GRADO EN COMERCIO

TRABAJO FIN DE GRADO

“BLOCKCHAIN Y CRIPTOMONEDAS”

INÉS VILLAMERIEL MARTÍNEZ

FACULTAD DE COMERCIO

VALLADOLID, JUNIO 2019

GRADO EN COMERCIO

CURSO ACADÉMICO 2018/19

TRABAJO FIN DE GRADO

“BLOCKCHAIN Y CRIPTOMONEDAS”

Trabajo presentado por: INÉS VILLAMERIEL MARTÍNEZ

Firma: VILLAMERIEL MARTINEZ INES - 12424183C Firmado digitalmente por VILLAMERIEL MARTINEZ INES - 12424183C Fecha: 2019.06.23 22:58:28 +02'00'

Tutor: FRANCISCO JAVIER GALÁN SIMÓN

Firma:

FACULTAD DE COMERCIO

Valladolid, 25 de junio de 2019

Índice

1 INTRODUCCIÓN 1

1.1 Justificación del trabajo 1

1.2 Objetivos 1

1.3 Resumen 1

1.4 Agradecimientos 2

2 Blockchain 3

2.1 Historia Blockchain 3

2.2 Definición 4

2.3 Características 4

2.3.1 Segura 4

2.3.2 Descentralizada y P2P 5

2.3.3 Transparente 6

2.4 Clasificación 6

2.4.1 Pública 7

2.4.2 Privada 7

2.4.3 Federada 7

2.5 Funcionamiento 7

2.6 Aplicaciones 13

2.6.1 Criptomonedas 14

2.6.2 Contratos inteligentes 14

2.6.3 Logística y cadena de producción 15

2.6.4 Administración 16

2.6.5 Gobierno 17

2.6.6 Inclusión económica 17

2.6.7 Servicios médicos 18

2.6.8 Propiedad intelectual 18

2.7 Especial mención: Ethereum 18

2.8 Blockchain en Valladolid 25

3 Criptomonedas 26

3.1 Bitcoin 26

3.1.1 Definición 27

3.1.2 Carteras Bitcoin 28

3.1.3 Características 29

3.1.4 Funcionamiento 30

3.2 Ether (ETH) 31

3.2.1 Definición 32

3.2.2 Monederos Ethereum 32

3.2.3 Características y Diferencias con BTC 34

3.2.4 Funcionamiento 35

3.3 Otras criptomonedas 36

3.3.1 Monero 36

3.3.2 Dash 36

3.3.3 Ripple 36

3.3.4 Litecoin 36

3.4 Creando mi criptomoneda 37

4 Conclusiones 45

5 Bibliografía 46

6 Anexos 49

Anexo I. Glosario de términos 49

Anexo II. Lenguaje Solidity (EIP20.sol) para el Smart Contract de la criptomoneda 51

Anexo III. Lenguaje Solidity (EIP20interface.sol) para la función del Smart Contract 54

Anexo IV. Apariencia página Remix de Ethereum 57

Anexo V. Apariencia Etherscan 58

Listado de imágenes

Imagen 1. De las redes centralizadas a las distribuidas 6
Imagen 2. Blockchain y contratos inteligentes 8
Imagen 3. Blockchain y contratos inteligentes 14
Imagen 4. Trazabilidad de productos farmacéuticos 16
Imagen 5. Valor de Bitcoin 27
Imagen 6. Blockchain y contratos inteligentes 31
Imagen 7. Evolución valor Ether 32
Imagen 8. Aspecto de una cartera Metamask 38
Imagen 9. Lenguaje Solidity en Smart Contract de Ethereum 40
Imagen 10. Seguimiento de criptomonedas en Ethereum 43
Imagen 11. Pasos creación criptomoneda 44
Imagen 12. Árbol de Merkle 49
Imagen 13. EIP.sol 51
Imagen 14. EIP20interface.sol 54
Imagen 15. Remix 57
Imagen 16. Etherscan 58

1 INTRODUCCIÓN

1.1 Justificación del trabajo

El presente TFG se propone desarrollar de manera clara la tecnología de la cadena de bloques y lo que supone esta revolucionaria tecnología. Es decir, comprender su concepto, cómo funciona y la importante cantidad de aplicaciones que puede tener. Además, con la creación de una criptomoneda realizada por mí, hacer entender que por complejo que parezca este tema, demostrar que es posible, seguro e interesante, además de ayudarme a entender más allá del marco teórico.

En mi opinión, Blockchain representa el futuro, una nueva forma de pensar y actuar que aún mucha gente desconoce. Por ello, la principal justificación de la realización de este trabajo es querer contribuir a que las personas que aún desconocen este concepto lleguen a entenderlo e incluso, quieran formar parte de ello.

Todo ello sin contar que a nivel personal ha sido un descubrimiento impactante, que estoy segura de que me va a servir, no solamente como una ampliación de conocimientos de una tecnología innovadora, sino también a nivel práctico y, posiblemente, desde un punto de vista profesional.

1.2 Objetivos

El objetivo principal de este trabajo de fin de grado es estudiar y describir la cadena de bloques, para poder ponerlo en práctica en este caso respecto a la creación de una criptomoneda, y con ello hacer ver cómo funciona, no solo teóricamente.

