Criptomonedas: Impacto Social y Futuro

Autor: Alejandro Fernández Trigo (alefertri1@alum.us.es) - G1 TI

Asignatura: Tecnología, Informática y Sociedad – TIS

Fecha: Curso 20/21 – Marzo/Junio 2021

Temáticas: criptomonedas, *bitcoin*, cadena de bloques, *blockchain*, *proof of work* (PoF), *proof of stake* (PoS), divisas electrónicas, ethereum.

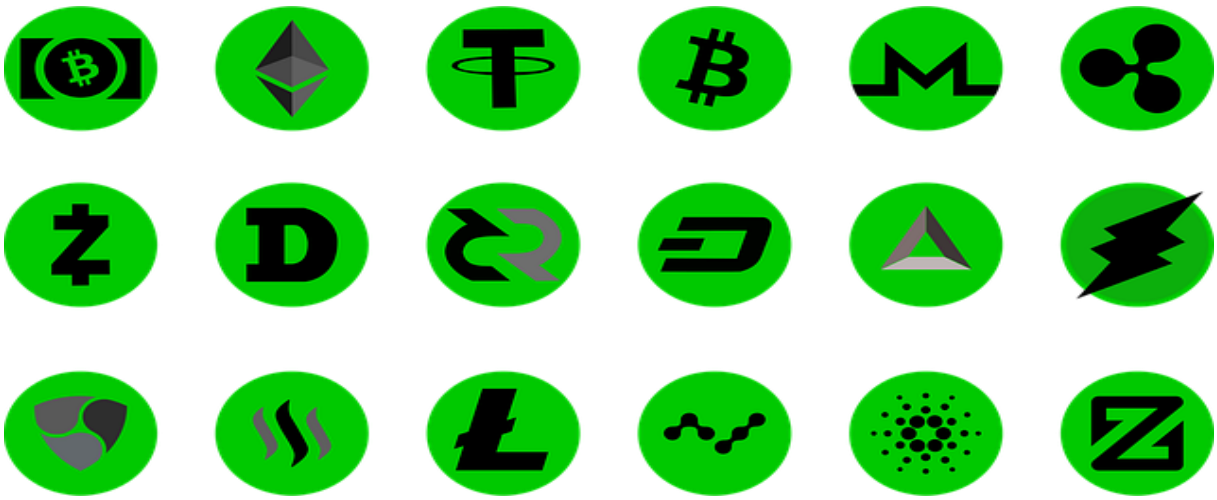
Resumen: El presente trabajo abarca el concepto de criptomonedas o divisas electrónicas; los principios de su funcionamiento (cadena de bloques y técnicas de actualización de la *blockchain*) y el impacto que han tenido en la sociedad y cómo definirán el futuro próximo.

Índice:

Introducción al tema

Vamos a empezar por definir qué y qué no son las criptomonedas. A menudo se confunden conceptos y se mete en el mismo saco a criptodivisas y monedas virtuales como tokens o similares, intercambiables por dinero fiduciario (dinero *fiat*) y que nada tienen que ver con las criptomonedas y su carácter privado.

Entonces, ¿qué son las criptomonedas? Las criptomonedas, criptodivisas, criptoactivos o monedas digitales criptográficas, es un nuevo tipo de divisa (como podría ser el euro, el dólar, etc.) cuyos orígenes se remontan al año 2009/2010 (nacimiento del Bitcoin), pero que a diferencia del dinero fiduciario (control centralizado), estas NO disponen de un ente controlador. Esto es, ninguna entidad las regula, emite, controla su precio y/o operabilidad; en su lugar, existen gracias a una base de datos descentralizada (*blockchain* o cadena de bloques) lo que les da la propiedad descentralizada que las caracteriza.



Algunos iconos de criptomonedas conocidas.

Piense el lector un momento en que propiedades tiene el dinero que usa a diario, pongamos, por ejemplo, euros. Este dinero, llamado dinero fiduciario, dinero fiat o dinero corriente, es emitido por los bancos centrales y su control se releva a las entidades públicas como el BCE (Banco Central Europeo) y el FMI (Fondo Monetario Internacional).

Esto implica varias cosas; por un lado, el dinero es controlado por entidades que atienden a intereses políticos quienes pueden emitir moneda a placer y, por otro lado, el valor del dinero emitido no atiende al valor de un material o bien de respaldo; en su lugar, se basa en una promesa de pago por parte de la misma entidad que emite el dinero. En definitiva, es un dinero cuyo control escapa al propio usuario final.

Conocimientos previos

Las criptomonedas tienen su origen en el nacimiento del *Bitcoin* en 2009 pero sus fundamentos se remontan a mucho antes; dado que la base que soporta la existencia de las criptodivisas, la llamada cadena de bloques (*blockchain*), se basa en principios criptográficos de clave pública, anteriores al *Bitcoin*.

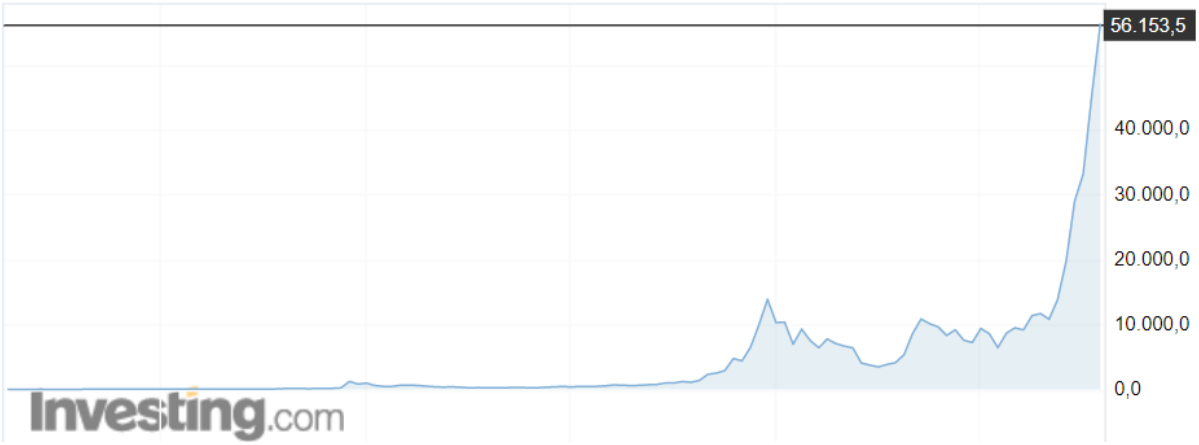
En la década de los 80 ya existían sistemas monetarios (como eCash, que luego evolucionaría hasta crear DigiCash) pero que, aunque se basaban en sistemas criptográficos, no eran independientes en tanto que dependían de sistemas centralizados.

Para la década de los 90 ya había indicios de sistemas de pago criptográficos privados que buscaban separar las transacciones de valor de un ente central. La agencia de seguridad nacional de los Estados Unidos de América, la NSA, ya investigaba a finales de los años noventa métodos para ello como se describe en el informe "*How to make a Mint: The Cryptography of Anonymous Electronic Cash*" escrito por Laurie Law, Susan Sabett y Jerry Solinas, y ahora desclasificado para su consulta con fines educativos.

