La guía del BITCOIN

TU MONEDA DIGITAL

EL FUTURO DEL DINERO

INTRODUCCIÓN

Seguramente has oído hablar del Bitcoin y las criptomonedas en algún lugar, pero no tienes ni la más remota idea qué es Bitcoin. La verdad es que hasta hace poco nadie lo conocía, o se asociaba a los mercados oscuros, pero esto cambió en el 2021 cuando Bitcoin alcanzó el precio de 64,854 dólares por Bitcoin desde su partida inicial que fue 0.00 dólares en el 2009.

Durante los últimos años el Bitcoin y las criptomonedas se han dado a conocer al público en general y ya no podemos decir que son futuristas, porque realmente el futuro ya se ha convertido en presente. Aunque no lo sepas, actualmente estamos asistiendo a la mayor revolución digital de todos los tiempos y lo que internet hizo por la información y telecomunicación, el Bitcoin, las criptomonedas y Blockchain lo hará por el sistema financiero a nivel mundial.

Ningún sistema informático ha estado operativo las 24 horas del día, los 365 días del año durante 12 años consecutivos, Bitcoin SÍ. Sin duda alguna, el "Bitcoin es el mejor y más justo dinero que existe"; ¿Te parece atrevida la frase? – Te retamos a que le dediques parte de tu tiempo a estudiarlo y nos contradigas la frase si aún sigues pensando que es atrevida.

Ya es hora de cambiar tu vida

Prepárate para adentrarte en, posiblemente, la mayor revolución tecnológica, social y política que ha ocurrido desde la invención de internet. Desconecta cualquier cosa que pueda molestarte y presta atención porque esto va a cambiar tu vida.

1.- INTRODUCCIÓN A LAS CRIPTOMONEDAS

1.1.- ¿Qué son las Criptomonedas?

Las criptomonedas, conocidas también como Criptodivisa o criptoactivo, son un tipo de moneda digital y divisa alternativa, las cuales se han convertido en un fenómeno mundial.

Las Criptomonedas tienen un control descentralizado, en oposición a las monedas centralizadas y a los bancos centrales, es decir, es dinero con el cual puedes realizar pagos a través de todo el mundo sin necesidad de bancos o tarjetas de crédito.

1.2.- ¿Hay otras Criptomonedas?

Sí, hay más de 10,000 monedas con diferentes utilidades. Por ejemplo, la segunda moneda más capitalizada es Ethereum y, entre otras cosas, destaca por su capacidad de ser programada en contratos inteligentes, es decir “Smart Contracts”. Los contratos inteligentes pueden permitir a los usuarios, entre otras cosas, crear un “Token ERC20” basado en Ethereum. Aunque la palabra “Token” y criptomoneda puedan parecer lo mismo, tienen algunas diferencias.

También hay otras monedas como Dash, que se caracterizan por envíos rápidos, muy baratos y anónimos. En definitiva, cada día surgen monedas, algunas de las cuales triunfarán y otras desaparecerán sin dejar rastro. Aquí podrás ver todas la Criptomonedas y capitalizaciones de cada una de ellas https://coinmarketcap.com

NOTA:

Tu Moneda Digital se va a concentrar en hablar sobre el Bitcoin que es la primera moneda y la más importante con la mayor capitalización en el mercado.

2.- INTRODUCCIÓN AL BITCOIN

2.1.- ¿Qué es el Bitcoin?

El Bitcoin es una moneda virtual y descentralizada. La red Bitcoin es la más segura del mundo y su abreviatura más común es BTC; aunque, también se puede ver con el símbolo XBT, sabiendo que la «X» indica que es una moneda sin curso legal en ningún país, como en el caso del oro y la plata.

Bitcoin es dinero libre de política económica, abierto y sus monedas no están emitidas por ningún banco, gobierno o empresa. Su diseño es tan revolucionario que ha desplazado el sistema financiero que conocemos, tarjetas de crédito, SEPA, SWIFT e, incluso, a figuras como los bancos centrales.

Administra una base de datos, llamada Blockchain, que es un libro de contabilidad que se replica por cada instalación del software, la cual se mantiene sincronizada al instante a nivel mundial.

Lo que hace especial a Bitcoin no es que sea una divisa digital, la principal diferencia, lo que de verdad hace mágico a Bitcoin, es que es una red P2P: nadie emite el dinero.

En términos generales el Bitcoin es la Criptomoneda más utilizada, y, por ende, es la más valiosa del mercado actual, por eso muchos inversionistas han decidido colocar sus ahorros en esta Criptomoneda.

2.2.- ¿Quién creó el Bitcoin?

Un desarrollador de software anónimo con el pseudónimo de Satoshi Nakamoto propuso Bitcoin en 2008. Todo empezó con el "Whitepaper" de Bitcoin, un documento explicativo sobre el concepto de una tecnología que por hoy no alberga dudas y con una presentación de estilo académico, es el llamado "Libro Blanco de Bitcoin".

El propósito del Bitcoin era crear un nuevo sistema de pago electrónico que fuera completamente descentralizado, sin un servidor o una autoridad central que lo controlase.

Por tanto, después de cultivar la idea general y la tecnología que lo sostuviera, a mediados del 2010 Satoshi Nakamoto hizo su última contribución pública al desarrollo del Bitcoin y pasó el testigo a Gavin Andresen que hoy en día es la cabeza visible del desarrollo del Bitcoin y, posteriormente, desapareció. Hasta el día de hoy, Satoshi Nakamoto sigue siendo un misterio.

2.3.- ¿Por qué se creó el Bitcoin?

En el año 2008, para superar la crisis financiera iniciada con el derrumbe de las hipotecas Subprime en los EE. UU., los principales Bancos Centrales inician una política monetaria extraordinaria y empiezan a implementar medidas no convencionales para inyectar liquidez en el sistema. La recesión global y la crisis de la deuda soberana en los países de la periferia europea, hace que la solidez de las divisas fiduciarias respaldadas por los gobiernos empiece a ser cuestionada.

La crisis financiera es la tormenta perfecta que planta la semilla para que surja una nueva moneda electrónica, el Bitcoin.

Desde el nacimiento de Internet, han existido varios intentos para crear una divisa digital. Sin embargo, como el dinero digital es sólo información, el mismo Token puede ser duplicado y gastado dos veces. La forma de solucionar este problema es que una fuente de confianza verifique si un Token ha sido ya gastado o no. Aunque para realizar esta función se puede crear una autoridad centralizada, el sistema es muy vulnerable a los ataques ya que sólo existe un solo punto de ruptura.

2.4.- ¿Quién controla Bitcoin?

Bitcoin es independiente de gobiernos, bancos y corporaciones mundiales, que da control total a los usuarios sobre sus finanzas. Ninguna autoridad puede interferir en sus transacciones, imponer tarifas de transacción o quitarles dinero a los usuarios. Además, el movimiento de las transacciones de Bitcoin se almacena en un libro público masivo distribuido llamado “Blockchain” que se explicara con más detalles en esta guía.

2.5.- ¿Cuánto vale el Bitcoin?

El precio de Bitcoin, al igual que cualquier valor en Bolsa y cualquier divisa o metal, tiene un precio libre en base a una oferta y una demanda en el mercado. Esto quiere decir que su precio cambia 24 horas al día, 7 días a la semana. Es una divisa mundial y no se para nunca.

2.6.- ¿Por qué comparar Bitcoin con otros métodos de pago?

Para poder compararlo con otras monedas y métodos de pago, debemos tomar en cuenta ciertas características que estos dos conceptos presentan o deberían presentar para ser ideales. A continuación, exploramos cuáles:

- Transferible y portable: es posible enviarlo, recibirlo y cargarlo con facilidad para adquirir bienes y servicios. En algunos casos, es incluso posible enviarlo al otro lado del mundo en tan sólo unos segundos.