Este objetivo se concreta en los siguientes:

- Identificar y describir la cadena de bloques, sus características y funcionamiento.

- Conocer algunas de las posibles aplicaciones que Blockchain puede ofrecer.

- Crear una criptomoneda propia, definiendo y explicando cada paso.

1.3 Resumen

El siguiente Trabajo de Fin de Grado trata de definir y explicar la tecnología Blockchain, centrándose en las criptomonedas. Tanto es así que como aportación única e innovadora yo, Inés Villameriel, he creado mi propia moneda.

Blockchain es una tecnología revolucionaria que mucha gente al igual que yo, consideramos como el futuro. Esto se debe a que es una tecnología segura, transparente, descentralizada y distribuida.

Su funcionamiento, que es llevado a cabo por los propios usuarios, es complejo pues se necesita resolver una incógnita a través del método prueba error. Pero la validación posterior y la ausencia de la confianza en terceras partes, como instituciones o gobiernos, hacen que sea una tecnología mejorada.

Las criptomonedas es posiblemente el uso más conocido de Blockchain por el momento. Dentro de estas, Bitcoin y Ethereum son las que encabezan la lista, aunque también hay otras muchas como Monero, Ripple, Dash, Litecoin...

Ethereum además, pertenece a Blockchain programable, es decir, su aplicación no solo se basa en criptomonedas sino que también en el Blockchain para aplicaciones.

Pues bien, la cadena de bloques tiene más aplicaciones posibles a parte de las criptomonedas. Esta tecnología revolucionaria se puede aplicar a la logística, el gobierno, a contratos y en más situaciones estudiadas en este trabajo.

Por último, con IVMtoken (el nombre de mi criptomoneda) muestro cómo es posible empezar a entender e integrarse en el mundo del Blockchain.

1.4 Agradecimientos

La realización de este trabajo tan laborioso, interesante y a la vez desafiante, te hace pensar en las causas que te han empujado a llevarlo a cabo. Por esta razón creo conveniente dedicar este apartado a las personas que me han ayudado y apoyado en este proceso.

A mis queridos padres, César e Irene, por su incondicional apoyo y paciencia en mis momentos de mayor desesperación, así como también, gracias por darme la oportunidad de estudiar este grado sin el cual no estaría en este punto. A mis hermanas, Clara y Henar por sus ánimos, consejos y por recordarme de lo que soy capaz. A mis amigas/os por escuchar mis quejas y hacer que me sienta mejor para poder continuar.

También, agradecer a mi tutor, Javier Galán por su paciencia, sus consejos y también su rápida respuesta a mis correos ya que no es fácil realizar las tutorías a distancia, por lo que mi agradecimiento y satisfacción es aún mayor. De nuevo, muchas gracias por su siempre disponibilidad y compromiso.

Por último, Dedico con todo mi cariño este Trabajo de Fin de Grado a mi abuela Emilia Galván.

2 BLOCKCHAIN

Para poder explicar bien qué es el Blockchain primero hay que remontarse a sus inicios para entender el motivo por el que se creó. Por ello, antes de definirlo, veamos su historia.

2.1 Historia Blockchain

Quién habría pensado que sería posible cambiar la forma en la que compramos, pagamos y hasta votamos, incluso sabiendo que en las últimas décadas ha habido una auténtica revolución en estos campos.

En efecto, de un tiempo a esta parte se ha extendido la utilización de tecnología de certificación para autentificar la realización de cualquier tipo de acción, desde transferencias bancarias, hasta presentación de declaraciones fiscales, recepción de notificaciones, etc. Sin embargo, estos sistemas no eran suficientemente aplicables para otro tipo de acciones, con una masiva cantidad de información y la necesidad de verificación de todas y cada una de las transacciones.

Pues bien, ya en 1991 Stuart Haber y W. Scott Stornetta introdujeron un sistema de cadena de bloques asegurado criptográficamente para almacenar documentos digitales con fecha y hora. De esta forma, no podían ser modificados ni alterados. En 1992 incorporaron árboles Merkle, lo que hizo posible que varios documentos se juntasen en un solo bloque. Sin embargo, esta tecnología no se utilizó y la patente caducó en 2004.

En 2004, el criptógrafo Hal Finney creó un sistema llamado RPoW, (*Reusable Proof of Work*). El sistema resolvió el problema del doble gasto manteniendo la propiedad de los bloques registrados en un servidor de confianza, el cual permitía ser verificado por los propios usuarios.

En 2008, una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto presentaba un sistema de dinero electrónico descentralizado de igual a igual, denominado Bitcoin.

Bitcoin está basado en la prueba de trabajo (PoW), pero en lugar de utilizar una función de confianza como el RPoW, utiliza un protocolo *peer-to-peer* descentralizado, evitando así la función de la confianza.

El 3 de enero de 2009, esta criptomoneda nació cuando el primer bloque de Bitcoin fue extraído por Satoshi Nakamoto, obteniendo una recompensa de 50 Bitcoins.

El primer destinatario fue Hal Finney, quien recibió 10 Bitcoins en la primera transacción de Bitcoin del mundo.

Pero esto es solo el principio. Actualmente en Blockchain 2.0 hay instrumentos financieros que nos permiten autenticar activos y propiedades.