Años más tarde, un desarrollador anónimo conocido como Satoshi Nakamoto (cuya identidad real sigue siendo desconocida hasta la fecha), daba a conocer en 2009 la primera criptomoneda conocida, el Bitcoin. Es aquí donde parte este trabajo.

El bitcoin, al igual que sus sucesores, emplea criptografía de clave pública SHA-256 y un algoritmo conocido como Sistema de Prueba de Trabajo o *Proof of Work* (PoW). Tras su crecimiento, nuevas criptomonedas han ido emergiendo (y otras tantas desapareciendo) apoyadas en la misma tecnología hasta llegar hasta nuestros días. No obstante, como vamos a ver a continuación, la tecnología de criptodivisas está evolucionando a pasos agigantados hacía nuevas alternativas: Prueba de Participación o *Proof of Stake* (PoS) y Prueba de Participación Delegada o *Delegated Proof of Stake* (DPoS).

Veremos estas tecnologías y su impacto a lo largo del trabajo.



Evolución del Bitcoin a lo largo de su historia hasta el día de hoy. Datos ofrecidos por Investing.com.

Terminología, conceptos y definiciones

- Dinero: entendemos por dinero a cualquier activo que empleamos en nuestro entorno como método de pago entre individuos y/o entidades.
- Dinero fiduciario (*fiat*): el dinero *fiat*, como hemos visto antes, es dinero sin respaldo real más que la confianza que los usuarios tienen en la entidad que emite dicho dinero.
- Patrón oro: sistema en el que el dinero es respaldado por un activo físico, real que posee valor propio debido a la escasez de dicho material. En el caso del patrón oro, el dinero está respaldado por una reserva de oro (escaso).
- Criptografía: ciencia que abarca las técnicas para codificar información con el fin de mantener la confidencialidad de los datos.
- SHA-256: Algoritmo de Hash Seguro o *Secure Hash Algorithm*; es un estándar criptográfico cuyo número SHA-X indica el tamaño en bits del bloque cifrado.
- Criptomoneda: como hemos visto antes, una criptomoneda es una unidad monetaria virtual (no física) respaldada por un base de datos no centralizada.
- Cadena de bloques (*blockchain*): un tipo de base de datos de carácter descentralizado que basa su funcionamiento en algoritmos criptográficos para mantener un registro distribuido, lo que permite a las criptomonedas funcionar de forma independiente.
- Prueba de trabajo/participación (PoW/PoS): protocolo para el consenso que se emplea en bases de datos descentralizadas para consensuar como se actualiza la información.

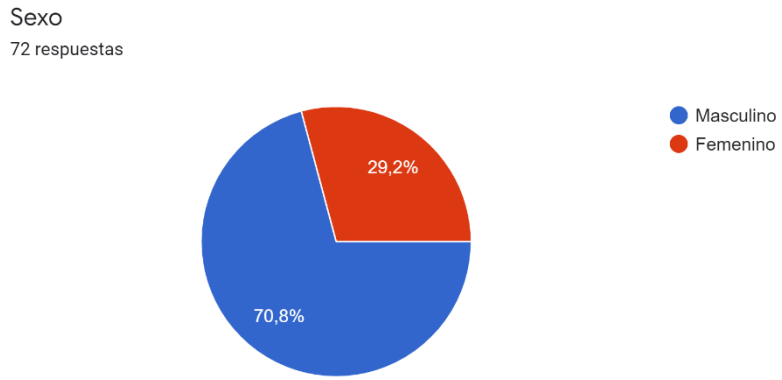
Encuestas (percepción pública)

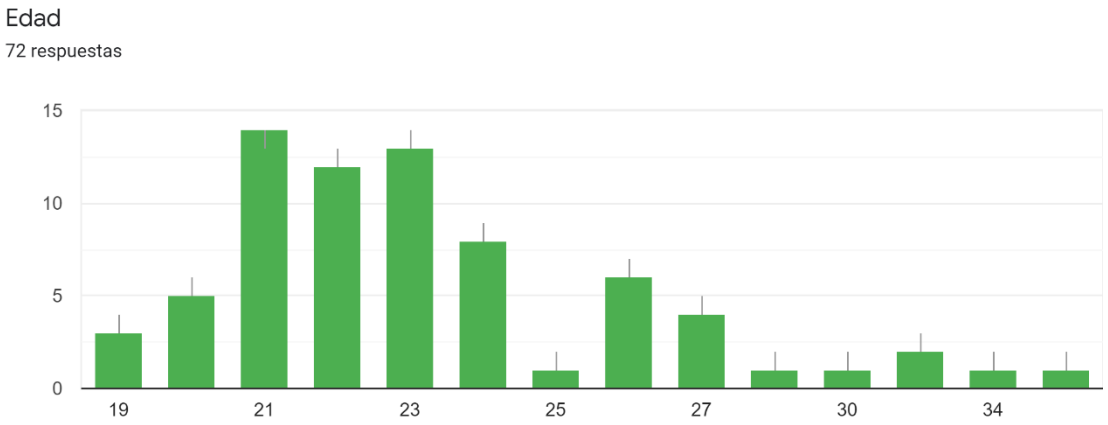
Para el desarrollo del trabajo se ha recogido la opinión de múltiples personas, de distinto género, edad y ámbito con el fin de entender mejor la percepción que tiene el público general de los conceptos que aquí se van a exponer.

Los datos han sido recogidos de forma anónima y buscando siempre que llegue a personas fuera del entorno donde se ubica esta asignatura para que la muestra sea lo más diversa posible.

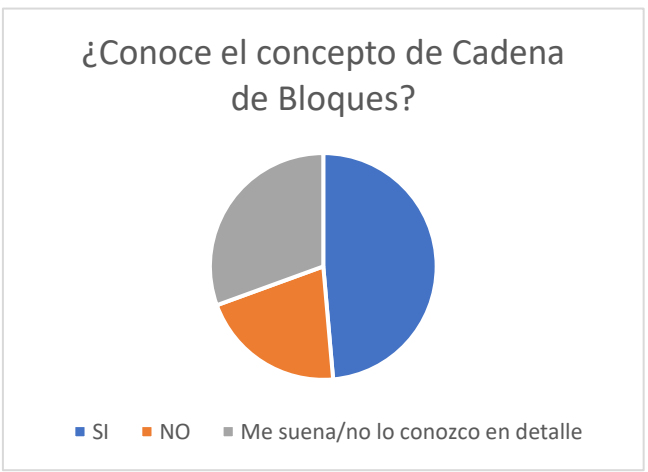
Se ha dividido la encuesta en conocimientos previos, impacto social y medioambiental y futuro de las criptomonedas.