- Posibilidad de realizar grandes transacciones: es posible transferir grades cantidades a manos de otra persona o entidad de forma fácil y rápida.

- Posibilidad de realizar micro-pagos: es posible transferir cantidades mínimas, como propinas a otra persona o entidad de forma fácil y rápida.

- Protegido contra la inflación: tiene un suministro establecido, es decir, que no es ilimitado porque no se puede producir cuántos se deseen. De tal manera, la inflación no será un problema, pues mientras menos haya, aumentará la demanda y por tanto el precio.

- Transacciones internacionales: puede utilizarse para enviar fondos de forma fácil, rápida y efectiva alrededor de todo el globo.

- Descentralizado: no es controlado por un ente central; como el gobierno o un banco y por tanto no es posible que se congelen, pierdan o devalúen fondos según el criterio o capacidad de ese ente.

- Transacciones privadas: la identidad no está directamente ligada a la cuenta donde se depositan los fondos.

- Seguro: tiene cierta resistencia al robo y al extravío.

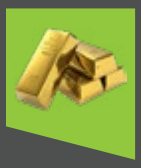
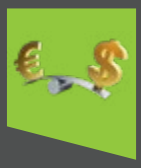
- Escalable: puede soportar miles o millones de transacciones por segundo y continuar creciendo según la necesidad.

- Divisible: es fácilmente divisible en muchas partes más pequeñas.

- Duradero: no desaparece o ni se daña con el tiempo.

- Fungible: es intercambiable por bienes, servicios u otras monedas en una proporción de igual valor.

TABLA COMPARATIVA

CARACTERISTICAS	 ORO	 FIAT	 PAYPAL	 BITCOIN
Trasferible y Portable	! (2)	✓	✓	✓
Posibilidad de Realizar Grandes Transacciones	✗	✓	✓	✓
Posibilidad de Realizar Micro Pagos	✗	✗	✓	✓
Protegido Contra la Inflación	✓	✗	✗	✓
Transacciones Internacionales	!	! (3)	✓	✓
Descentralizado	✗	✗	✗	✓
Transacciones Privadas	✗	✗	✗	! (4)
Seguro	! (5)	!	!	✓
Escalable	!	✓	✓	! (6)
Divisible	!	✓	✗ (7)	✓
Duradero	✓	✓	✓	✓
Fungible	✓	✓	✗	✓

01 A diferencia de los demás, PayPal no es una moneda, sino solamente un método de pago. A través de su plataforma se utilizan otras divisas, como el Dólar, el Euro, la Libra Esterlina etc.

02 El oro es sólo relativamente portable y transferible en su forma original. Sólo utilizando papel moneda redimible por el metal se vuelve realmente portable. Y, aun así, el papel moneda no es tan manejable como otros métodos.

03 Las transferencias internacionales en dinero fíat son posibles, pero incluyen engorroso papeleo, altos costos y tiempo valioso.

04 Bitcoin es pseudo-anónimo, pues a simple vista sólo puede verse la dirección pública, que no está ligada a ningún documento personal.

05 No existe una moneda o método de pago que sea 100% seguro. Siempre hay posibilidad de robo o extravío, tanto en lo físico como en lo digital. Sin embargo, como los Bitcoins están dentro de la Blockchain y si el usuario resguarda su llave privada, puede decirse que la posibilidad de robo o extravío es bastante ínfima, a diferencia de otras monedas.

06 Bitcoin actualmente presenta problemas de escalabilidad, pero muchos desarrolladores en todo el mundo están trabajando para resolverlos, y se están discutiendo diversas propuestas al respecto.

07 PayPal no es una moneda sino una plataforma de pago, por tanto, no es divisible ni fungible por lo que la posibilidad de robo o extravío es bastante ínfima, a diferencia de otras monedas.

2.7.- ¿Cómo obtener Bitcoin?

Principalmente se obtienen de las siguientes formas:

- 1. - Comprarlos en alguna casa de cambio de Bitcoin (Crypto.com).
  Nota: Regírtrate con nuestro código ***fpgxyfb3su*** y te regalarán $25 en CRO (ver en www.tumonedadigital.com).
- 2.- Pago por venta de bien u ofrecer algún servicio.
- 3.- Intercambiarlos con alguien.
- 4.- Minarlos.

NOTA:

Antes de que compres tu primer Bitcoin es necesario tener un Monedero o Billetera para así poder almacenar tus BTC de manera segura.

3.- INTRODUCCIÓN A LOS MONEDEROS

3.1.- ¿Qué es un monedero?

Es aquella que nos permite almacenar las Criptomonedas en wallets: (cartera o monedero) y tiene semejanza con lo que sería una cuenta corriente, la diferencia sería que con un monedero nosotros tenemos el control total de las Criptomonedas que guardamos de forma libre, autónoma y sin intermediarios.

En definitiva, los monederos son programas informáticos básicos que te permiten custodiar tus Bitcoins u otras Criptomonedas y, además, conectar con la red de Bitcoin mediante internet para autorizar una transacción monetaria. Además es necesario conocer que usamos una aplicación de monederos para generar una o varias direcciones de Bitcoin para enviar y recibir dinero. Por eso es vital que comprendas que un monedero Bitcoin puede contener varias direcciones de tu propiedad.

3.2.- ¿Cómo Funcionan los monederos?

Funcionan mediante una dirección especial que te da el monedero virtual en el cuál te hayas registrado, dicha dirección es la que debes dar a la persona y/o entidad que te vaya a transferir y esta procederá a hacer el envío, colocando la cantidad a enviar y la dirección de tu monedero.

Bitcoin y otras Criptomonedas se basan en criptografía, pero no necesitas saber grandes tecnicismos para manejar un monedero.

Es importante saber que para la protección, custodia y transacción de los Bitcoins, necesitas dos claves únicas que tu monedero generará de forma aleatoria y automática.

3.2.1.- La clave pública:

Es la dirección que podemos compartir con quien queramos y permite la recepción de dinero, similar a lo que es tu número de cuenta en un banco, es decir que con la clave, cualquiera que la tenga puede enviarte dinero, pero no acceder a tus fondos. Pero la clave pública depende la clave privada.

3.2.2.- La clave privada:

Es una contraseña que nunca debemos compartir, ya que da acceso total a tus fondos almacenados, se puede asemejar a la contraseña de acceso a tu cuenta bancaria.

Cuando se tienen las dos claves puedes acceder desde cualquier lugar, sólo necesitas instalar de nuevo el programa o aplicación (monedero) en un móvil u ordenador nuevo y restaurar tu cuenta introduciendo tu clave privada.

3.3.- ¿Tipos de monederos billeteras?

Se pueden distinguir dos tipos de monederos en base a la exposición a internet que tienen las claves de las mismas:

3.3.1.- Las hot wallets, o carteras calientes:

Son aquellas que siempre están en línea, siempre están conectadas a la Blockchain.

3.3.2.- Las cold wallets, o carteras frías:

Son aquellas que no están conectadas a internet y por tanto tampoco a la red Blockchain. Las cold wallets se usan para proteger fondos que no se quieren mover en un tiempo. Es una forma de prevenir ataques, borrados fortuitos o erróneos, y formateos de ordenador sin backup.

3.4.- ¿Cuáles son los tipos de hot wallets?

3.4.1.- Online:

Son wallets que ofrecen algunas páginas web para almacenar las Criptomonedas. Con esta opción delegamos la custodia de la clave privada y por lo tanto de nuestros fondos a dicha empresa.

3.4.2 Ordenador:

La mayoría de las Criptomonedas ofrecen su propio software que actúa como wallet. Con este tipo de wallets, la responsabilidad de los fondos recae en el usuario.