Además, en Blockchain 3.0 tenemos el internet de las cosas, en el que podemos registrar nuestros dispositivos, asignarles una identidad y coordinar pagos entre ellos.

"En la primera era de internet nada de esto era posible. Ahora tenemos una plataforma en la que la gente y aun las cosas disponen de verdaderos incentivos financieros para colaborar eficazmente y crear casi cualquier cosa." (*Blockchain Revolution,* Alex y Don Tapscott)

2.2 Definición

De acuerdo con su creador, Satoshi Nakamoto (2008) "Blockchain es la red que sella transacciones en el tiempo en una cadena continua de *proof-of-work* basada en *hash*, estableciendo un registro que no se puede modificar sin rehacer la *proof-of-work*".

En otras palabras, Blockchain es una tecnología que permite que transacciones y sistemas de información se ejecuten de manera segura. Para ello, los registros o bloques están enlazados y cifrados. Además, varios usuarios han de verificar esas transacciones. Una vez corroboradas, esa información no puede ser eliminada ni modificada.

En resumen, Blockchain contiene un registro seguro y verificable de cada una de las transacciones realizadas por los distintos usuarios. Aunque esas transacciones muchas veces se asocian con criptomonedas, Blockchain puede llevar a cabo muchos tipos de transacciones, las cuales veremos más adelante.

2.3 Características

Ahora que el concepto ya está explicado, ¿qué es lo que la hace tan especial? ¿Por qué es una tecnología revolucionaria?

2.3.1 Segura

Blockchain sin lugar a dudas aporta seguridad y esto se debe a su funcionamiento.

Cada bloque perteneciente a esta cadena no puede ser corrompido, puesto que, para lograr la alteración de cualquier dato, se deberían modificar los *hashes* de los anteriores bloques y así continuamente hasta lograr modificar el bloque génesis.

Es decir, si alguien quiere corromper la red, deberá modificar todos los datos almacenados en cada nodo de la red.

En resumen, la información está cifrada en cada etapa del proceso, además, está distribuida, por lo que no depende de ningún miembro individualmente. Los derechos de decisión y los incentivos hacen que comportarse fraudulentamente sea imposible o cueste tanto tiempo, energía y dinero que no merezca la pena.

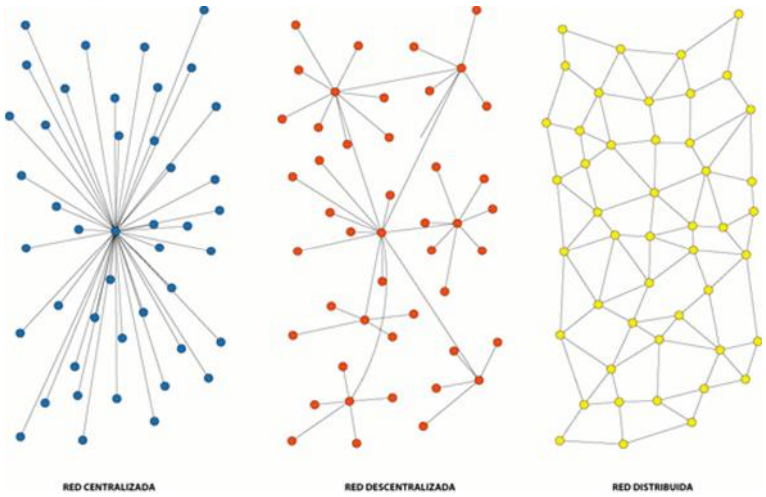
2.3.2 Descentralizada y P2P

Su creador, Satoshi Nakamoto decidió quedarse en el anonimato por lo que no tiene dueño o autoridad que lo gobierne. Es decir, Blockchain funciona gracias a los usuarios que participan en ella.

Peer to Peer hace referencia a la interacción entre los distintos participantes (nodos), se realiza sin clientes o servidores. Es decir, actúan conjuntamente como consumidores y servidores respecto a los demás nodos de la red, sin necesidad de terceros. Las redes P2P admiten el cambio directo de información, de cualquier formato, entre los ordenadores conectados a la red.

Blockchain incentiva a participar y además nos da derecho a ser “propietarios” de la plataforma. Teniendo y utilizando criptomonedas fomentamos el desarrollo de la cadena de bloques.

Imagen 1. De las redes centralizadas a las distribuidas



Fuente: (Gutiérrez, 2012)

En resumen, Blockchain no es solo una red descentralizada, sino que también es distribuida.

2.3.3 Transparente

Esta característica puede variar según el tipo de red. En el caso de las redes públicas, que explicaré con detenimiento más adelante, la transparencia es total. La razón es porque sea el usuario que sea el que se registre en la cadena tendrá una copia de toda la red Blockchain, pudiendo comprobar el estado y el historial de las transacciones. En las redes privadas el acceso es limitado y los administradores son los que aportan la transparencia.

Esta característica es más fácil de conseguir gracias a que, a diferencia de los métodos tradicionales, Blockchain asegura la integridad de las transacciones a través de códigos inteligentes y no porque las personas decidan comportarse correctamente, es decir, la cadena de bloques evita la corrupción o simplemente errores.

2.4 Clasificación

Como bien acabamos de ver en el apartado anterior, según el tipo de Blockchain que sea las características pueden variar. Entonces, veamos cómo se clasifica Blockchain dependiendo de sus características.