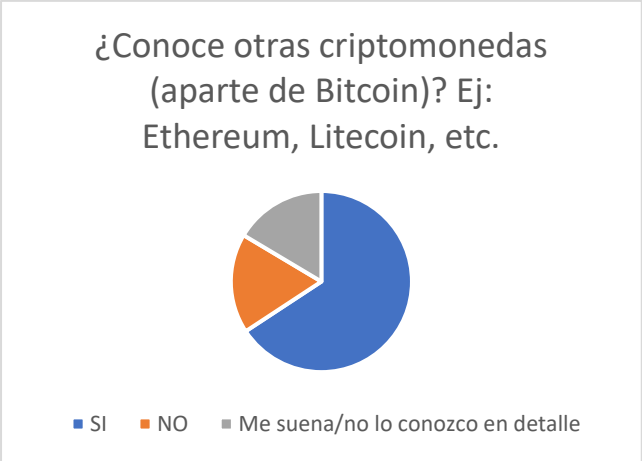
A continuación, se exponen los resultados de dicha encuesta.



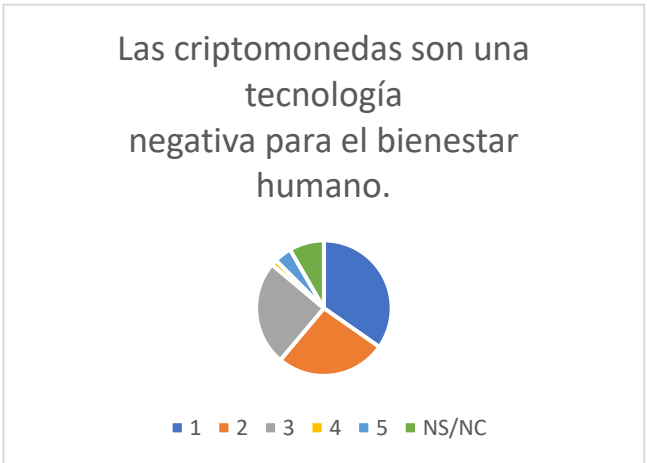


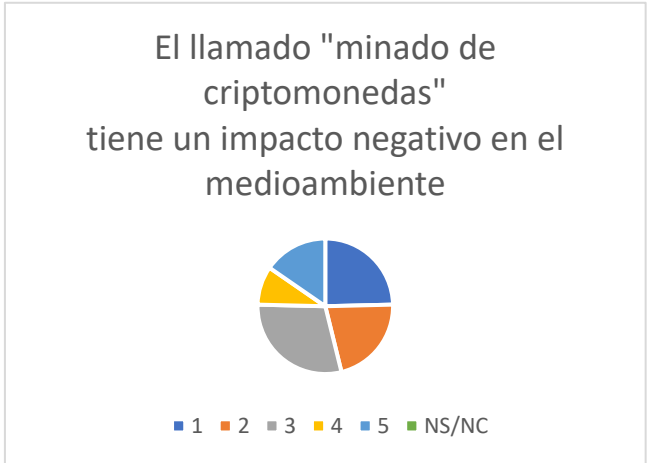
- Conocimientos previos encuestados:

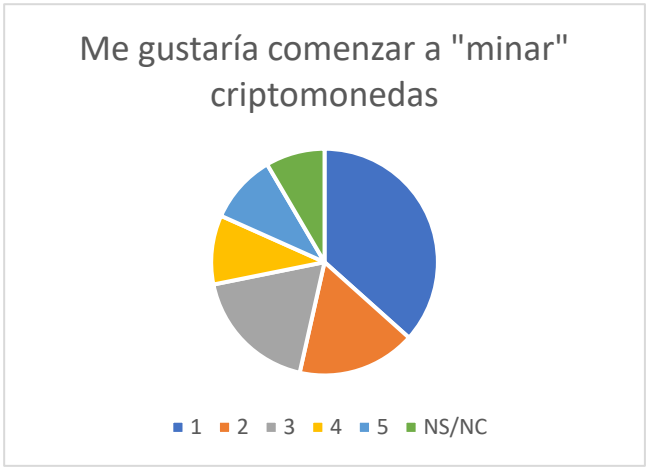


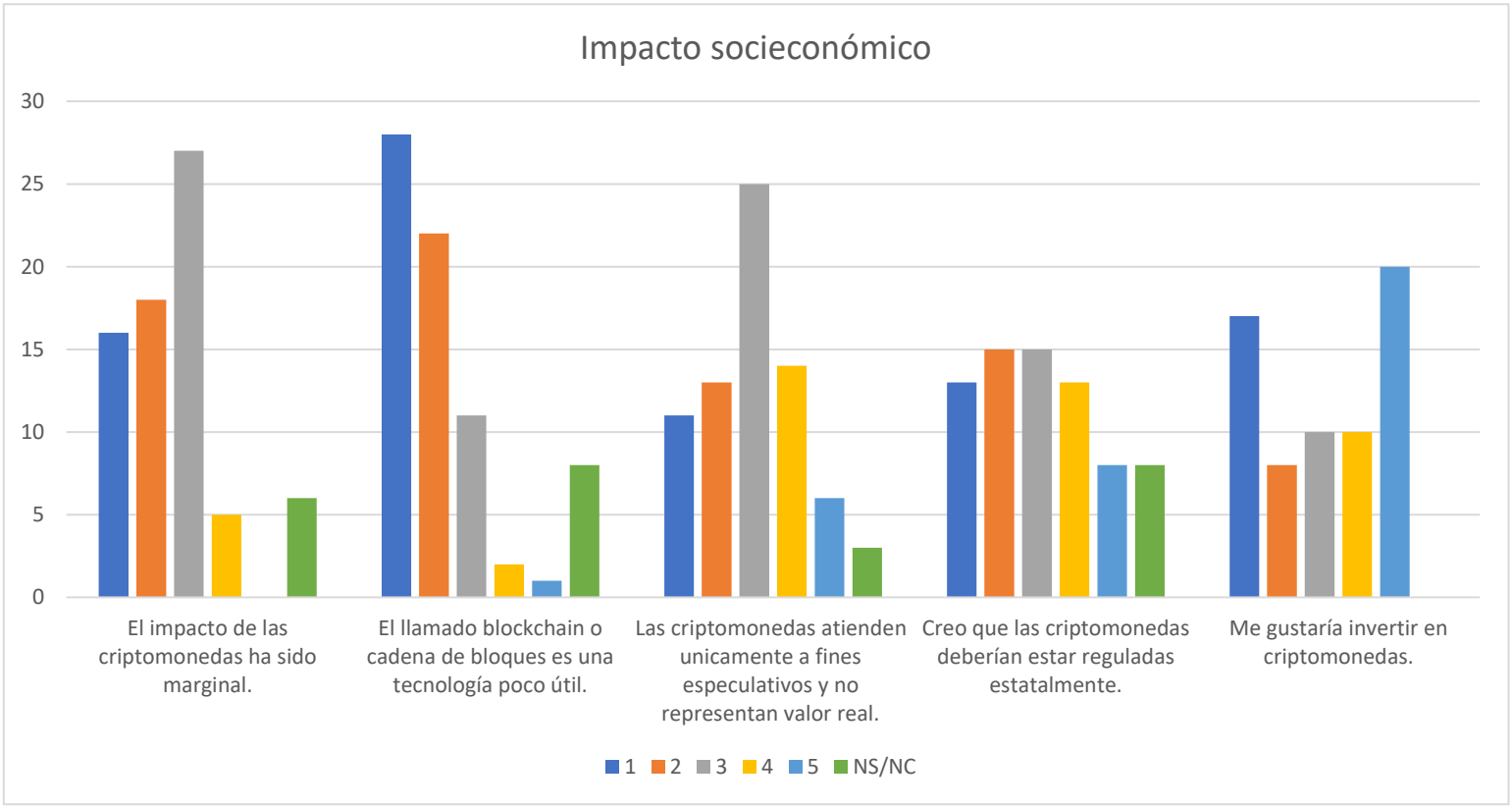


- Impacto socioeconómico y medioambiental encuestado: se recoge la opinión siendo 1 más en desacuerdo y 5 más de acuerdo con las siguientes afirmaciones.