3.4.3.- Smartphone:

Son aplicaciones de smartphone que actúan como wallet y permiten realizar pagos en establecimientos que permitan pagar con Criptomonedas. También debemos asegurarnos de guardar bien la clave privada. La principal ventaja de una billetera móvil es que los fondos del usuario siempre están a la mano, es una forma muy conveniente de pagar productos escaneando códigos QR.

3.5.- ¿Cuáles son los tipos de cold wallets?

3.5.1.- Físicas (hardware):

Suelen ser unidades USB especiales para almacenar las Criptomonedas, las billeteras de hardware son dispositivos portátiles que pueden contener llaves privadas y ayudar a facilitar los pagos. Existen diferentes tipos de billeteras de hardware, pero todas ellas permiten a los usuarios cargar esencialmente cualquier cantidad de dinero en su bolsillo.

Los más populares son los desarrollados de (Ledger y Trezor), que nos garantizan resguardo de los fondos, ya que además de la clave privada, permiten programar un PIN para asegurarse de que nadie no autorizado, acceda a las monedas.

3.5.2.- Papel:

Tal vez una de las opciones más seguras para el almacenamiento de Bitcoin. Una billetera de papel es básicamente dos códigos QR, generados mediante un servicio designado. Una de ellas es una llave pública, una dirección que puede usarse para recibir BTC. El otro es una llave privada, con la que puedes gastar los Bitcoins almacenados en esa dirección. Estas suelen darse en los cajeros que permiten cambiar dinero Fiat por Criptomonedas. Suelen llevar un código o código QR, para poder acceder a las monedas, ya sea mediante Smartphone u ordenador.

3.6.- ¿Qué son monederos HD?

Viene de “Hierarchical Deterministic”. Es un monedero de dirección compleja. Un monedero que no es HD, por cada dirección nueva que crea genera una clave privada, que es la contraseña que le permite administrar esa dirección Bitcoin.

En cambio, un wallet HD parte de una “semilla” (un numero variable de caracteres). Con esa semilla, y a modo gráfico para que puedas verlo mentalmente, se genera “un árbol” donde cada “rama” posee una clave privada y de ella se saca una clave pública y una dirección Bitcoin. Con la misma semilla se puede generar el mismo árbol siempre. Es decir, si guardas tu semilla siempre podrás acceder a todas las ramas (todas las claves privadas), y con ello, a los fondos que hay en las direcciones, sin hacer ningún backup extra en el futuro, solo el inicial.

3.7.- ¿Qué es un monedero SPV?

Simplified Payment Verification. Estos monederos son una mezcla entre el monedero completo y el ligero para aprovechar ventajas de ambos, ocupan poco pero verifican criptográficamente los datos recibidos para evitar mostrar al usuario información falsa debido a un ataque al servidor.

Te permite descargar una copia completa de las cabeceras de todos los bloques disponibles en la cadena de bloques. Mediante ese proceso podemos revisar si una transacción pertenece a un bloque de la cadena sin necesidad de descargar la ‘Blockchain’ de Bitcoin completa.

3.8.- ¿Cómo se realiza la validación?

Encontramos tres elementos importantes a lo largo de todo el proceso:

- Cada transacción tiene un hash.
- Cada bloque tiene un hash.
- El hash de una transacción y el de un bloque pueden relacionarse mediante una prueba del Merkle Tree. (modelo matemático donde el bloque es la cúspide y la transacción se colocaría en una estructura similar a un árbol). Con la prueba del Merkle Tree se obtiene una lista de todos los hashes entre el bloque y la transacción.

Por lo tanto y antes de confiar en una transacción, las SPV Wallets siempre verifican:

- Prueba del Merkle Tree para comprobar la existencia de una transacción en un bloque.
- El propio bloque para validar que se encuentra en la cadena principal.

Una vez ambas respondan satisfactoriamente, estamos hablando de una transacción correcta y será añadida a nuestro monedero en forma de ingreso o gasto.

3.9.- ¿Cuáles son la wallets recomendadas para Bitcoin?

Se recomiendan las siguientes a manera de consejo, pero cada uno es libre de elegir la Wallet que quiera.

✓ Online / Web

- Binance: Sin duda es el mejor Exchange (casa de cambio) online que existe. Intuitiva, clara y completamente funcional. Esta empresa es pionera y solvente, es segura y valida para almacenar tus Bitcoins y Criptomonedas. Todas las Cripto están (SAFU) - Fondo de activos seguros para los usuarios.

✓ Ordenador

- Electrum: Una Wallet que ha demostrado durante años ser la más solvente, completa y segura que podemos tener instalada en nuestro ordenador.

- Exodus: Es simple y intuitivo, el cual es fácil de usar para los principiantes, y lo puedes usar desde tu ordenador o teléfono móvil

IMPORTANTE: Es vital mantener las wallet (Electrum y Exodus) actualizad a su última versión y solo descargar el software desde la pagina oficial.

✓ Smartphone

- Electrum: Lo mismo que su versión de escritorio (ordenador). Una app segura, eficaz y con soporte actualizado de forma continua.

- Mycelium: Una alternativa segura y funcional a la wallet móvil de Electtrum.

- Exodus: Lo mismo que su versión de escritorio (ordenador). Una app segura, eficaz y con soporte actualizado de forma continua. Esta es la mejor opción para para principiantes.

✓ Hardware wallet (físico)

- Trezor: Dispositivo electrónico físico para custodiar y gestionar tus transacciones.

- Ledger: Al igual que Trezor, Ledger es una marca de alta confianza y valoración dentro del mundo Bitcoin.

Nuestra Recomendación: Sin duda es (Ledger Nano X, con la app Ledger Live). El Trezor Model T tiene un costo de 192,39 € y el Ledger Nano X es de 119,00 €.

3.10.- ¿Cómo hacer transacciones de Bitcoin?

Mi monedero de Bitcoin realmente no guarda mis bitcoins. Lo que hace es guardar mi dirección de Bitcoin, que tiene un registro de todas mis transacciones, y por tanto sabe mi balance total. Esta dirección, es una combinación de 34 números y letras, (la clave pública). Cualquier dirección o clave pública tiene su correspondiente clave privada, que consiste en 64 letras y números, con esta información, el programa utilizado registra una firma digital, que entonces se manda a la red de Bitcoin para que se verifique.

Si quiero mandarte algo de mis bitcoins, publico la intención y el nodo escanea toda la red de Bitcoin para validar que:

- Tengo los Bitcoins que quiero mandar.
- Que no los haya mandado a alguien anteriormente.

Al confirmar la información, mi transacción se incluye en un bloque, que se introduce en un bloque previo, es por ello el término “Blockchain”.

Las transacciones no pueden ser revertidas o modificadas, porque eso significaría que todos los bloques que se hicieron después de esa transacción tendrían que ser modificados.

Puedes ver cómo fluyen las transacciones de Bitcoin en blockchain.info. Es una de las webs que dan información acerca de los bloques y transacciones que ocurren en este momento.

4.- MEDIDAS DE SEGURIDAD

4.1.- ¿Qué medidas de seguridad debo considerar?

Los Bitcoin poseen un protocolo infranqueable. La seguridad básicamente dependerá del cuidado del usuario, que debe tener en cuenta ciertas medidas de seguridad y entre esas medidas, destacan las siguientes:

4.1.1.- Gestiona tus propias claves

Es un consejo básico, pero que se nos olvide. Debes ser muy precavido con los servicios online donde almacenar Bitcoins y analizar la reputación del servicio antes de mandar tu dinero.

4.1.2.- Mantén tu software actualizado

Por regla general vas a usar un programa informático como monedero y cliente Bitcoin, y lo harás a través de tu ordenador o Smartphone. En este caso preocúpate de que todo lo que tu ordenador o teléfono móvil tiene esté actualizado y libre de programa maligno de cualquier tipo.