2.4.1 Pública

Las redes Blockchain públicas, como Bitcoin, son aquellas a las que cualquier persona tiene acceso. Así pues, es posible unirse a esta cadena de bloques y obtener la historia completa de la cadena y hacer uso de la misma. En definitiva, está abierto a quien lo desee.

La gran ventaja es la total descentralización: Blockchain es pública, inmutable y no existe ninguna entidad que pueda manipularla. Además, al ser un sistema distribuido es más resistente a ataques ya que no existe un único objetivo central. Cuantos más nodos participan en la cadena de bloques, más difícil es atacarla porque cada nodo posee una copia.

2.4.2 Privada

El acceso directo a los datos de la cadena de bloques y a las transacciones se limita a una lista predefinida de participantes. Además, han de ser autorizados y no todos los participantes disponen de los mismos permisos.

Las cadenas de bloques privadas sí están controladas por una entidad. En este tipo, se suele dar la circunstancia de que no se requiera la prueba de trabajo. Por este hecho muchos no las consideran como cadenas de bloques reales.

2.4.3 Federada

La cadena de bloques federada es muy parecida a una cadena de bloques privada, ya que no permiten la participación a cualquier usuario. Estas cadenas son más rápidas y proporcionan más privacidad en las transacciones.

Normalmente se asocian a bancos, gobiernos o asociaciones que realizan muchas transacciones.

Además, los mineros no reciben una recompensa, ya que no tienen criptomonedas asociadas a la cadena de bloques.

2.5 Funcionamiento

Blockchain es, como ya se ha indicado, una base de datos donde se “escriben” las transacciones de los usuarios, organizada en una cadena de bloques enlazados secuencialmente por unas huellas o claves llamadas *hash*. Esa base de datos no se

encuentra en un único ordenador, ni en un único lugar del planeta. Se trata de una red de ordenadores interconectada, la cual va a funcionar simultáneamente como si fuera un único superordenador.

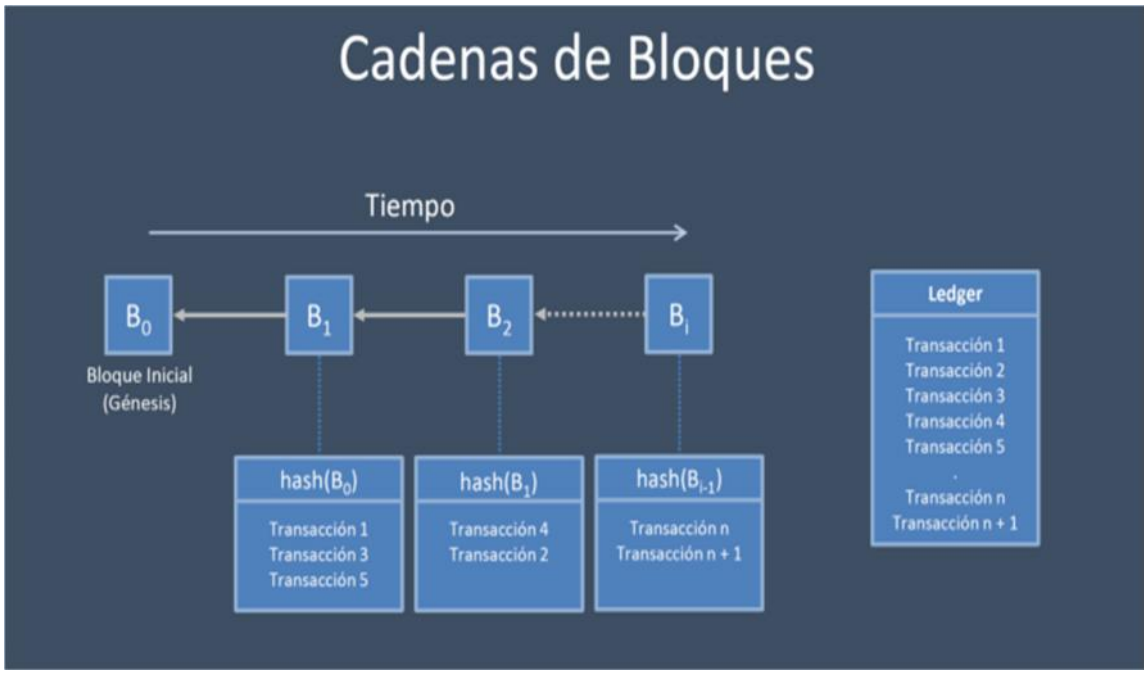
Vamos a ver cómo funciona la tecnología Blockchain teniendo en cuenta los objetivos primordiales que pretende:

- Universalidad
- Ausencia de censura
- Seguridad en las transacciones
- Anonimato

El funcionamiento secuencial sería el siguiente:

Previamente es preciso tener descargado el software necesario para conectarse a la cadena, si bien, también es posible acceder a webs especializadas que permitan el acceso a la red de nodos, siendo la primera opción la más habitual.