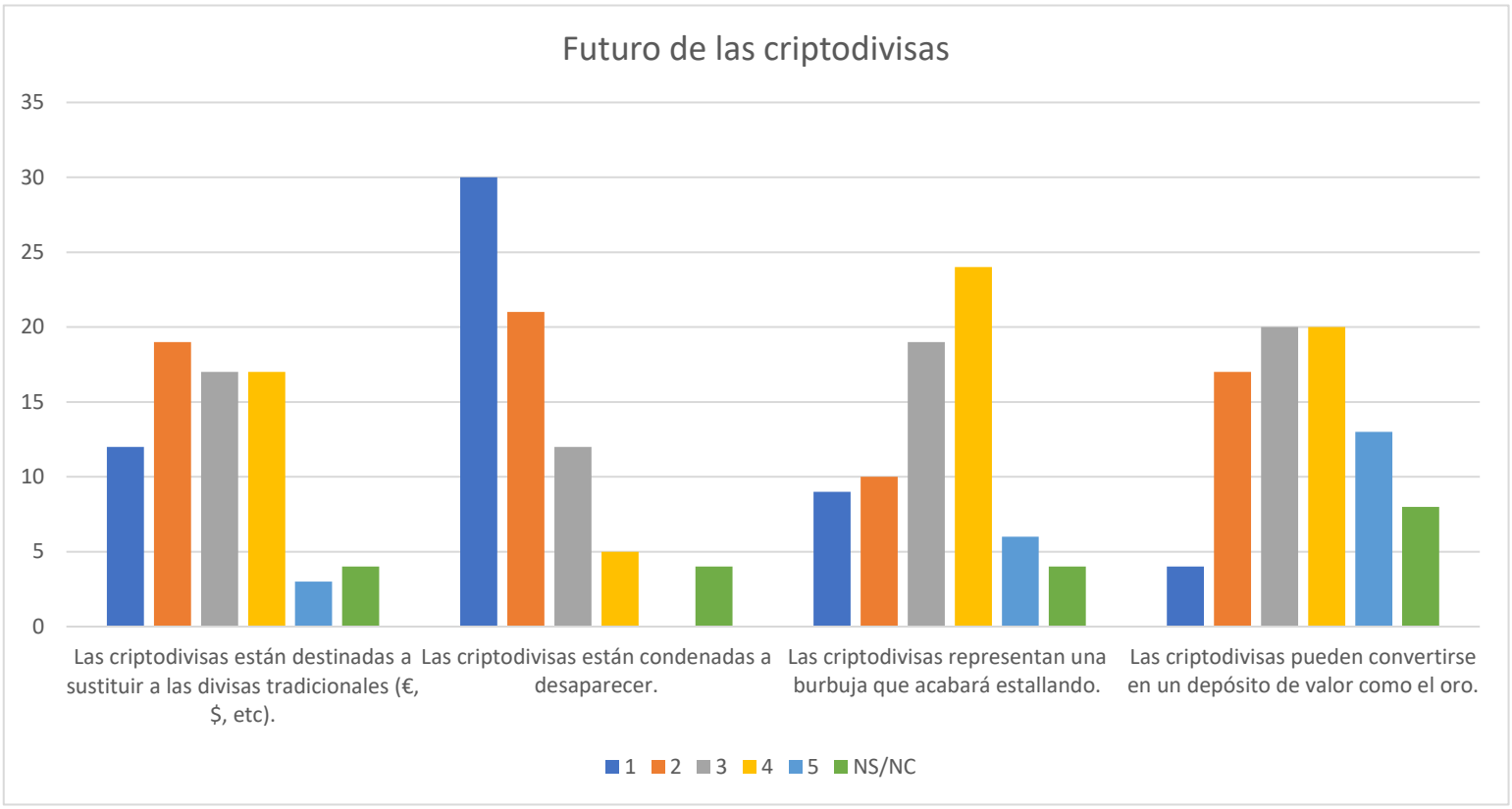





Me gustaría comenzar a "minar" criptomonedas
1
2
3
4
5
NS/NC


Impacto socieconómico
30
25
20
15
10
5
0
El impacto de las criptomonedas ha sido marginal.
El llamado blockchain o cadena de bloques es una tecnología poco útil.
Las criptomonedas atienden unicamente a fines especulativos y no representan valor real.
Creo que las criptomonedas deberían estar reguladas estatalmente.
Me gustaría invertir en criptomonedas.
1
2
3
4
5
NS/NC

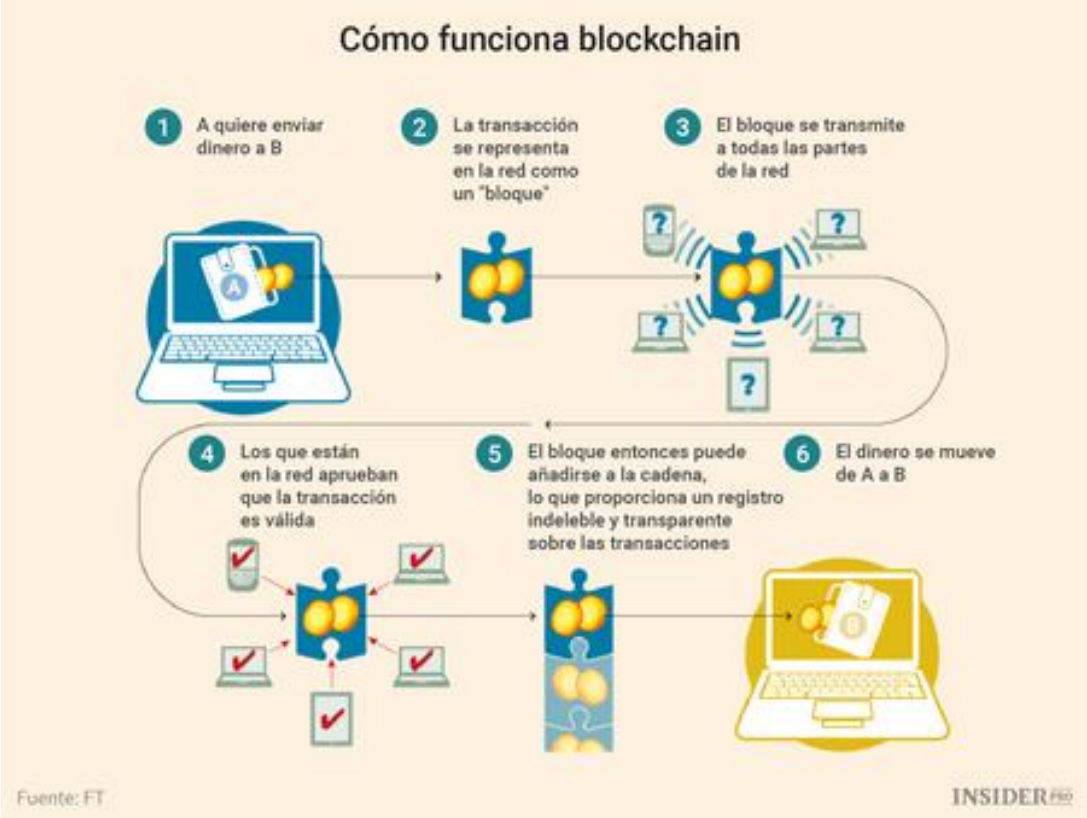
- Futuro de las criptomonedas encuestado: se recoge la opinión siendo 1 más en desacuerdo y 5 más de acuerdo con las siguientes afirmaciones.



