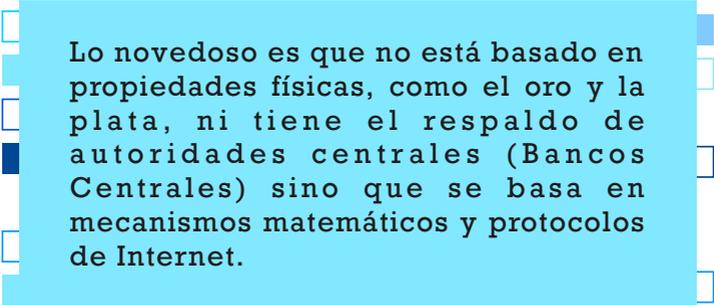


Las posibilidades de uso, por tanto, son variadas, desde alojar a múltiples aplicaciones hasta migrar procesos a la red, o incluso para aplicar estrategias de gobernanza de un sistema, o hasta como sistema de toma de decisiones sin estructura jerárquica.

Los usos de las criptomonedas son múltiples, aunque suelen ser empleadas principalmente para las actividades comerciales, son aceptadas en muchos sitios para realizar transacciones en línea, pagos en línea y fuera de la misma, o bien para inversión o para pagos comerciales.

En resumidas cuentas y atendiendo al uso fundamental como medios de pago y como inversión resulta complicado entender como una moneda virtual puede cotizar en dólares y por tanto tener un valor económico contable determinado.

Para darle explicación debemos tener en cuenta que, en principio bitcoin tiene valor porque es útil como moneda. Ya de por sí tiene las cualidades básicas del dinero, es decir, portabilidad; durabilidad; escasez; divisibilidad; reconocibilidad y fungibilidad.



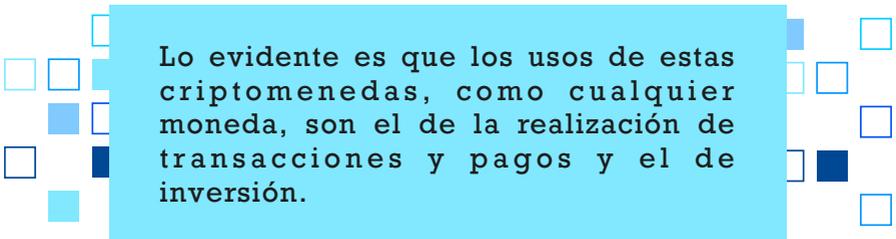
Lo novedoso es que no está basado en propiedades físicas, como el oro y la plata, ni tiene el respaldo de autoridades centrales (Bancos Centrales) sino que se basa en mecanismos matemáticos y protocolos de Internet.

Por tanto, el valor del Bitcoin se sustentaría en que es un bien escaso al haber un número limitado de bitcoins. Solo existirán 21 millones,

que requiere un gran número de recursos para su producción, siendo un activo digital y financiero que es intocable, no puede ser congelado ni incautado por el estado, no respeta fronteras políticas, lo que a la vez de ser una facilidad genera uno de los grandes problemas en cuestión de control de evasión de capitales, blanqueo de capitales, financiación de terrorismo o narcotráfico, al poder ser una moneda que no puede controlarse es utilizada por estos colectivos.

No es un problema en sí mismo de la criptomoneda, sino del uso que se le pueda dar, pero que, sin lugar a dudas, puede establecer uno de sus grandes peligros.

Podemos decir que su virtud es su pecado.



Lo evidente es que los usos de estas criptomonedas, como cualquier moneda, son el de la realización de transacciones y pagos y el de inversión.

¡Ejemplos de criptomonedas, además de **Bitcoin**, son **Ethereum (ETH)**, que es una plataforma descentralizada que ofrece Smart Contracts y Dapps (aplicaciones que usan blockchain); **Ripple**, que es una plataforma que permite realizar pagos con un coste muy bajo y en tiempo real; **Litecoin** que fue una de las primeras criptodivisas; **Dash**, que ofrece el anonimato, y otras muchas.

5

COMO ADQUIRIR CRIPTOMONEDAS

Las criptomonedas, como norma general, **se adquieren a través de las casas de intercambios o exchanges**, que son lugares donde se pueden comprar y vender las criptomonedas usando dinero fiduciario, como el dólar, euros, etc...

Un exchange, también conocido como «plataforma de intercambio» o «casa de cambio», es una plataforma que permite que sus clientes operen con activos digitales. Algunos de estos exchanges, han incorporado algunas divisas fiduciarias para ampliar y facilitar el proceso a sus clientes.