4.1.3.- Cifra tus claves privadas

Los mismos monederos suelen realizar el proceso para cifrar la clave privada con una contraseña o "PIN", de esa forma en el momento de hacer un envío te la pedirá, pero si alguien te roba las claves privadas deberá saber esa clave. Esto quiere decir que tu clave privada se modifica en base a esa contraseña o PIN dejando de ser útiles.

Si el monedero o generador de monederos que usas te da solo la opción de elegir tu clave privada, será el momento de elegir un texto complejo, de aproximadamente 200 caracteres alfanuméricos (con caracteres raros).

Recomendamos utilizar gestores de contraseñas como LastPass, que son muy seguros si se usan bien y te ayudan a generar contraseñas fuertes y recordarlas con riesgos mínimos. Pero cuidado, si pierdes acceso a LastPass no podrás recordar la contraseña.

4.2.- Usa doble autenticación (2FA)

Si depositaste tus Bitcoins en algún servicio web te recomendamos que, como mínimo, uses un segundo nivel de seguridad.

El factor de doble autenticación es un proceso que sirve para verificar tu identidad a la hora de acceder a un servicio web, ya que el 99% de las contraseñas se roban a través de procesos de Phishing, con un programa maligno. Es recomendable que grandes cantidades de Bitcoin no se guarden de manera online.

Con el segundo factor de seguridad se evitaría que, si alguien obtiene tu contraseña, no pueda acceder a tu cuenta, pues necesita una segunda clave única proporcionada en ese mismo momento a través de una vía alternativa.

Por ejemplo, Binance te permite hacer esto por SMS, Yubikey, 2FA o por email.

4.3.- Haz copias de seguridad

Si utilizas un monedero que no esté alojado en algún servicio online, es conveniente que hagas diferentes copias de seguridad almacenadas en distintos lugares.

Una vez hayas hecho estas copias, encríptalas con otros servicios para hacerlas incorruptibles. Puedes guardar las copias en pendrives, tarjetas SD, cds, papel, etc.

Al utilizar un monedero HD, solo necesitas hacer una copia de seguridad de la semilla. Al realizarlo te olvidas de ningún otro Backup. Si usas un monedero que no es HD, deberás hacer una copia de seguridad en cada transacción que hagas.

4.4.- Usa direcciones multi-firma.

Son sin duda una de nuestras opciones preferidas en Tu Moneda Digital, debido al equilibrio entre su baja complejidad de gestionarlos y la seguridad que aportan. Mientras que una dirección simple tiene asociada una clave privada, en las direcciones Multi-Firma se pueden asociar varias claves privadas, es decir, se necesitan varias claves para firmar una transacción y que esta se realice (se valide por los nodos y se incluya en el Blockchain). Es lo que se conoce como una dirección 2 de 3 (3 claves, 2 son necesarias).

4.5.- Mantenlos fuera de la red

Este es uno de los procesos que anexa otra capa de seguridad.

Para evitar que nadie pueda robarme las claves privadas, las almacenaré en un lugar desconectado de internet y se puede hacer de 3 maneras:

- Paper Wallets: Consiste en imprimir la clave en uno o varios papeles y almacenarlos en lugares seguros.

- Brain Wallets: Memorizar la clave privada. Para ello pueden usarse claves nemotécnicas usadas en monederos de tipo HD.

- Hardware Wallets: Son dispositivos físicos que almacenan tus claves y jamás salen de ellos. Para ello se conectan por USB/OTG y tu monedero les pasa la transacción para que el dispositivo lo firme con la clave privada. Es una de las mejores opciones para este tipo de proceso.

Puedes hacer transacciones desde un ordenador sin internet a través de lo que se conoce como “Transacciones Offline “:

4.6.- Nuestra recomendación.

Si vas a almacenar pequeñas cantidades de euros/dólares, te recomendamos usar Exodus; aunque hay mas monederos. Exodus es simple e intuitivo, el cual es fácil de usar para los principiantes, y lo puedes usar desde tu ordenador o teléfono móvil. Es importante hacer una copia de seguridad de la semilla, cífrala sí lo deseas y guárdala bien. Finalmente protege el monedero con un pin o contraseña.

Si vas a almacenar grandes cantidades, nuestra recomendación es usar un dispositivo de Hardware para tus Bitcoin o Criptomonedas. Nuestra elección es el (Ledger Nano X, con la app Ledger Live).

- 1.- Creas una nueva transacción en ordenador conectado a internet y con el monedero Bitcoin.
- 2.- Copias en un USB la transacción y la firmas con el ordenador desconectado de internet.
- 3.- Usas el USB de nuevo para llevar la transacción firmada al ordenador conectado a internet para que se envíe a la red.
- 4.- Es un proceso costoso, pero bastante seguro.

5.- ¿CÓMO COPRAR Y DÓNDE GASTAR?

5.1.- ¿Dónde comprar Bitcoin?

Hay muchos sitios en la web donde puedes comprar Bitcoin, lo mejor es siempre dirigirnos a sitios de confianza, ya sea al conocerlos por referencia de amigos que han tenido buenas experiencias con ellos o porque lo recomienda alguna web como Tu Moneda Digital. En nuestro caso te recomendamos que compres tus Bitcoins en Crypto.com ya que sin lugar a duda es una de las mejores casas de cambio y fáciles de usar.

Nota: Regírtrate con nuestro código ***fpgxyfb3su*** y te regalarán $25 en CRO (ver en www.tumonedadigital.com).

También puedes elegir una opción de compra de Criptomonedas que se adapte a tus necesidades, algunas de las cuales ni siquiera requieren acceso a Internet o una billetera BTC.

5.1.1.- Cajeros automáticos:

Los cajeros automáticos de Bitcoin aparecen en ciudades de todo el mundo.

5.1.2.- Tarjetas de regalo:

Los Bitcoins a menudo se usan para comprar tarjetas de regalo, ya que son anónimas y, en ocasiones, pueden ser más económicas que el uso de efectivo, también son una excelente forma de almacenar BTC, teniendo en cuenta la fluctuación de su valor.

5.1.3.- Intercambios:

Los intercambios ofrecen una opción inigualable de alternativas de comercialización. Ya sea que estés buscando una plataforma completa para comerciantes institucionales o una solución más simple para un comercio de una sola vez, encontrarás un intercambio que se adapte a tus necesidades.

5.1.4.- P2P:

Permite mantener tus transacciones de Bitcoin en el anonimato. Además, si no quieres lidiar con las complicaciones bancarias y vives en una ciudad, un intercambio cara a cara con un vendedor local sería la forma más fácil de comprar Bitcoins. Entre numerosos sitios web y foros, LocalBitcoins es la plataforma más popular para facilitar esas transacciones y también proporciona un servicio de custodia para proteger aún más a ambas partes y sus fondos.

5.1.5.- Una inversión de confianza:

Un fideicomiso de inversión es una forma de inversión colectiva en la que el dinero de los inversores se junta con la venta de un número fijo de acciones, que un fideicomiso emite cuando se lanza.

5.2.- Usando Bitcoin

Para poder utilizar bitcoins lo primero que debe poseerse es el equipo requerido: un dispositivo móvil o un ordenador donde poder instalar un monedero electrónico. De seguida, la opción más evidente es comprar esos Bitcoins a cambio de dinero fíat. Y, por último, sólo quedará enviarlos e incluso recibirlos.

5.3.- ¿Cómo funciona el envío de Bitcoin?

El proceso de envío de Bitcoin es muy similar al envío de un correo, tanto el emisor como el receptor poseen una dirección de correo electrónico; cada usuario posee una dirección pública y una dirección privada.

