**Criptomonedas: Impacto Social y Futuro**

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

Asignatura: Tecnología, Informática y Sociedad – TIS

Fecha: Curso 20/21 – Marzo/Abril 2021

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

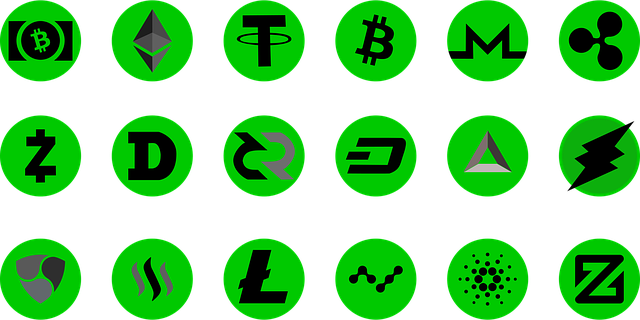
Resumen: El presente trabajo abarca el concepto de criptomonedas o divisas electrónicas; los principios de su funcionamiento (cadena de bloques y técnicas de actualización de la *blockchain*) y el impacto que han tenido en la sociedad y como definirán el futuro próximo.

Índice:

* Introducción al tema …………………………………………………………………………. 3
* Conocimientos previos ……………………………………………………………………… 4
* Terminología, conceptos y definiciones ……………………………………………. 5
* Encuestas (percepción pública) …………………………………………………………. 5
* Desarrollo del tema
  + Cadena de bloques ………………………………………………………………… 10
  + Proof of Work (PoW) vs. Proof of Stake (PoS) ………………………… X
  + Coste de la cadena de bloques ……………………………………………….. X
  + Uso de la tecnología ……………………………………………………………….. X
  + Alternativas ……………………………………………………………………………. X
* Discusión …………………………………………………………………………………………… X
* Conclusiones y recomendaciones ……………………………………………………… X
* Agradecimientos ………………………………………………………………………………. X
* Bibliografía, referencia y anexos ………………………………………………………. X

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

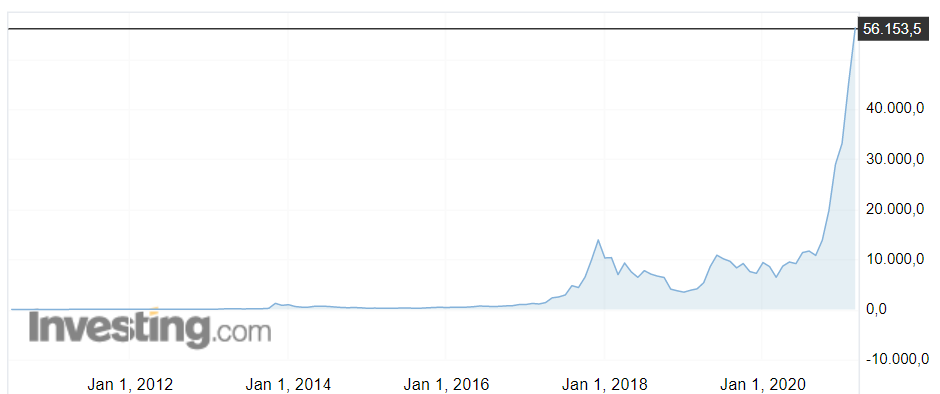
Las criptomonedas tienen su origen en el nacimiento del *Bitcoin* en 2009 pero sus fundamentos se remontan a mucho antes; dado que la base que soporta la existencia de las criptodivisas, la llamada cadena de bloques (*blockchain*), se basa en principios criptográficos de clave pública, anteriores al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