Imagen 2. Blockchain y contratos inteligentes



Fuente: (Cervera, 2018)

Cuando se pretende realizar una transacción, entendiendo por ello no solamente la monetaria (criptomonedas), sino cualquier tipo de información susceptible de ser

almacenada o incluida en un “paquete” o bloque (ver aplicaciones de Blockchain en el siguiente apartado del trabajo), la envía a los nodos con los que se encuentra conectado para que lo incluyan en un bloque, previa verificación.

El proceso de verificación se realiza inicialmente por la red Blockchain, que exige toda la información precisa para comprobar que todo es correcto.

Una vez recibida la transacción en los nodos conectados, y efectuada la validación, estos remiten instantáneamente dicha transacción a los nodos que a su vez se encuentran conectados, replicándolos, y así sucesivamente, de tal forma que todos los nodos añaden a su lista de transacciones la que nos ocupa. De esta forma cada nodo va incluyendo en su lista (denominada *pool*) todas las transacciones que va recibiendo.

Después de un lapso de tiempo, que puede variar desde unos segundos hasta varios minutos, el sistema global de nodos selecciona uno de ellos aleatoriamente para proponer un bloque, utilizando para ello lo que se denominan protocolos de consenso.

El más utilizado es el conocido como PoW, acrónimo en inglés de *Proof of Work* (Prueba de Trabajo).

El procedimiento consiste en proponer a la totalidad de nodos (llamados mineros, porque la operación se llama minar) la resolución de una incógnita con las siguientes características:

- Contiene la información de las transacciones incluidas en el bloque.
- Incluye asimismo una condición aleatoria a cumplir (por ejemplo, que los primeros 30 bits del hash sean ceros).
- No es de resolución automática. Esto quiere decir, que no existe un algoritmo o fórmula matemática de aplicación inmediata que lo genere, por lo tanto, la única manera de encontrar la solución a la incógnita planteada consiste en la realización de operaciones de computación a gran velocidad (método de prueba-error) hasta encontrarla.

Este sistema lleva implícita una ventaja o privilegio, es decir, no existe la igualdad a la hora de participar en la minería Blockchain.

En efecto, aquellos nodos cuya capacidad de computación sea muy grande tienen ventaja a la hora de resolver la incógnita planteada, ya que son capaces de realizar las operaciones matemáticas a mayor velocidad (mayor número de operaciones por unidad de tiempo), por lo tanto, la probabilidad de validar el bloque es mayor, si bien la seguridad absoluta no la tienen.

Se debe tomar en consideración que este sistema implica un gran consumo energético, si tenemos en cuenta que se trata de ordenadores con una enorme capacidad y, sobre todo, porque han de estar constantemente actualizando la totalidad de cadenas de bloques, con su correspondiente verificación o validación. Ello conlleva una importante inversión, tanto en los equipos, como en el suministro energético (a mayores de los gastos habituales en las actividades económicas como alquileres, sueldos, etc.).

Teniendo en cuenta lo anterior, se ha establecido un premio o incentivo para los mineros que consigan encontrar la solución a la incógnita planteada y la consiguiente validación de los bloques. Si aplicamos el ejemplo más conocido de utilización de Blockchain, las criptomonedas y, fundamentalmente, el Bitcoin, el minero que consigue validar un bloque y generar el *hash* correspondiente se queda con una comisión, establecida previamente.

Esta recompensa empezó siendo de 50 Bitcoins pero cada 4 años aproximadamente (210.000 bloques), se reduce a la mitad. A este proceso se le llama *halving*.

Actualmente la recompensa es de 12,5 Bitcoins por cada bloque minado. En un futuro dicha recompensa tendrá que ser de 1 Bitcoin ya que existe un número limitado de esta moneda.

Con la utilización de este protocolo tiene mucha relevancia la velocidad, o, mejor dicho, el tiempo medio que tarda la red de nodos en conseguir validar los bloques (actualmente unos diez minutos).

En efecto, cada bloque va llenando su lista de transferencias paulatinamente, y en cuanto se valida, finaliza, y se inicia el llenado de uno nuevo. A medida que la capacidad de computación de los ordenadores en Blockchain se incrementa, o acceden un mayor número de ellos a la red de nodos, las posibilidades de resolver las incógnitas generadoras de hashes aumentan, por lo que el tiempo de validación disminuye y, consecuentemente, los bloques se minarán cada vez más vacíos. Ello implicaría un incremento en los costes de las transacciones.

La forma de resolver este problema es incrementando la dificultad de resolución de las incógnitas, lo que se realiza periódicamente (aproximadamente dos semanas). Mediante cálculo de funciones de probabilidad se adapta el tiempo de validación de hashes a lo pretendido.

Existen otros protocolos de consenso, si bien son menos utilizados, como el PoS (*Proof of Stake*) y sus variantes: LPoS (*Leased Proof of Stake*) y DPoS (*Delegated Proof of Stake*).

En todos ellos el propio sistema asigna una probabilidad a cada minero en función de sus aportaciones a la red de nodos. En el segundo caso los mineros con poca capacidad pueden delegar su pequeña probabilidad a otro más grande y, en caso de haber recompensa, participaría de la misma en su proporción. El tercer caso es otra derivación, del PoS, en la que los nodos proponen a otros nodos para que estos decidan acerca de aspectos importantes del funcionamiento de Blockchain, tales como tiempo de validación o tamaño de bloques.