- **Dirección pública:** Es aquella que conocerán los demás, cualquier persona que la conozca podrá hacer envío de Bitcoin.

- **Dirección privada:** Es aquella que permitirá tu autenticación y de esta forma podrás acceder a los fondos que poseas en tu cuenta, así como realizar envíos. Es importante saber que debe ser mantenida en privado.

5.4.- ¿Qué puedes comprar con Bitcoin?

Bitcoin te permite comprar tíquets de viajes, ocio y tiempo libre a través de los siguientes sitios webs.

5.4.1.- Viajes y ocio

- **Expedia:** Reservas de hotel, vuelos, eventos y alquiler de vehículos permite realizar el pago de nuestros intereses para nuestras vacaciones con Bitcoin.
- **Destinia:** Especializada en viajes.
- **13tickets:** Portal de entradas para diferentes eventos y experiencias.
- **Gran Teatro Bankia Príncipe Pío:** Este teatro de Madrid permite pagar las entradas y los abonos mediante bitcoins.

5.4.2.- Tiendas digitales

Entre las más famosas destacan:

- **Showroomprive:** Para los fans de la moda.
- **Overstock:** Tienda con gran variedad de artículos, desde informática o electrodomésticos a relojes y muebles.
- **Gear Best:** La tienda de productos chinos es otra de las que ofrece la posibilidad de pagar mediante bitcoins.
- **CeX:** Tienda de productos de segunda mano de Reino Unido que está especializada en tecnología, informática, videojuegos y reparación de productos electrónicos.

5.4.3.- Informática y electrónica

- **Newegg:** Es la tienda informática minorista que mueve más volumen cada día.
- **Microsoft USA:** No está disponible en Europa, pero en Estados Unidos la compañía permite comprar licencias de Windows o de Office mediante bitcoins, sus consolas, membresías de Xbox Live y otros servicios.

NOTA:

Cada vez hay más tiendas físicas y electrónicas que admiten el pago de los productos mediante Bitcoins por diferentes plataformas de pago.

5.4.4.- General

- **Massachusetts Institute of Technology o MIT:** Permite comprar libros y otros materiales pagando con bitcoins.
- **Robapinzas:** Es una web exclusivamente de ropa.
- **Gift cards:** Existen webs que permiten comprar tarjetas regalo para Amazon, Netflix y muchas otras tiendas y servicios que aceptan este tipo de tarjetas regalo.
- **HumbleBunde:** Página especializada en packs de juegos y de otro tipo de contenido que permite donar a organizaciones benéficas.

6.- MINERIA DE BITCOIN

6.1.- ¿En qué consiste la minería de Bitcoins?

A pesar de que Bitcoin no es físico, se le llama así porque es similar a la minería de oro, solo que las de Bitcoin aún no han sido minadas por completo, y al igual que el oro, aquí también tendrás que hacer un trabajo duro para poder recibir la moneda.

De todas estas formas de obtener Bitcoins, la más compleja es la minería. Esta consiste en generar «bloques» al invertir la capacidad computacional para procesar las transacciones, es decir, un minero va a procesar las transacciones y va a asegurar la red, usando un software y hardware especializado para esto; y a cambio obtiene Bitcoins.

Los mineros reciben un nuevo problema matemático cada diez minutos y el más rápido en resolverlo se lleva las nuevas monedas que se ponen en circulación. Este problema matemático se basa en cálculos aleatorios que tienen como objetivo encontrar la solución y así obtener la validación del bloque.

En conclusión, los mineros reciben las monedas como recompensa al crear bloques de transacciones válidas y que estas se incluyan en la Blockchain.

La minería de Bitcoin utiliza equipos informáticos complejos que realizan cálculos computacionales y como compensación obtienen dos incentivos:

- Nuevos Bitcoins que se ponen en circulación.
- Las comisiones de las transacciones.

6.2.- ¿Conceptos de la minería que debemos recordar?

Nodos: Un nodo es un ordenador que ejecuta el software de Bitcoin y ayuda a que la red de Bitcoin siga siendo descentralizada. Cualquier persona puede correr un nodo, al descargar el software de Bitcoin (gratuito) y dejar abierto un puerto específico. Dejar un nodo operativo y conectado las 24 horas al día, consume energía y espacio en el disco duro, alrededor de unos 150GB de información.

Los nodos distribuyen las transacciones de Bitcoin por toda la red. Un nodo enviará información a otros nodos con los que esté conectado, que a su vez necesitarán información de otros nodos a los que ellos conozcan.

Algunos de estos nodos, son nodos mineros (conocidos como “mineros” a secas). Este grupo procesa las transacciones, las introduce en bloques y las añade en la Blockchain. ¿Cómo hacen esto? Resolviendo un complejo algoritmo matemático.

Este algoritmo necesita resolver un problema, encontrar un número que, combinado con la información del bloque y combinada con una función hash, produce un resultado entre un rango predefinido.

Resolver el algoritmo: Para ello debes ir probando combinaciones al azar. La función de Hash hace que sea imposible adivinar cuál será la respuesta numérica de ese bloque. Entonces, los mineros tienen que probar aleatoriamente un número y aplicar la función de hash y la información de ese bloque. La respuesta a este algoritmo tiene que empezar por un serial establecido de números empezando por ceros.

No hay manera de saber que número funcionará, porque dos integrales consecutivas pueden darte resultados muy variados. Pero hay más, es posible que haya diferentes números que den el resultado esperado, o tal vez no hay ninguno, en este caso, los mineros siguen intentándolo, solo que con una configuración de bloque diferente.

El primer minero en resolver el problema matemático anuncia que lo ha encontrado al resto de la red. Todos los otros mineros paran inmediatamente de intentar resolver el problema matemático de ese bloque, y empiezan a intentar encontrar el número del próximo bloque. El minero que ha resuelto el problema matemático, como recompensa, recibe unos nuevos Bitcoins por su colaboración con la red.

6.3.- ¿Cuál es la función de la minería?

La misión de la minería es básicamente, crear un sistema que permita comprobar todas las operaciones realizadas, constatar que nadie usa las monedas dos veces y que no se puedan introducir en el mercado Bitcoins falsos.

Así los mineros revisan las transacciones y juntan las últimas transacciones creadas en un grupo (bloque). El conjunto de los bloques sería algo así como un libro de contabilidad que certifica todos los movimientos y el saldo de los usuarios.

6.4.- ¿Qué es la cooperativa de minería o pool?

Es importante saber, que al tener mayor potencia de computación será más fácil resolver un bloque y por tanto obtener una recompensa. Por esta razón se crearon los pools de minería, para realizar un trabajo conjunto y así obtener una recompensa justa entre todos los miembros por el trabajo realizado.

Unirse bajo un pool garantiza más posibilidades de resolver un bloque y por tanto obtener la recompensa. Así pues, asociarnos con otros usuarios que aportan máquinas de minado nos garantiza que obtendremos una recompensa con mayor probabilidad.

6.5.- ¿Cuál es la recompensa para el minero?

Dentro del código de Bitcoin está establecido que cuando se valida un bloque, se obtiene una cantidad determinada de monedas. Cada 210.000 bloques se reducen a la mitad la cantidad de Bitcoins que se dan como recompensa, lo que se conoce como Halving.

Esto implica que el valor de cada Bitcoin tenga que aumentar para que siga siendo rentable el minado. El siguiente Halving será el 11 de mayo de 2020, que modificará la recompensa por bloque pasando de los 12.5 BTC en la actualidad a los 6.25 BTC cada 10 minutos.

6.6.- ¿Qué necesito para minar Bitcoins?

Los primeros Bitcoins se minaron mediante el procesador de los equipos informáticos, luego se dio el salto a las tarjetas gráficas debido a que las GPU (procesador gráfico) tienen más potencia de cálculo que el procesador.