Desarrollo del tema: *Blockchain*, la cadena de bloques

Las bases de datos descentralizadas no son un concepto nuevo, las redes P2P cómo las que usan las famosas aplicaciones para compartir archivos (BitTorrent, etc.) son un ejemplo de sistema distribuido. La diferencia radica en su uso.

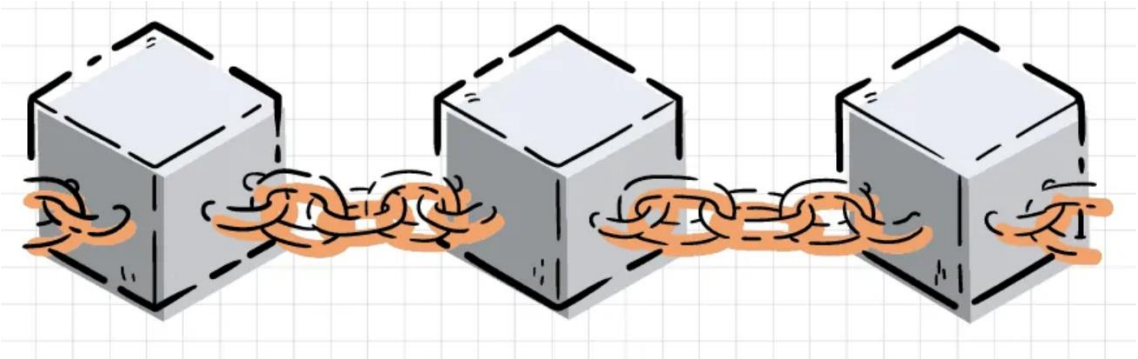
Imaginemos una base de datos centralizada tradicional; cuenta con información organizada en tablas o páginas, compuestas de columnas y filas a la que se va añadiendo información entre otras operaciones. Esta base de datos está siendo controlada por alguien, que puede ser una persona o empresa. Ahora pensemos en una base de datos similar pero que cuyas tablas o páginas ahora llamaremos "bloques", sus usuarios pueden ser cualquier persona del mundo sin necesidad de un registro y aquellas personas que lo mantienen se llamarán "mineros". Tenemos una cadena de bloques.



Cómo en principio estamos hablando de dinero, nos limitaremos por ahora a hablar de transacciones de monedas. De la misma forma que un banco (con su base de datos centralizada) apunta los detalles de las transacciones, una cadena de bloques hace lo mismo con esa información y lo almacena todo en bloques de datos de un tamaño prefijado.

Una vez que un bloque se ha creado (una vez que añadimos información) esta debe ser verificada; cómo no hay una entidad central, deben ser los usuarios (los mineros) quienes verifiquen la nueva información. ¿Qué se consigue con esto? Por un lado hacemos la red inmutable (para alterar la información, un pirata debería competir contra toda la red dado que cada bloque nuevo contiene una "huella" del bloque anterior y así sucesivamente) y, por otro lado, recompensa a los mineros por su trabajo.

Desarrollo del tema: *Blockchain*, ¿cómo funciona?



Para entrar más en detalle sobre la tecnología vamos a desglosar algunas cosas:

- Un bloque contiene tantas transacciones (u otros datos) cómo defina el algoritmo concreto que se está usando.
- Cada bloque de la cadena incluye, además, un "hash" (que antes llamamos huella) que se corresponde a una firma digital (cabecera) que generó el bloque anterior. Este "hash" llamado HASH256 hace que alterar un bloque sea tarea imposible mientras se siga minando ya que cada "hash" verifica el contenido del bloque anterior → modificar un bloque implica tener que modificar TODOS los bloques anteriores.
- Los usuarios, también llamados nodos, son aquellas personas que hacen uso de la red, pero no deben confundirse con los mineros. Los usuarios, que pueden ser personas o empresas, emplean softwares especializados para descargar una copia actualizada de la cadena de bloques y enviar registros nuevos a estos.
- Por último, los mineros, son un tipo concreto de usuario que dispone de recursos informáticos suficientemente potentes para mantener la red. Esto es, verificar las transacciones nuevas, crear nuevos bloques. El trabajo de los mineros viene definido por el tipo de algoritmo que implementa la criptomoneda concreta que están minando. El minado, viene a su vez recompensado por una comisión en forma de monedas o tokens de la propia cadena de bloques.
- Este proceso de verificación se conoce cómo consenso y a continuación explicaremos cómo se desarrolla.

Desarrollo del tema: *Proof of Work* (PoW) vs. *Proof of Stake* (PoS)

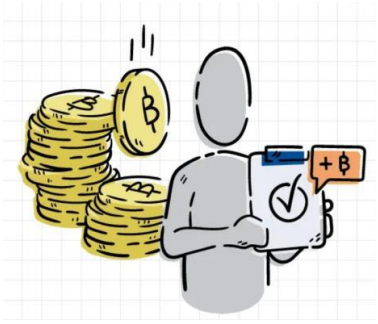
Cómo hemos comentado previamente, el minado de criptomonedas es la forma en que se mantiene una cadena de bloques, pero vamos a darle una vuelta de tuerca a este concepto, principalmente porque (salvando excepciones) tenemos dos posibilidades:

- Minar criptomonedas usando la Prueba de Trabajo.
- ¿Futuro? La prueba de participación.

Minar criptomonedas hace inviable que exista un solo tipo de usuario, esto es, deben existir por un lado los mineros y entonces podrán existir los usuarios finales. Esto se debe a que la prueba de trabajo es un algoritmo intenso que requiere de mucho esfuerzo computacional, lo cual no es viable si se quiere que un usuario participe en esto con un dispositivo móvil.