El objetivo de estos sitios es proporcionar las herramientas para poder intercambiar criptomonedas entre sí y, en algunos casos, con otros activos financieros.

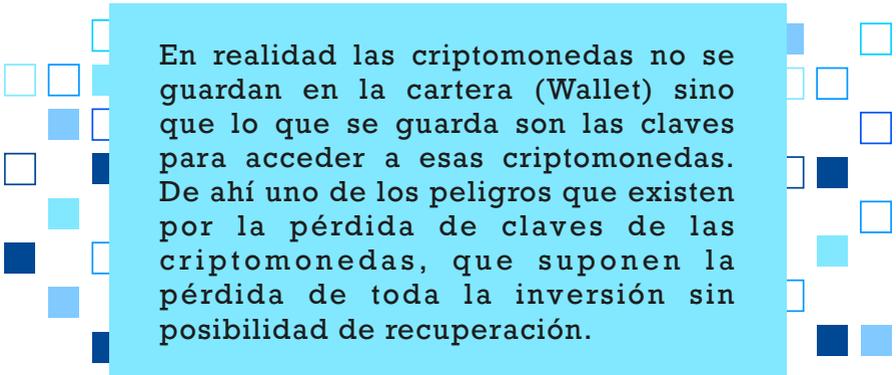
Un ejemplo de estas plataformas es **Coinbase**, que sólo permite operaciones de compra o venta de criptomonedas con dinero fiduciario en Estados Unidos, Canadá, Reino Unido, Australia, Singapur y Europa.

Otro ejemplo es **Binance**, que es uno de los mayores exchanges de criptomonedas en la actualidad, y una de sus más importantes

cualidades es que las transacciones comerciales tienen tarifas reducidas, pudiendo sus usuarios recibir hasta un 50 por ciento de descuento si la transacción se realiza con la moneda de Binance (BNB).

Otras plataformas (como ejemplo) son Cex.io, Poloniex, Bitso, etc..

Igualmente, estas casas de cambio realizan funciones de cartera (wallet) en las que se permiten almacenar criptomonedas. Pero es importante advertir que lo recomendable cuando se empieza a invertir en el mercado de las criptomonedas es crear tu propia cartera digital (es como si fuera una cuenta de valores). Aunque siempre debemos tener en cuenta que se trata de inversiones altamente peligrosas, volátiles y no recomendables para pequeños ahorradores consumidores.



En realidad las criptomonedas no se guardan en la cartera (Wallet) sino que lo que se guarda son las claves para acceder a esas criptomonedas. De ahí uno de los peligros que existen por la pérdida de claves de las criptomonedas, que suponen la pérdida de toda la inversión sin posibilidad de recuperación.

Ejemplo de carteras en línea son Blockchain, Coinbase, Xapo, Jaxx o MyEtherWallet.

6

**LOS PELIGROS DE LA INVERSIÓN EN CRIPTOMONEDAS.
FRAUDES AL AHORRO**

Aunque en ocasiones se escuche lo contrario en publicidad interesada, lo cierto y verdad es que las criptomonedas carecen de valor intrínseco, lo que las convierte, cuando se las utiliza a modo de inversión, en inversiones altamente especulativas y complejas, que pueden tener como resultado en los inversores no avezados, consumidores o ahorradores, la pérdida total de lo invertido, ya que sus precios se forman sin los mecanismos adecuados para evitar su manipulación y con criterios alejados de informaciones públicas o noticias que respalden un valor u otro.

Tienen una gran volatilidad, complejidad y falta de transparencia que las hacen inversiones muy arriesgadas. No existe, ni siquiera a nivel europeo una normativa que proporcione garantías mínimas para estas inversiones.

Sin embargo, en el año 2022 se ha publicado la Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre cryptoactivos presentados como objeto de inversión, en la que se regula la publicidad de estos activos, ya que han sido fuente de fraudes y estafas, y la publicidad enlazada a estas empresas de venta de cryptoactivos ha podido ser muy invasiva

y contraria a los derechos de los pequeños ahorradores.

Porque lo que es evidente es que las criptomonedas tienen una presencia cada vez mayor en el sistema financiero y eso requiere establecer mecanismos de protección. Puede ser este el comienzo de una regulación en ciernes impulsada por los organismos europeos.