El 16 de diciembre de 2009 se lanzó la versión 0.2 del software de Bitcoin que incorporaba la novedad que permitía el uso de varios procesadores en un mismo sistema. Lo que permitía la versión 0.2 de Bitcoin era el desarrollo de máquinas especializadas para la computación.

Los ASIC es un ordenador, pero que cuenta con muchos procesadores aumentando mucho la potencia de cómputo de cada uno de estos sistemas y que dejó la minería mediante tarjetas gráficas completamente obsoleta.

6.7.- ¿Cuál es la dificultad y el hashrate?

Al tener más equipos informáticos añadidos a la red aumenta la capacidad de cómputo de la red, lo que causa más competencia y es menos probable obtener una recompensa.

La dificultad es el cálculo necesario para garantizar que los bloques se obtienen cada diez minutos. Si los nuevos bloques de repente se generarán en menos de 10 minutos de media durante 2016 bloques, Bitcoin se reajustará automáticamente para aumentar la complejidad del problema. Lo contrario ocurre si de repente la media en esos 2016 bloques subiese de 10 minutos.

El Hashrate es la capacidad de procesamiento de la red de Bitcoin por cada uno de los equipos que se añaden. La suma de la potencia de todos los equipos de la red nos da como resultado el Hashrate total en la red.

6.8.- ¿Cuál es la rentabilidad del minado de Bitcoin?

Dependerá de la potencia del ASIC que tengamos y el pool en el que te encuentres. La rentabilidad depende del valor del Bitcoin, la dificultad de la red y el factor determinante: el coste eléctrico.

El precio de la electricidad será el que determine si es viable o no minar Bitcoin y si obtendremos una compensación por el trabajo realizado.

También hay que tener en cuenta el coste de adquisición del equipo y la competencia o lo que es lo mismo, la cantidad de máquinas que hay operando en la red y que suelen aumentar.

7.- BLOCKCHAIN: BLOQUES, TRANSACCIONES, FIRMAS DIGITALES Y HASHES

7.1.- ¿Qué es blockchain?

Es una base de datos que permite leer y escribir registros, y no se puede modificar nada de ella. Todos los registros que se guardan en ella están vinculados entre sí, por lo que es imposible incluir algo que sea incoherente con el resto de registros.

Además, digitaliza la propiedad de todo lo que tenga valor, lo que permite crear registros inmutables de propiedades y activos digitales que pueden ser transferidos entre las personas sin tener que requerir de un intermediario de confianza como hasta ahora (bancos, notarios, entre otros…)

7.2.- ¿Blockchain: bloques, firmas digitales y hashes?

Las Criptomonedas funcionan utilizando cadenas de bloques (Blockchain), que son listas crecientes de registros de información cifrada, cada uno encadenado al anterior con criptografía. Esos 'registros' son los bloques en los que se asientan y validan las transacciones.

Debemos conocer el contenido de un bloque en una Blockchain, tomando como referencia la Blockchain de Bitcoin y ver su funcionamiento.

7.3.- ¿Hash criptográfico?

Una función hash criptográfica es un algoritmo que cuenta con propiedades útiles para el cifrado de datos, lo que se traduce a la protección de contenido mediante el uso de claves. Al aplicarla, se toma un mensaje de cualquier tamaño, se cifra, y se consigue a cambio una cadena alfanumérica única de longitud fija (llamada digest o simplemente hash), sin importar el tamaño del mensaje original. Funciona para verificar que, en efecto, se trata de ese mensaje (o transacción) en particular y que no fue modificado antes de su entrega. Si una sola parte, aunque sea un solo punto del mensaje original, cambia, el hash (digest) también lo hace de forma radical. De esta forma, es casi imposible averiguar el mensaje original a partir del digest, y, por tanto, tampoco sería posible modificarlo.

7.4.- ¿Hash como función unidireccional?

Una función unidireccional, en matemática, se define como una función (relación entre los elementos de dos conjuntos) que es fácil de calcular, pero difícil de invertir.

Las funciones hash, sin embargo, se hacen para ser lo suficientemente difíciles de invertir. Sólo así es posible que sean útiles para la criptografía, pues revertirlas tomaría una cantidad contraproducente de tiempo y recursos. Construir un hash es un proceso matemático complejo, pero una de las formas de hacerlo es mediante funciones modulares, que asegurarían su 'unidireccionalidad'. Los datos resguardados por una función hash están seguros.

7.5.- ¿Propiedades de una función hash segura?

Para ser seguros, deben poseer cuatro características principales:

1.- Computacionalmente eficiente: Las funciones hash se utilizan en computadores. Estos computadores deben ser capaces de realizar labores matemáticas necesarias para crear un hash en un período de tiempo corto.

2.- Determinista: Esto implica que el mismo mensaje (entrada) debe producir siempre el mismo Digest (salida) cada vez que sea utilizado o consultado. El punto de un hash, para el caso que nos ocupa, es corroborar que una firma digital sea auténtica sin tener acceso a la llave privada.

3.- Resistente a pre-imagen: Significa que la salida no debe revelar ningún dato en absoluto sobre la entrada. Es por eso por lo que un hash debería tener siempre la misma longitud en el Digest, independientemente del tamaño del mensaje.

4.- Resistente a colisión: Dos o más entradas diferentes no deberían producir la misma salida (digest). Las salidas tienen una longitud determinada, a diferencia de las entradas que pueden ser de cualquier tamaño, así que el número de resultados es finito y, por tanto, propenso a colisión. Sin embargo, la meta de cualquier función hash es hacerla lo más pequeña posible.

7.6.- Los tipos de hash.

Existen numerosos tipos de algoritmos para crear hash en distintas plataformas, con diversas funciones, para autenticación de documentos y verificación de contraseñas, de firmas digitales y, por supuesto, minería de Criptomonedas. Entre los que continúan siendo efectivos, podemos mencionar el BLAKE2, MD6, Streebog y, especialmente, la serie SHA (Secure Hash Algorithm).

La serie SHA fue diseñada por la Agencia Nacional de Seguridad (NSA) estadounidense e incluye el SHA-256.

El SHA-256 produce un digest de 256 bits y 64 caracteres. Por otro lado, tenemos el SHA-3, incluido en el mismo estándar, pero con estructura diferente, pues produce digest de tamaño arbitrario. Este es el algoritmo utilizado para el sistema Ethash de Ethereum.

7.7.- Árbol de Merkle.

Sabiendo ya qué es un hash, hay que apuntar que las transacciones en una Blockchain usan hashes para cifrar los datos, pero estas líneas alfanuméricas se ordenan de forma estricta y se resumen a medida que aumenta la cadena, proporcionando un método seguro, rápido y ligero para verificar los datos. Con ese propósito está implementado el Árbol de Merkle.

El nombre del árbol criptográfico proviene de su inventor, Ralph Merkle, un científico computacional estadounidense que patentó esta estructura en 1979. Merkle, en 2019, también inventó el hash criptográfico por lo que es uno de los inventores de la criptografía de llave pública.

7.8.- Raíz de Merkle.

El principal propósito del árbol de hash es crear una raíz de Merkle. En este caso, se podría creer que de este valor provienen los valores “hoja”, pero, en realidad, el valor raíz es un resumen de todos los valores hoja.

Este resumen se crea agrupando todos los hashes de las transacciones en pares a los que, a su vez, les será aplicada de nuevo la función hash criptográfica pertinente para crear un nuevo digest que equivale a ambos. Esa es la raíz de Merkle, y hay una sola por bloque en una Blockchain.

Recordemos que cada transacción en una Blockchain tiene su propio hash, y, si hablamos de hashes creados con SHA-256, cada uno pesa 32 bytes.

7.9.- Firmas digitales.