Existe asimismo distintas variantes del PoW, que en este caso se asigna probabilidad para generar *hashes* en función de su actividad en la red de mineros, si bien, como ya se ha apuntado, el más utilizado a nivel mundial es el PoW.

Llegados a este punto vamos a analizar cómo el funcionamiento de Blockchain consigue los cuatro objetivos fundamentales para los que fue creado: universalidad, ausencia de censura, seguridad en las transacciones y anonimato.

La universalidad está relacionada con la posibilidad de acceso a toda persona, física o jurídica, a la tecnología Blockchain y la red de nodos. Como hemos visto, para acceder a Blockchain únicamente se precisa, bien descargar un software libre, bien a través de webs especializadas que gestionen dicho acceso. En ambos casos, al menos en principio, no se prejuzga la posible utilización con fines maliciosos o fraudulentos, por lo que no hay restricciones, al menos inicialmente.

En cuanto a que hay ausencia de censura es obvio, al menos en lo que respecta a Gobiernos, instituciones financieras y de todas clases, ya que su funcionamiento se basa en internet sin intervención de estos organismos.

Teniendo en cuenta que la totalidad de información de los bloques se encuentra en todos y cada uno de los nodos, y estos se encuentran repartidos por todo el mundo, la posibilidad de censura sería impensable.

El tema del anonimato es relativo. La red Blockchain no es completamente anónima y, de hecho, es rastreable mediante técnicas de Big Data, si bien estas solo están al alcance de pocos, por lo que la cualidad del anonimato se puede decir que está garantizada en un porcentaje muy alto, sin que llegue al 100 %. Para aquellos que deseen un mayor nivel de privacidad, existen técnicas, como generar nuevas direcciones

Bitcoin desde nuestro monedero (*wallet*), mantener monederos diferentes en función del tipo de operación que queramos realizar, ocultar la IP mediante aplicaciones (navegador TOR), etc.

Sin embargo, incluso con la utilización de "trucos", el anonimato absoluto no existe, si bien, como ya se ha apuntado, el rastreo se encuentra al alcance de muy pocos.

Este apartado tiene importancia en otros aspectos que hacen, precisamente deseable, la no existencia del anonimato absoluto. Su utilización por redes criminales de blanqueo de dinero, transferencias opacas del narcotráfico, venta ilegal de armas, etc. tendrían un refugio seguro en Blockchain, así como el fraude fiscal, es decir, nos encontraríamos ante un auténtico paraíso fiscal.

Por último, en cuanto a la seguridad el funcionamiento de Blockchain está basado en dos códigos, los cuales se encuentran relacionados entre sí: el *hash*, del cual ya hemos hablado, y el nonce.

El *hash* es único para cada bloque y todos los bloques se encuentran relacionados por *hashes* validados. Cualquier intento fraudulento de modificar cualquier transacción de un bloque, modificaría su *hash* y, simultáneamente, todos los *hashes* de la cadena, por lo que es muy fácil detectar el fraude sin más que comparar, por ejemplo, el que teníamos correcto (validado) con el que nos aparece actualmente.

El nonce es un código cuya principal característica es que es aleatorio y que nos va a permitir generar hashes aplicando una condición previamente elegida. Evidentemente, si aplicamos la función hash a elementos fijos e invariables, como son el *hash* del bloque previo, la información de las transacciones y la firma del minero, siempre vamos a obtener el resultado, y muy rápidamente. Debemos por tanto introducir un número aleatorio que, una vez añadido a los códigos anteriores, estos cumplan una determinada condición en término de número de ceros iniciales.

Resumiendo, el funcionamiento de los mineros, ya apuntado anteriormente, consiste en probar constantemente con distintos nonces hasta conseguir que el resultado cumpla la condición preestablecida, en cuyo caso si es el primero en obtenerlo conseguiría el premio o comisión. Como vemos, se trata del protocolo PoW (*Proof of Work*).

Un aspecto importante a tener en cuenta es quién determina las condiciones que rigen en Blockchain, por ejemplo, el nivel de dificultad de resolución de las incógnitas, cambios en los códigos y, en definitiva, el software que rige el sistema.

El software es abierto y lo desarrollan unos programadores relacionados entre sí voluntariamente y sin una estructura jerárquica. Trabajan por consenso y sus conclusiones finales las aplican al sistema Blockchain. El problema surge cuando el consenso se rompe y existen grupos diferentes que tratan de imponer criterios distintos de funcionamiento. Es lo que se denomina como *forks*.

Esto sucedió en agosto de 2017 en lo referente a la criptomoneda Bitcoin. Dos grupos de desarrolladores no consiguieron ponerse de acuerdo y, finalmente, cada uno desarrolló distinto software, existiendo desde entonces, respecto de esa criptomoneda, el Bitcoin y el Bitcoin cash.

Por último, y aunque sea casi a nivel anecdótico, el funcionamiento de la tecnología Blockchain genera reticencias en la gente por su desconocimiento.

Actualmente existen empresas que están tratando de superarlas. Para ello han establecido un sistema de venta de cupones en estancos y otro tipo de locales, que, posteriormente, en su ordenador, los canjea por criptomonedas, con lo que ya puede comenzar a trabajar en Blockchain. Con ello se consigue acercar esta tecnología sin que tenga que implicar importantes conocimientos de la misma.