En detalle, la prueba de trabajo o proof-of-work (PoW) (cuyo ejemplo más simple es el "captcha"), consiste en resolver operaciones matemáticas. Dicho de forma simple, acertar un número. El algoritmo que mantiene la cadena de bloque implementa un sistema que regula la dificultad de estas operaciones matemáticas, esto se conoce como "halving". Los mineros, ponen a disposición de la red su poder de cómputo para calcular ese número, con un incentivo, hacerlo implica una recompensa (en forma de monedas o tokens). Cuanto más poder de cómputo más aumenta el llamado "hash-rate" que es una medida de la capacidad de procesamiento de una blockchain.

VS



Visto esto, ahora llegamos a la alternativa de futuro. La prueba de participación, pero sobre esto hablaremos en detalle en la página X.

Desarrollo del tema: Ethereum: El futuro

Vamos a centrarnos ahora concretamente en las aplicaciones de futuro que plantean estas tecnologías, dejando atrás la simple idea de un dinero digital para dar el salto a conceptos cómo los contratos inteligentes o las aplicaciones distribuidas.

Aunque Ethereum NO es el único proyecto que da pie a estas tecnologías, hemos decidido centrarnos en esta alternativa por ser la que más desarrollo tiene a sus espaldas y nos permite dar una visión más tangible de cómo se están usando de verdad hoy día.

Ethereum aparece unos años después del nacimiento de Bitcoin, concretamente en 2013, de la mano de Vitalik Buterin. El proyecto Ethereum ha ido creciendo con los años, tanto es así que en 2017 nace la Ethereum Alliance formada por empresas de la talla de Google o Microsoft, y en la actualidad es uno de los proyectos con más crecimiento.

La primera versión de Ethereum o ETH v.1 implementa también Prueba de Trabajo (PoW) pero plantea diferencias sustanciales con respecto a su hermano mayor el Bitcoin. Sólo comentaremos que, por ejemplo, la recompensa para los mineros es fija y el tiempo de procesado de los bloques nuevos es de un bloque por 14 segundos. Lo verdaderamente nuevo viene ahora.

Desarrollo del tema: Contratos inteligentes

El concepto de contrato tal y cómo lo conocemos hoy día tiene asociado una serie de intermediarios sobradamente conocidos; abogados, aseguradoras, expertos varios, asesores, etc. De la misma forma que una criptomoneda se plantea cómo una moneda sin intermediarios, los contratos inteligentes hacen lo mismo con los contratos “de toda la vida”.

Para dar un ejemplo que nos sirve para interiorizar este concepto, pensemos por ejemplo en un pago recurrente (cómo una nómina) que queremos establecer por contrato. Mientras que un contrato “tradicional” implica de la ratificación de dicho documento por intermediarios habilitados para tal tarea, un contrato inteligente hace lo siguiente:

Los detalles del contrato se especifican (veremos cómo más adelante) de la misma forma que un contrato escrito, pero eliminando los procesos intermedios. Los detalles del contrato no están abiertos a interpretaciones, cuando los requisitos del contrato se cumplen (desencadenante o "trigger"), se procede a cumplir con los acuerdos (consecuencia), que en nuestro caso es un pago.

Piense el lector en cómo esto puede reducir drásticamente la cantidad de burocracia e intermediarios necesarios para verificar pagos, transacciones, nóminas de empleados públicos, contratos públicos, etc. Pero por si todo esto parece demasiado futurista, ya podemos ver aplicaciones reales de este concepto en la actualidad:

- HTLC (Hash Time Locked Contracts): contratos de tipo temporal para asegurar pagos bidireccionales (asegurar que todas las partes pagan su parte).
- Compra/venta de acciones automatizada cómo consecuencia de un desencadenante.
- Sistemas de apuestas.
- Registro público de propiedad intelectual (patentes registradas en la cadena de bloques y, por tanto, públicamente disponibles a la vez que inmutables).
- Otros.

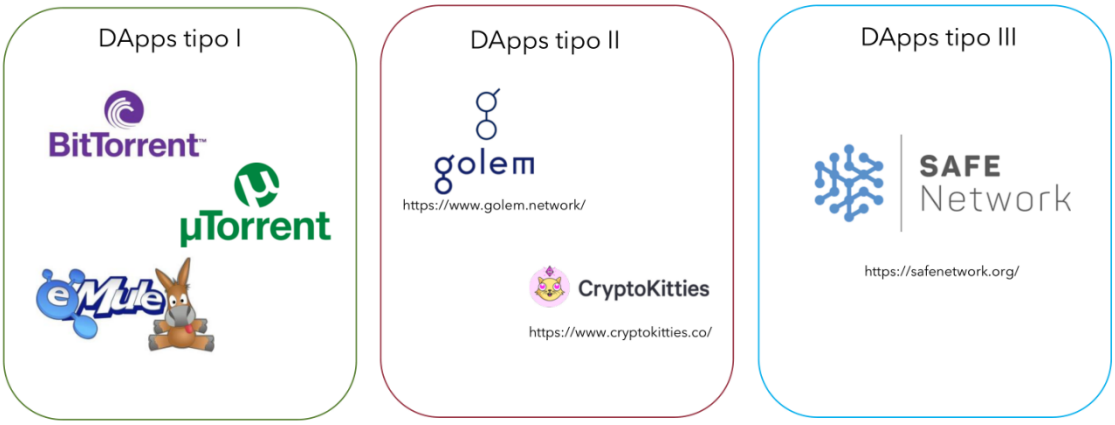
Desarrollo del tema: DApps

Las DApps o aplicaciones descentralizadas no son utilidades nuevas; el lector probablemente sepa de la existencia de servicios P2P cómo Emule, Ares, etc. Sin embargo, estas aplicaciones se enmarcan en el conjunto de las DApps de tipo I, siendo estas, las que disponen de su propia red descentralizada para funcionar.

La novedad surge en las nuevas DApps de tipo II y III, las cuales se caracterizan por funcionar SOBRE una blockchain y no sobre una red propia. Esto es, dichas aplicaciones utilizan la cadena de bloques de una criptomoneda para almacenar la información que

usan. Con carácter general, una DApp de tipo II o III podría ser confundida con un contrato inteligente, pero existen diferencias:

- Los contratos inteligentes precisan de un nº fijo de participantes mientras que las DApps pueden manejar números cambiantes de personas.
- Las DApps no se limitan a usos financieros y/o similares, sino que pueden emplearse para casi cualquier cosa; prueba de ello son los ejemplos que vamos a ver a continuación para arrojar algo más de luz sobre su uso:



Podemos ver aquí unos ejemplos de DApps de tipo I (las "clásicas") y a la derecha, DApps de tipo II y III cómo CryptoKitties (el primer juego del mundo cuyos datos se almacenan en la red de bloques de Ethereum).

Piense el lector ahora en un cambio de paradigma en el cual los datos de las principales aplicaciones que usa no se almacenan en un clásico servidor centralizado sino de forma distribuida en una red de bloques.