Se trata de un sistema criptográfico que genera para sus usuarios, mediante la aplicación de algoritmos específicos, dos “claves” o “llaves”: una pública, que puede ser distribuida a cualquiera sin riesgo, y otra privada, que sólo debe ser conocida por su dueño.

Utilizando este sistema, la persona remitente puede cifrar cualquier mensaje usando la llave pública del destinatario. Una vez ese mensaje esté cifrado con esa llave pública, sólo la llave privada de ese receptor puede descifrarlo, pues ambas llaves están relacionadas matemáticamente. En este sentido, la clave pública puede ser comparada a una dirección de correo electrónico, mientras que la privada sería la contraseña.

7.10.- Proceso de una firma digital.

Hagamos un recorrido por la creación de la firma digital.

1.- Se toman los datos de la transacción y se utiliza el algoritmo SHA-256 (en el caso de Bitcoin) para cifrarlos en un hash de 64 caracteres.

2.- El hash obtenido se “combina” o se “firma” con la llave privada del usuario, dando como resultado dos números conocidos como R y S. Esa, de forma más concreta, es la firma digital.

3.- Se envían a otro usuario los datos de la transacción, la firma digital y la clave pública del emisor.

4.- Utilizando la llave pública del emisor, el sistema por parte del receptor podrá descifrar la firma digital (sin revelar la clave privada del emisor) para conseguir el hash de 64 caracteres correspondiente a los datos de la transacción, que antes el emisor había cifrado con SHA-256 y combinado con su llave privada.

5.- Como los datos de la transacción también fueron recibidos por un receptor, el sistema repite el proceso de cifrarlos con SHA-256 para conseguir el hash correspondiente.

6.- Se verifica que los hashes de los pasos 4 y 5 sean exactamente iguales. Si no lo son, esto indicaría que alguien alteró los datos o la clave pública del emisor no corresponde con su clave privada. Por tanto, la transacción sería inválida, ya que fue modificada durante su tránsito o no corresponde al dueño de los fondos.

7.11.- ¿Cuáles son las propiedades de una firma digital segura?

Existen varios algoritmos para crear firmas digitales: en el caso de Bitcoin, se usa el algoritmo de firma digital de curva elíptica (ECDSA), que toma la matemática detrás de los campos finitos y las curvas elípticas para generar las llaves públicas a partir de las privadas.

7.12.- Características para otorgar la seguridad entre los usuarios:

1.- Autenticación: Utilizar una firma digital debería asegurar al destinatario que la transacción proviene de un remitente en específico, cuya identidad puede ser verificada con matemáticas. La firma generada se basa en datos precisos y es casi imposible de falsificar.

2.- Integridad: Esta propiedad garantiza que los datos llegarán al remitente, sin ser modificados de ninguna forma durante su transferencia.

3.- No repudio: El usuario que utilizó su firma digital personal puede que no lo hizo. Por tanto, las firmas digitales también son vinculantes y controlables.

7.13.- ¿Qué es un bloque completo?

El bloque de una Blockchain se trata de un "contenedor" de datos de tamaño variable. La mayor parte de esos datos lo conforman las transacciones (en Bitcoin, un promedio de 2.188), que a su vez utilizan hashes, firmas digitales y UTXO. Además, dentro de un bloque encontramos su cabecera, en la cual registra la metadata del propio bloque; es decir, información técnica sobre su composición y validación dentro de la cadena.

7.14.- Nonce y minería

Cada bloque posee una identificación única en forma de hash. Este se crea pasando la cabecera del bloque a través del algoritmo SHA-256 (en el caso de Bitcoin). Dentro de esa cabecera se encuentra el hash del bloque anterior, así que, de forma automática, ambos bloques quedan entrelazados.

Encontrar ese hash aceptable para hacer válido un bloque es lo que se llama minería de Criptomonedas, y se implementa con la intención de hacer casi imposible la modificación de la cadena de hashes.

¿Cómo se puede encontrar ese hash aceptable para que el bloque se vuelva válido?

Ese hash debe salir de la cabecera del bloque. Pero allí se presenta un problema, porque todos los datos de esa cabecera son esenciales y no pueden ser modificados.

El Nonce: se trata de un número por completo al azar que es añadido a la cabecera del bloque como un dato adicional, sin más propósito que ser cambiado una y otra vez por los mineros para poder encontrar un hash válido.

Si el primer Nonce no funciona, se quita y se añade uno nuevo, hasta dar con un hash válido que satisfaga la condición de dificultad de la red (que esté dentro del objetivo).

Más que de número de intentos, la minería se trata de suerte, pues cada Nonce es al azar, así que otorga también un número al azar. No obstante, aquellos mineros que cuenten con mejores equipos tendrán más oportunidades, pues, después de todo, el número y la velocidad de esos intentos aumenta sus probabilidades de hallar el hash correcto en el menor tiempo posible.

7.15.- Cabecera de bloque.

La cabecera de bloque en una Blockchain incluye seis datos:

1.Versión: se trata del número que indica el nivel de desarrollo del software en el momento en que el bloque fue minado.

2.Hash del bloque anterior: es una larga línea alfanumérica que empieza con varios ceros. En Bitcoin, tiene 64 caracteres.

3.Raíz de Merkle: todas las transacciones en el bloque se unen en un solo hash, que es esta raíz.

4.Marca de tiempo: indica el momento exacto en que fue minado el bloque. En Bitcoin, se pone el número de segundos pasados desde enero de 1970.

5.Objetivo (target): es el número de 256 bits que indica a los mineros cuál puede ser el hash correcto.

6.Nonce: número adicional al azar que los mineros utilizan para encontrar un hash válido para el bloque.

8.- VENTAJAS DEL BITCOIN

8.1.- ¿Cuáles son las ventajas del Bitcoin?

- 1.- Rápido: Enviar cualquier cantidad de dinero, es cuestión de minutos, no importa cantidad o destino.
- 2.- Barato: El costo de realizar una transferencia a cualquier parte del mundo a través Bitcoins, es de céntimos o gratis.
- 3.- Global: Puedes enviar Bitcoins a cualquier país del mundo, no tiene fronteras.
- 4.- Emisión descentralizada: Ningún gobierno ni banco central puede interferir en la valoración del Bitcoin, ni en su creación ni distribución.
- 5.- Propio: Tus Bitcoins te pertenecen al 100%; no puede ser intervenido por nadie, no hay corralitos, ni las cuentas pueden ser congeladas.
- 6.- Dinero programable: Bitcoin es simple de implementar y lleva todo un lenguaje de programación, permite crear pedazos de código que se ejecutarán en la transacción.
- 7.- Cifrado y distribuido: Bitcoin es muy seguro, tiene en su núcleo, y en las operaciones, uno de los sistemas criptográficos más potentes que existe. Su carácter distribuido lo hace resistente a caídas de la red o ataques. Es el único sistema informático que ha estado operativo las 24 horas del día, los 365 días del año durante 12 años. Algunos de sus nodos se encuentran en bunkers de la segunda guerra mundial.