2.6 Aplicaciones

La principal aplicación de Blockchain, por lo que es mayormente conocido, es por ser la tecnología detrás de las criptomonedas, pero como bien hemos visto anteriormente, tiene muchas más posibles aplicaciones.

A continuación, explicaré brevemente algunas de ellas, pero cada día se estudia la posibilidad de extender esta tecnología a distintos ámbitos.

Imagen 3. Blockchain y contratos inteligentes

Fuente: (Cervera, 2018)

2.6.1 Criptomonedas

Las criptomonedas pueden considerarse simplemente como una moneda digital que funciona como un medio de cambio para la compra y venta de diversos bienes y servicios.

La realización de pagos transfronterizos puede ser, gracias a esta tecnología, un proceso rápido y poco costoso, ya que la cadena de bloques puede facilitar las transacciones entre pares (*peer to peer*), lo que significa que ya no es necesario que participen intermediarios.

Este tema será tratado más detalladamente en la siguiente parte del trabajo.

2.6.2 Contratos inteligentes

Son básicamente contratos con capacidad de autoejecutarse sin intermediarios, es decir, los contratos suelen tener un conjunto definido de requisitos que deben cumplirse para que sean válidos, sin embargo, requieren la presencia de una tercera parte para comprobar que se han cumplido las condiciones. En este caso, los contratos inteligentes pueden ser fácilmente implementados para reemplazar a dicho intermediario, ya que los requisitos pueden ser verificados algorítmicamente.

Para realizar el proceso de verificación y ejecución del contrato, es preciso que los organismos, instituciones y entidades involucradas admitan y se encuentren incluidos en Blockchain. Por ejemplo, en un contrato de compraventa de una vivienda, ha de ser posible para el contrato inteligente verificar que las transferencias se realizan correctamente y, en caso de incumplimiento, por ejemplo, poder remitir automáticamente y basado en los datos aportados, la demanda de desahucio al juzgado, y en caso de cumplimiento, remitir automáticamente al Registro de la Propiedad el documento generado de la transmisión (la escritura pública de compraventa), teniendo en cuenta que es posible verificar sin lugar a dudas, por parte de todos ellos, que todo está correcto.

En el caso de determinados contratos inteligentes, existe una circunstancia que hace precisa la intervención de terceros árbitros. Supongamos, por ejemplo, la realización de una apuesta en relación a si el Valladolid desciende a Segunda o se mantiene en Primera. Alguien "generalmente aceptado" debería "grabar" en el bloque correspondiente el resultado, dado que si nadie lo hace, el contrato inteligente no podría ejecutarse, en este caso, realizando la transferencia del perdedor al ganador, que previamente habían autorizado los apostantes en el contrato.

Para ello se han desarrollado herramientas informáticas que actualizan la información (Oracle, oráculo) con fuentes exteriores (mercados de divisas, resultados deportivos, etc.), aunque realmente siguen siendo terceros sobre los que hay que depositar cierta confianza, si bien generalmente verificable.

Este tema tan apasionante tiene muchas más vertientes. Por ejemplo, los aspectos legales. En la actualidad pocos países cuentan con legislación al respecto, si bien es de esperar que al popularizarse se promulguen normativas, sobre todo en el tema de la ejecución de contratos incumplidos.

2.6.3 Logística y cadena de producción

Gracias a Blockchain la falta de transparencia durante la movilidad de un producto a lo largo de la cadena de suministro, así como la posibilidad de que éste sea falsificado, desaparecen. Esto se logra gracias a la capacidad de la cadena de bloques para permitir la digitalización de los activos.

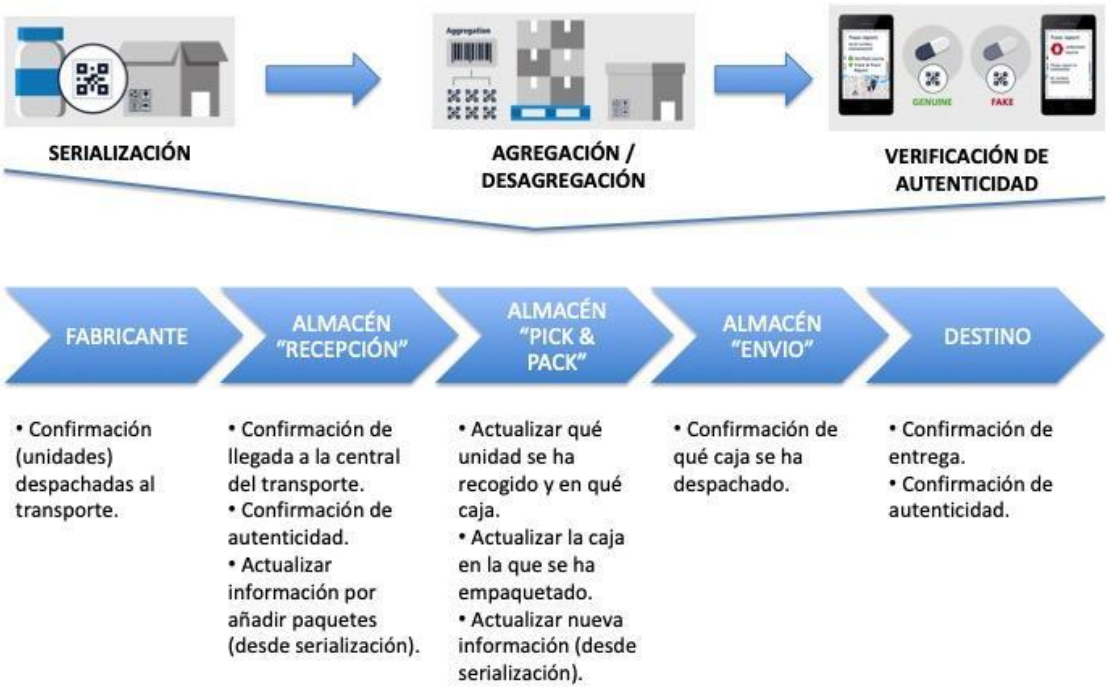
Con este método, los productos pueden ser etiquetados y asignados con identidades únicas que luego se trasplantan a una cadena de bloques transparente e