Nota: Las DApps de tipo III, con respecto a las de tipo II, sólo cambian en un pequeño detalle: las de tipo III además de funcionar sobre una cadena de bloques (en este caso Ethereum), implementan sistemas de pago haciendo uso de esta misma moneda (el ETH).

Desarrollo del tema: EVM: Ethereum Virtual Machine

Cómo dejamos pendiente antes, aún no hemos explicado cómo se introduce toda esta información en la cadena de bloques. Teniendo en cuenta que ya no hablamos de registros “simples” de transacciones monetarias sino de contratos con condiciones, etc. se hace necesario una vía para introducir todos estos datos en la blockchain.

Dado que nos estamos centrando en Ethereum, vamos a ver de que trata la Ethereum Virtual Machine o EVM. La EVM es una máquina virtual o sistema con conexión directa a la red de Ethereum desarrollada por Greg Colvin y Gavin Woods, que es capaz de introducir instrucciones o códigos de operación (OPERATION_CODES) en la blockchain.

Estos operation codes recuerdan a las pseudo-instrucciones que emplean los procesadores, un nivel antes del lenguaje máquina (binario). Aún así, de la misma forma que un programador de bajo nivel no escribe en instrucciones sino en un lenguaje más formal (como C), un “programador de la blockchain” no escribe en códigos de operación (no digamos ya en binario) sino que lo hace en un lenguaje de mucho más alto nivel: SOLIDITY.

SOLIDITY es un lenguaje formal de alto nivel basado en Python que permite a cualquiera con conocimientos no necesariamente muy avanzados en Python, crear sus propios contratos inteligentes para la cadena de bloques sin necesidad de trabajar en bajo nivel.

```
pragma solidity 0.5.1;

contract MyContract {

    uint256 public peopleCount = 0;
    mapping(uint => Person) public people;

    struct Person {

        uint _id;
        string _firstName;
        string _lastName;

    }

    function addPerson(String memory _firstName, string memory _lastName) public {

        peopleCount += 1;
        people[peopleCount] = Person(peopleCount, _firstName, _lastName);

    }

    ......
}
```

Ejemplo de código escrito en Solidity para definir un contrato inteligente.

Desarrollo del tema: Prueba de Participación

Retomamos lo que aparcamos antes en el apartado de Proof-of-Work vs. Proof-of-Stake. Cómo vimos antes, estos dos algoritmos son la forma en que las cadenas de bloque alcanzan un consenso, es decir, la forma que definen sus algoritmos para crear nuevas monedas o tokens, verificar las transacciones y/o operaciones, crear nuevos bloques, etc.

Vimos que la prueba de trabajo (PoW), si bien es eficaz, no es eficiente. Esto se debe al "halving" y cómo el coste de estas operaciones cada vez es mayor lo que da lugar a todo tipo de problemáticas (contaminación, necesidad de equipos computacionalmente muy potentes y caros, re-descentralización de la red, ataques del tipo "51%", etc.). En respuesta a estos problemas y otros, surge la prueba de participación (PoS).

Este es quizás un protocolo más confuso debido a que su implementación puede ser muy variante, pero por lo general, se basa en incentivar a los usuarios a poseer una determinada cantidad de monedas o tokens. Mientras que en una red PoW el consenso lo establece aquel que consigue averiguar el "número mágico", en una red PoS lo hace aquel con mayor nº de "participaciones". Esto no es sino una explicación a grandes rasgos, pero tenemos que entender que:

- PoS ELIMINA el concepto de minado al no ser necesario realizar cálculos matemáticos complejos se vuelve una alternativa sostenible y permite eliminar la separación entre mineros/usuarios.
- Aumenta la escalabilidad de la red al contrarrestar el efecto del fin de la Ley de Moore. (Si cada vez es más difícil minar, aumentar la capacidad de cómputo nos ayuda a minar mejor, si la capacidad computacional tiende a un límite, ¿que hacemos? PoS responde a esta pregunta eliminando el minado).
- Elimina la posibilidad de controlar la red con una participación mayoritaria. Los conocidos cómo ataques del 51% consisten en controlar el 51% de una red descentralizada (justo 1% más de la mitad) para tener control total sobre ella.
- El sistema de recompensa es más equitativo debido a su carácter aleatorio, lo cual hace al algoritmo más democrático pues, aunque exige ser partícipe de la red, no garantiza que una persona controle esta, sino que se basa en la aleatoriedad. Aquí debemos destacar el extraño carácter de PoS y es que, dependiendo de la implantación del algoritmo, estas propiedades pueden variar.

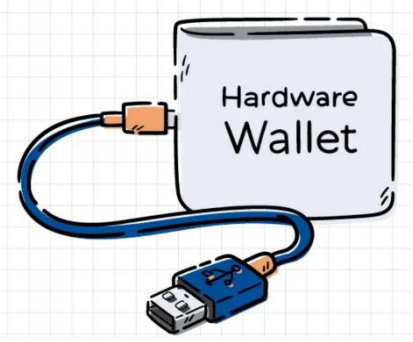
Desarrollo del tema: Miscelánea

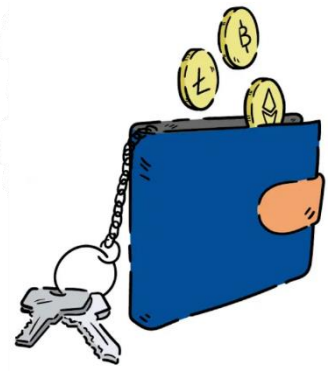
Antes de pasar al final de este trabajo, vamos a ver unos conceptos relevantes para el uso de criptomonedas: monederos, claves públicas/privadas y NFTs.

Llevamos todo el trabajo hablando de usuarios que usan monedas, pero no hemos visto cómo; y haciendo un símil con el dinero "fiat", las criptomonedas cómo no podía ser otra manera, se gestionan por los usuarios finales gracias a monederos (llamados también carteras, wallets o billeteras).

Estas carteras electrónicas son softwares (o incluso hardware) que permiten enviar y recibir monedas a través de una red de bloques haciendo uso, lógicamente, de una conexión a internet. Las carteras en definitiva se encargan de almacenar nuestras claves públicas y privadas (ahora explicamos de que se trata). Sobre las carteras destacaremos las siguientes características:

- Una buena cartera debe ser una pieza de software auditable, esto es, código abierto. Aquellos programas cuyo funcionamiento interno no es consultable suelen merecer poca confianza.
- Igual que existen carteras ejecutables en dispositivos móviles, ordenadores, etc. también existen carteras físicas (también llamadas carteras frías):
    - De hardware: dispositivos electrónicos (con un software público) encargado de gestionar las claves en un entorno seguro (algo así cómo un "pendrive" con software).
    - De papel: las más seguras, pero dependen completamente del usuario.
- No se deben confundir las carteras de criptomonedas con los "exchanges" o bancos tradicionales. Debido al auge de esta tecnología, muchas empresas y bancos tradicionales ofrecen a sus clientes comprar y vender criptoactivos que pueden almacenar en su "banco de toda la vida". Esto no es un ejemplo de cartera dado que la gestión de las claves público/privadas no son competencia del cliente sino de la entidad y en algunos casos, ni siquiera se almacenan criptomonedas sino registros bancarios asociados a su precio actual.