- 8.-Transparente: Todas las transacciones son públicas, y son visibles en tiempo real con pseudónimos en forma de dirección Bitcoin. Cualquiera puede desvelar la dirección Bitcoin que gestiona mostrando con absoluta transparencia donde va el dinero.
- 9.- Código abierto: Bitcoin es un software abierto, libre y gratuito. Cualquier persona del mundo puede ver su código fuente, estudiarlo, auditarlo o mejorarlo a diario.
- 10.- Basado en consenso: Bitcoin opera bajo el sistema de consenso como eje fundamental y cambia si la mayoría acepta este cambio. Lo mismo ocurre con el libro de contabilidad, el Blockchain: solo si la mayoría de los nodos dan por válida la transacción ésta queda aceptada y registrada en el libro de cuentas.
- 11.- Emisión limitada: Nadie puede generar miles de bitcoins en vista de que jamás existirán más de 21 millones y todos van apareciendo por la minería, siempre bajo unas reglas que son totalmente públicas.
- 12.- Sin barreras: En Bitcoin eres tu propio banco, no pagas coste adicional ni comisiones, tener un monedero es gratis y te permite almacenar todos los bitcoins que desees, así como enviarlos a cualquier parte del mundo.
- 13.- Privado: Bitcoin tiene un concepto claro, y es que no es completamente anónimo, pero trabaja para serlo.
- 14.- Divisibilidad: La unidad más pequeña de Bitcoin es llamado un Satoshi. Es una cien millonésima parte de un Bitcoin. (0.00000001) Lo que hace posible las micro transacciones que los pagos electrónicos no pueden permitirse.

9.- BITCOIN Y LOS COMERCIOS

9.1.- ¿Por qué Bitcoin les gusta a los comercios?

Parte de las razones es que, en Bitcoin, un pago no puede ser revertido, además es gratis de implementar, y sus costes de transacción son insignificantes, esto permite que los comercios, puedan ofrecer descuentos en el precio del producto si paga con Bitcoin.

Bitcoin les permite a los comercios:

Ahorro en transacciones: Lo que se traduce en que disminuirán el gasto en comisiones dado que con Bitcoin los costes de transacción rozan la gratuidad sin importar la cantidad de dinero que envíes.

Sin fraudes: NO existe forma de falsificar un Bitcoin, al contrario que con el efectivo.

Mayor conversión: En los comercios, es importante ofrecer diversas plataformas de pago ya que mientras más ofrezcan, más posibilidades de conversión tienen. Por tanto, si incluimos a Bitcoin en sus diferentes formas de pago, aumentarán las conversiones.

Reducción del riesgo de robos: Nadie puede acceder al dinero sin tu consentimiento, por lo que se reduce el riesgo de robos. No se necesita utilizar una caja, ni caja fuerte, ni compañías que transporten tu dinero a un banco, agilizarás la velocidad de los pagos y mejorarás la calidad de trabajo de los empleados.

Marketing: Las innovaciones están muy bien vistas por el público. Cuantas más tecnologías y mejoras proporcionen, más valorará eso el cliente y más le visitará. Bitcoin marca la diferencia de tu empresa.

Sin fallas humanas: Elimina los errores de todo tipo a la hora de verificar los pagos, ya que es un sistema automático y rápido.

Inmutabilidad: Evita el fraude conocido por los comercios como “Chargebacks”.

10.- ESTATUS LEGAL DE BITCOIN

10.1.- ¿Es legal Bitcoin?

Su estatus legal, actualmente, se encuentra en pleno desarrollo en todo el mundo, por lo que es muy usual que en la mayoría de los países aún se encuentre en medio de un vacío jurídico en el que bien podría aplicarse el principio de prohibición de Hans Kelsen: “Todo lo que no está prohibido, está permitido”. Por lo general Bitcoin no es ilegal, pero todo depende de cada jurisdicción.

En algunos países como Japón, ya tiene un estatus establecido como método de pago y no como moneda. En Reino Unido, es tratado como divisa (moneda extranjera). En España es considerado un bien digital. En Latinoamérica no se considera una moneda de curso legal, pero no está regulado. Sólo en Bangladesh, Bolivia, Ecuador y Kirguistán está oficialmente prohibido.

10.2.- ¿Pueden heredar mis Bitcoins?

En caso de un fatal acontecimiento, puede ser de utilidad usar el monedero Multi-Firma donde puedes crear una configuración de copias de claves guardadas en cajas fuerte o lugares que tras tu muerte serán heredados.

Es importante conocer a Smart Contracts, que serán capaces de enviar tus bitcoins a quien tú decidas una vez fallezca

TU MONEDA DIGITAL

EL FUTURO DEL DINERO

10.3.- ¿A quién seguir?

• Andreas. M. Antonopoulos: Es autor de Mastering Bitcoin (Dominado Bitcoin) y los libros de Internet del Dinero. (@aantonop)

• Adam Back: Es cofundador y CEO de Blockstream, que proporciona fondos para el desarrollo del Bitcoin Core, cliente de referencia de Bitcoin. (@adam3us)

• Alex Tapscott: Es coautor del libro "Revolución Blockchain". CEO de Northwest Passage Ventures, una empresa de asesoramiento que construye negocios de Blockchain. (@alextapscott)

• Barry Silbert: Es fundador y CEO de Digital Currency Group, una compañía de capital de riesgo que se enfoca en el mercado de divisas digitales. (@barrysilbert)

• Brett King: Lidera Breaking Banks, podcast global sobre fintech. (@BrettKing)

• Brian Armstrong: Es cofundador y CEO de Coinbase. (@brian_armstrong)

• Charlie Shrem: Es fundador de la Fundación Bitcoin y Desarrollador de Negocios en Jaxx, billetera de criptomoneda móvil. (@CharlieShrem)

• Erik Voorhees: Es escritor, emprendedor y economista de sillón. CEO de Coinapult, un servicio que permite a los usuarios de bitcoins enviar la moneda a cualquier número de teléfono celular en los EE. UU. O Canadá, o a cualquier dirección de correo electrónico. (@ErikVoorhees)

• Gavin Andresen: Es el desarrollador principal de Bitcoin y científico jefe de la Fundación Bitcoin. (@gavinandresen)

• Jon Matonis: Es un Director Fundador de la Fundación Bitcoin. CEO de Hushmail, un servicio de correo electrónico seguro que permite a los usuarios enviar y recibir correos electrónicos privados y encriptados. (@jonmatonis)

• Nick Szabo: Es un científico informático que diseñó un mecanismo para una moneda digital descentralizada llamada "Bit Gold" en 1998. (@ NickSzabo4)

• Patrick Byrne: Es fundador y CEO de Overstock, primer minorista importante que acepta Bitcoin como forma de pago. (@OverstockCEO)

• Peter Wuille: Es un desarrollador del Bitcoin Core y cofundador de Blockstream. Es responsable de importantes mejoras en Bitcoin. (@pwuille)

• Roger Ver: Es un inversionista en los startups de Bitcoin que incluyen Bitcoin.com, Blockchain.com, Zcash, BitPay, Kraken y Purse.io. (@rogerkver)

• Charlie Lee: Es un creador de Litecoin. Ex-Director de Ingeniería en Coinbase. (@SatoshiLite)

• Tyler Winklevoss: Cofundador y CEO de Gemini, intercambio de Bitcoin. Uno de los gemelos Winklevoss, que demandaron a Mark Zuckerberg por el concepto de Facebook. (@tylerwinklevoss)

• Vitalik Buterin: Es cofundador de Ethereum y cofundador de Bitcoin Magazine. (@VitalikButerin)

• Cameron Winklevoss: Es cofundador y presidente de Gemini. (@winklevoss.)

• Wences Casares: Es CEO de Xapo. (@wences)

RECUERDA.

Recuerda que los movimientos de dinero en Bitcoin son irreversibles, si te roban no puedes llamar a ninguna autoridad central para que cancelen el envío y te devuelvan tus Bitcoins. Ni el mismo Satoshi Nakamoto puede hacer esto.

Si te han robado los Bitcoins debes contactar con la policía, concretamente con el departamento de seguridad lógica (o su homólogo en tu país) que es quien se especializa en estos aspectos.

"Las monedas virtuales, quizás en particular el Bitcoin, han capturado la imaginación de algunos, infundido temor entre otros, y confundido al resto de nosotros". – Thomas Carper, Senador de los Estados Unidos.

TU MONEDA DIGITAL

EL FUTURO DEL DINERO