Todos estos peligros se acrecientan cuando los que intervienen en este mercado están localizados en distintas zonas geográficas, sin jurisdicción clara aplicable o normativa que los regule o limite, no existiendo mecanismo alguno de poder solucionar cualquier conflicto o desavenencia que surja en las transacciones o en la propia inversión.

Pero si aún así quisiéramos comprar criptoactivos no debemos olvidar que antes de eso es muy **importante investigar con cierta profundidad el funcionamiento del mercado de criptomonedas** y diferenciar, por ejemplo, entre los casos en los que tratamos con una moneda, que funciona como método de pago o intercambio, y un *token*, que se vincula con valores y utilidades.

Dentro de los problemas y posibles fraudes nos podemos encontrar con el robo de monederos, que por defecto se guardan sin cifrar, lo que posibilita que aparezca **malware** específicos para ese robo de monederos, de ahí la importancia de las copias de seguridad de los monederos, pero lo relevante son los fraudes en la propia inversión, el que sea y se convierta en una burbuja especulativa, como ha ocurrido en otras ocasiones, y en este sentido son bien conocidas las fuertes fluctuaciones que experimentan estas criptomonedas que parecen propias de las clásicas burbujas especulativas.

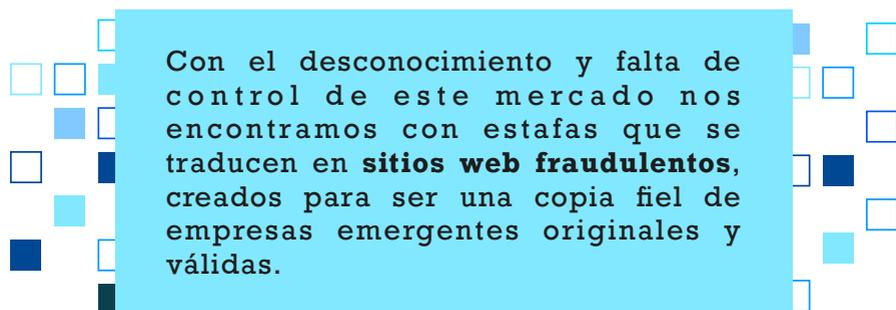
La especulación forma parte de este mercado de criptodivisas,



donde se da a estas inversiones una expectativa mayor de lo que sería razonable. Se trata de activos que compras para venderlo sin que aporte un valor.

Se trata de activos que es necesario conocer para invertir con cierta seguridad, por lo que no es idóneo para consumidores o pequeños ahorradores que desconocen los entresijos del mercado.

La realidad es que nos encontramos con que no hay una regulación específica para criptomonedas y organismos supervisores como la Comisión Nacional del Mercado de Valores (CNMV) o el Banco de España, quienes se limitan a alertar sobre los riesgos y posibles fraudes en la inversión en criptomonedas, limitándose a controlar mínimamente la publicidad de estas inversiones y a crear un registro para los proveedores de estos servicios, pensando y con el fin de controlar el blanqueo de capitales, no la protección del inversor.



Con el desconocimiento y falta de control de este mercado nos encontramos con estafas que se traducen en **sitios web fraudulentos**, creados para ser una copia fiel de empresas emergentes originales y válidas.

En estos casos es importante observar si tienen un pequeño ícono de candado de seguridad junto a la barra de URL y la dirección del sitio no inicia con "https". También existen **aplicaciones móviles falsas** de intercambio de criptomonedas que se pueden descargar. Incluso correos electrónicos de estafas iguales a los de una empresa legítima de criptomonedas. Es importante por tanto tomarse tiempo para

analizar todos los detalles de una posible inversión y su veracidad.

Las estafas y fraudes consisten básicamente en la idea de captar capital para prometer altas rentabilidades a futuro con el activo. Por ejemplo en España la mayor criptoestafa fue la de *Algorithms Group*, que ofrecía servicios de inversión en criptomonedas sin contar con la autorización de la CNMV eludiendo las obligaciones de información. Se limitaba a captar clientes que entregaban sus capitales a cambio de altas rentabilidades, pero que se dejaron de pagar a modo de sistema *Ponzi*, como cualquier estafa piramidal.





7

DICCIONARIO ELEMENTAL DE 20 CONCEPTOS SOBRE CRIPTOMONEDAS

BITCOIN es un protocolo y red de pagos entre usuarios abierta y libre, la propiedad no es de ninguna empresa ni gobierno. Se gestiona con un libro de contabilidad descentralizado llamado Blockchain a través de matemáticas avanzadas (criptografía).