Las claves públicas y privadas son en esencia nuestras monedas, aquello que almacenamos en nuestra cartera. La clave pública, al igual que la privada, es generada mediante criptografía asimétrica, sin esto, no existiría nada de lo que hemos explicado antes. Ambas claves están estrechamente relacionadas, sin una no existiría la otra y viceversa.

La clave pública es generada SIEMPRE en base a la privada y es la primera la que compartimos. Por llevar la explicación a un campo más general, la clave pública sería nuestro IBAN bancario, aquello que comunicamos a los demás. Recalcamos aquí el carácter críptico de esta tecnología: cada usuario no da NUNCA sus detalles (nombre, teléfono, DNI, etc.), en su lugar genera una clave pública (tantas cómo quiera) que comparte con los demás. Si queremos enviar dinero a un usuario, le pediremos su (una) clave pública.

Por otra parte, la clave privada, para compararlo con un caso general, sería cómo nuestra contraseña. Quien controla la clave privada asociada a una clave pública, controla esa cartera. Así pues, para usar una cartera debemos conocer su clave pública y su clave privada.

El carácter seguro de las criptomonedas viene del echo de que averiguar la clave privada a partir de la pública es imposible en el tiempo. Las claves privadas siguen una estructura tal que:

A5373D44C6D87DC0FA6A6738334369F4553213303DA61F20BD67FC233AA37485

Expresada en formato hexadecimal (base 16), dado que se generan con 256 bits, el rango de combinaciones es de 2^256 combinaciones. Es fácil ver cómo calcular el número asociado a una clave pública es computacionalmente imposible de resolver en tiempo humano.

Por último, antes de cerrar el trabajo, vamos a ver una última novedad derivada de estas tecnologías: El Criptoarte o arte digital.

Los llamados NFTs o “Non-fungible tokens” son tokens (que NO monedas, dado que no son particionables) que se sustentan en la red de bloques de Ethereum y que posee características que lo hacen único.

Hablando en términos quizás menos liosos: los NFTs permiten registrar arte (sea este del tipo que sea) en la cadena de bloques, de forma parecida a cómo vimos que hacían los contratos inteligentes para registrar propiedad intelectual, pero con la diferencia de que aquí, dicha pieza de arte constituye un “ente digital”.

Esto que estamos viendo, en si mismo, es un NFT. A menudo se confunde el concepto, pero los NFTs no registran la obra de arte en sí, prueba de ello es que esta imagen aquí presente podemos copiarla tantas veces cómo queramos, cuando y cómo queramos.

¿Entonces que es? Los NFTs constituyen una prueba de la propiedad, de la misma forma que un cuadro famoso tiene miles de copias hechas por otros artistas, fotos en internet, etc. pero sólo existe una copia original, los NFTs no impiden que se haga una copia del arte, pero permiten certificar al poseedor cómo dueño de esa obra. Dado que la cadena de bloques es pública, todo el mundo puede ver que somos el dueño del NFT.

Aquí hay que destacar varios aspectos importantes para no confundirnos:

- Cualquier cosa puede ser representada cómo un NFT dado que este lo que certifica es la propiedad de este, no el "ente". (Piense el lector en dominios de páginas web, por ejemplo).
- Aunque los NFTs funcionan sobre la red de Ethereum en la actualidad son escalables a casi cualquier red de bloques.
- Es una tecnología muy sencilla de implementar.
- Dado que los NFTs constituyen en si un contrato inteligente, comprar una obra digital en formato de NFT garantiza que el dinero pagado vaya directamente al creador de la obra sin intermediarios.

Discusión

No todo son luces en este camino de innovación, sino que también existen sombras. Problemas que, si bien no todos son nuevos, algunos se han incrementado cómo consecuencia de estas tecnologías.

Entre todos los problemas actuales y de futuro cabe destacar varios más inmediatos, pero a la par que los mencionamos, también vamos a ver posibles soluciones; a saber:

- Contaminación → hemos visto que PoW supone un coste computacional y energético enormemente elevado, pero, aunque esta perspectiva es negativa, hemos visto cómo PoS puede cambiar esto por completo (un proyecto al respecto sería Ethereum 2.0).
- La falta de legislación / reconocimiento → una de las problemáticas más recurrentes y actuales, dado que, sin el reconocimiento legal de las entidades

legislativas vigentes, estas tecnologías sufren problemas ante las arbitrariedades políticas.

- Falta de formación → aunque el concepto de criptomonedas forma parte del imaginario común (cosa que podemos contrastar con las encuestas realizadas), sus detalles más específicos escapan al entendimiento del gran público lo que da lugar a problemas derivados cómo son las diversas estafas en nombre de promesas de mercado, ofertas iniciales de monedas falsas, etc. Si bien es cierto lo anterior, tenemos la suerte de contar con cada vez más fuentes de formación al respecto y mayor cobertura mediática.

Conclusiones y recomendaciones

Para cerrar el trabajo, me gustaría destacar el creciente potencial de estas tecnologías que frecuentemente son reducidas a la mera especulación de activos por parte de medios de comunicación. Sin embargo, cómo hemos podido ver estas tecnologías plantean sistemas mucho más complejos y enrevesados, capaces de modelar sociedades futuras. Aunque esto parezca a priori descabellado, piense el lector en cómo la burocracia podría ser reducida a algoritmos públicos encargados de pagar nóminas, ejecutar contratos, mantener cuentas públicas a la vista de todos, etc. Las posibilidades bien merecen la pena.

Agradecimientos

Agradecer antes de nada a todas las personas que se tomaron unos pocos minutos de su valioso tiempo para responder a la encuesta planteada que da lugar a este trabajo, así como a los compañeros y compañeras que siguieron la presentación de este trabajo en directo.

Bibliografía, referencia y anexos

Algunas fuentes y libros consultados:

- "Todo lo que querías saber sobre bitcoin, criptomonedas y blockchain: y no te atrevías a preguntar" por Carlos Domingo, disponible en fama.us.es
- "How to Make a Mint – The Cryptography of Anonymous Electronic Cash" por Laurie Law, Susan Sabett y Jerry Solinas, disponible en archive.org
- "Proof of Work VS Proof of Stake: Which one is better?" de Laura M., disponible en bitdegree.org
- "Documentación de Solidity" disponible en solidity-es.readthedocs.io
- "Artículos de Bit2Me Academy" disponibles en academy.bit2me.com
- "3 en 1: Blockchain, la revolución descentralizada, Ethereum, un mundo de posibilidades y La fiscalidad de las criptomonedas" de publicación independiente.

Algunos sitios relevantes que merece la pena consultar:

- Web de Ethereum (https://ethereum.org/en/).
- Web especializada analizar el estado de la minería en la actualidad (https://whattomine.com/).
- Web en la que poder consultar transacciones reales de una cadena de bloques en tiempo real (https://www.blockchain.com/btc/unconfirmed-transactions).