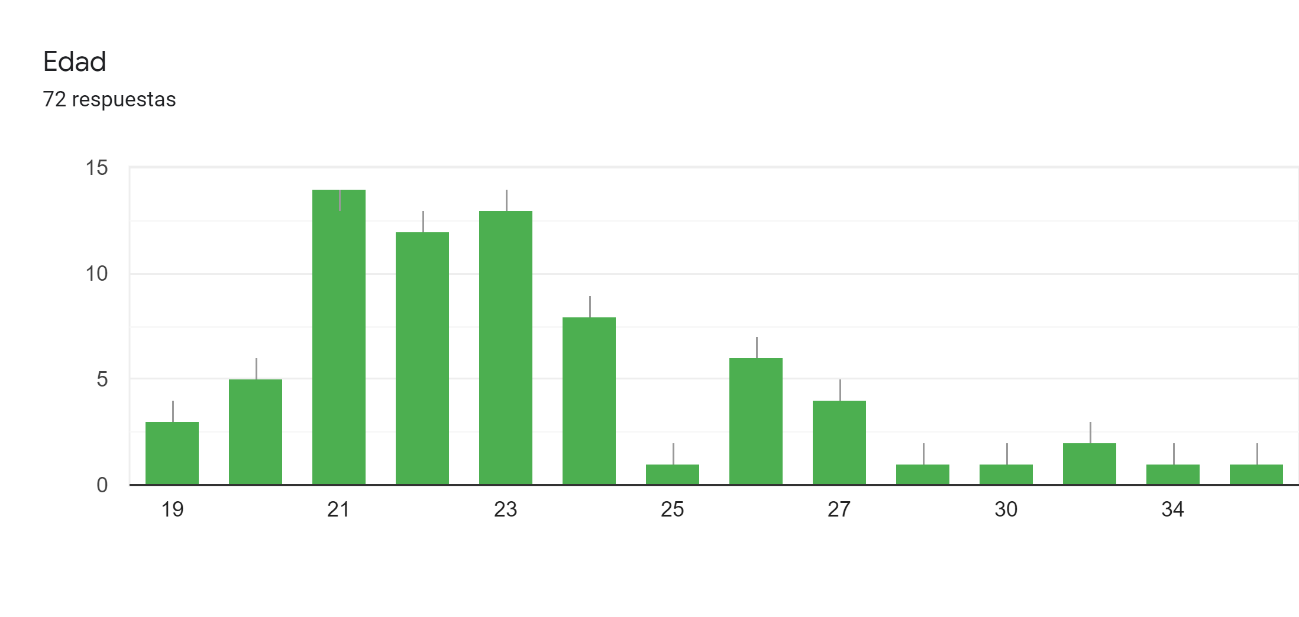
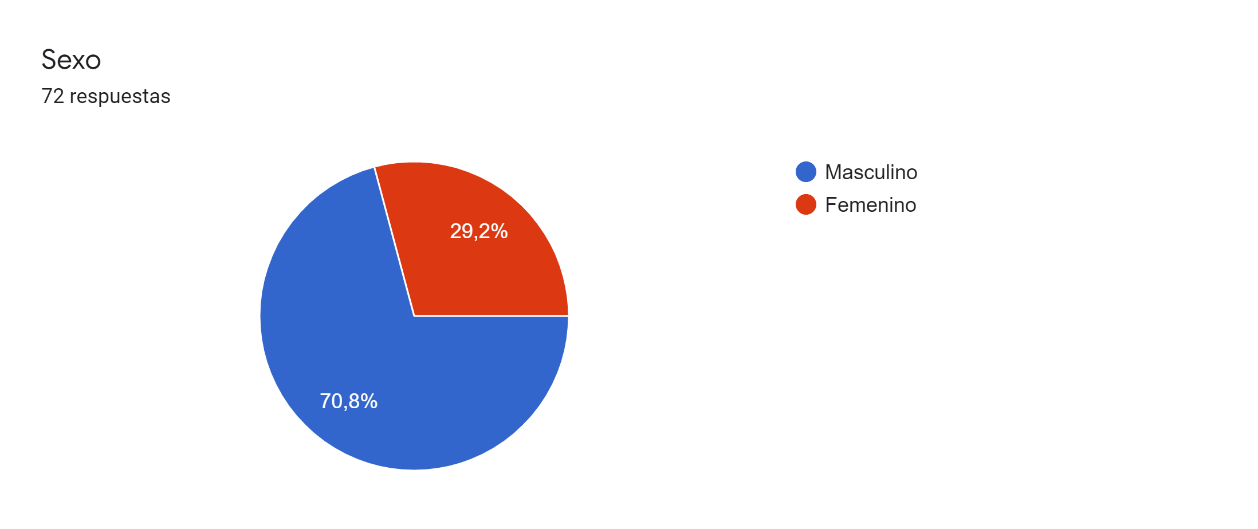
Encuestas (percepción pública)

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.
* 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

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

Desarrollo del tema: Coste de la cadena de bloques

Desarrollo del tema: Uso de la tecnología

Desarrollo del tema: Alternativas

Discusión

Conclusiones y recomendaciones

Agradecimientos

Bibliografía, referencia y anexos