BLOCKCHAIN (cadena de bloques), es un tipo de red distribuida que permite desarrollar tecnologías como las criptomonedas y lo que llamamos Internet del Valor.

CRIPTOACTIVO es representación digital de un derecho, activo o valor que puede ser transferida o almacenada electrónicamente, utilizando tecnologías de registro distribuido u otra tecnología similar.

CRIPTOGRAFÍA es una técnica utilizada para salvaguardar los datos e impedir que terceros no autorizados puedan acceder a información valiosa, alterarla para su propio beneficio o en perjuicio de otros.

CRIPATOMONEDA es una moneda virtual creada gracias a un código informatizado.

DINERO es todo activo o bien aceptado como medio de pago o medición del valor por los agentes económicos para sus intercambios y además cumple con la función de ser unidad de cuenta y depósito de valor.

DINERO FIDUCIARIO es el dinero cuyo valor no viene dado por la existencia de unas reservas que lo respalden, sino por la confianza que inspira su emisor.

ETHEREUM es una plataforma digital que adopta la tecnología de cadena de bloques (blockchain) y expande su uso a una gran variedad de aplicaciones.

EXCHANGE de criptomonedas es una plataforma en internet en las que es posible el intercambio de dinero fiduciario.

HOT WALLET es una cartera que está siempre conectada a la blockchain. Las monedas almacenadas pueden ser rápidamente intercambiadas con otros miembros de la red o ser usadas para hacer trading.

LEDGER es el Libro Mayor y consiste en un registro contable de todas las transacciones en un archivo o base de datos desde los inicios del dinero y el comercio. Las redes de tipo blockchain de las criptomonedas tienen la posibilidad de crear libros mayores digitales distribuidos.

MINERIA es el proceso de resolución de un problema matemático para dar seguridad a una red distribuida. Minar está incentivado económicamente: el minero recibe nuevas criptomonedas recién emitidas por el programa además de las comisiones de las transacciones que añade al bloque.

NODO es el conjunto de los ordenadores que se conectan a la red y disponen de una copia actualizada de la blockchain. Junto con los mineros son los garantes de que la red funcione adecuadamente.



PROTOCOLO DE RED son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red.

SMARTS CONTRACTS es un acuerdo digital entre dos o más partes, por bienes, servicios o cualquier cosa imaginable. Una vez se cumplen todos los requisitos, este se liquida automáticamente y las partes reciben lo acordado previamente.

TRANSACCIONES PEER TO PEER (p2p) son transferencias de dinero entre particulares realizadas a través de aplicaciones móviles, banca móvil, redes sociales o por Internet..

TOKEN es una ficha, una unidad de valor o moneda digital construida con criptografía que depende del blockchain de otra moneda para existir. El creador de esta herramienta decide para qué sirve y cuánto vale.

UNIDAD MONETARIA hace referencia a la moneda que se establece en un determinado país, existen algunos países donde pueden coexistir más de una moneda, pero lo normal es que tenga una única que emite el Banco Central de ese país.

WALLET (Monedero) es el software que permite almacenar y transaccionar las criptomonedas sin permiso ni mediación de nadie.

WHITEPAPER es el documento técnico que describe las principales características o propiedades de un proyecto basado en tecnología blockchain y su correspondiente criptomoneda.

Infórmate y participa para ser un consumidor crítico,
responsable y solidario con Adicae CV. Únete a la fuerza
colectiva de los consumidores y consumidoras.

NUESTRAS REDES SOCIALES



@ADICAE



AdicaeConsumidores



user/ADICAE1

NUESTRA PÁGINA WEB

comunidadvalenciana.adicae.net

VEN A NUESTRAS SEDES EN:

VALENCIA

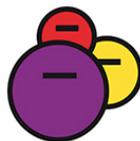
C/ Navarra 9, bajo
46008 . Valencia (Zona
Abastos, metro Ángel
Guimerá)
963 540 101

ALICANTE

C/ Arquitecto Guardiola,
15, Entresuelo A.
03007 - Alicante (Barrio
Benalúa)
965 286 538

CONTACTA CON ADICAE COMUNIDAD VALENCIANA:

coordinacionvalencia@adicae.net
963540101



ADICAE CV

Asociación de Usuarios de Bancos, Cajas y Seguros



**GENERALITAT
VALENCIANA**

Conselleria d'Economia
Sostenible, Sectors Productius,
Comerc i Treball