inmutable. Información sobre el producto, por ejemplo: el estado del producto, la hora, la ubicación, todo ello se puede rastrear en la cadena de bloques.

En efecto, la digitalización de activos habilitada para la cadena de bloques permite que la cadena de suministro de un producto se traslade de manera efectiva a una cadena de bloques.

Es lo que se denomina trazabilidad: procedimientos que permiten seguir el proceso de evolución de un producto en cada una de sus etapas. Es posible aplicarlo a todo el proceso productivo no solamente a la logística.

Imagen 4. Trazabilidad de productos farmacéuticos



Fuente: (Maestre, 2018)

2.6.4 Administración

Blockchain podría rastrear dónde y cuándo se ha pagado el IVA ayudando a evitar el fraude. Además, permitiría a la administración tributaria obtener los datos de manera inmediata y directa según se realiza una transacción, sin tener que esperar a informes trimestrales o anuales.

Asimismo, el comercio internacional se vería muy beneficiado, fundamentalmente en lo relativo a la gran cantidad de trámites en las aduanas. Por un lado, las empresas comerciales se evitarían la mayor parte de la tramitación, y por otro, la administración fiscal tendría una mayor seguridad en lo relativo a las mercancías transportadas.

2.6.5 Gobierno

El voto online es una aplicación que se está resistiendo debido a preocupaciones de seguridad y fraude. Con el voto físico, estas preocupaciones no existen, ya que el voto en papel está protegido de los hackers porque no puede ser alterado digitalmente. La cadena de bloques es la candidata adecuada para abordar los problemas de seguridad y fraude.

Blockchain puede eliminar las preocupaciones de fraude electoral al proporcionar un registro claro de los votos emitidos.

La piratería de un sistema de votación con cadena de bloques también sería una tarea difícil, debido a sus características a prueba de manipulaciones. Con las preocupaciones sobre la seguridad y el fraude disipadas, el proceso de votación podría llevarse a cabo en la comodidad de los hogares de los votantes, lo que podría contribuir significativamente a aumentar la participación de los votantes.

Además, en otro aspecto relativo al ámbito político, podría resolver el problema del desconocimiento del manejo de fondos públicos por parte de la población. Los fondos de inversión social quedarían en un registro contable común, asegurando que los recursos lleguen a los fines destinados. Así como el registro, seguimiento y auditoría del progreso de obras públicas. Es decir, los organismos encargados del control público del funcionamiento de la Administración pública, como la Intervención General de la Administración del Estado o el Tribunal de Cuentas, podrían acceder a una herramienta de valor incalculable para el cumplimiento de sus fines.

2.6.6 Inclusión económica

La tecnología Blockchain puede liberar muchos servicios financieros de los confines de las antiguas instituciones, fomentando la competencia y la innovación. Esto es bueno para el usuario final, incluso cuando se conecta a la vieja red de Internet, miles de millones de personas quedan excluidas de la economía por la sencilla razón de que las instituciones financieras no les proporcionan servicios como la banca porque serían clientes poco rentables y arriesgados.

Con la tecnología de la cadena de bloques, estas personas no sólo pueden conectarse, sino que también pueden ser incluidos en la actividad financiera, pudiendo

comprar, vender y de otro modo tener la oportunidad de construir una vida próspera. (*Blockchain revolution*, Don Tapscott and Alex Tapscott).

2.6.7 Servicios médicos

Crear un registro con los datos y el historial médico de los pacientes. Blockchain puede ayudar a aliviar los problemas encontrados dentro del cuidado de la salud al servir como una base de datos segura y a prueba de manipulaciones en la que se pueden almacenar los registros médicos de los pacientes.

Esto haría mucho más fácil para los médicos comprender mejor la historia clínica de un paciente, al poder acceder a información como por ejemplo los medicamentos que el paciente ha tomado en el pasado.

La cadena de bloques también sería útil para hacer frente a los medicamentos falsificados en la cadena de suministro médico, actuando como un medio con el que se puede verificar la autenticidad de estos. Los medicamentos serían etiquetados y rastreados en cada etapa de su cadena de suministro, y toda esta información se registraría en la cadena de bloques para asegurar su autenticidad (trazabilidad).

2.6.8 Propiedad intelectual

Las cadenas de bloques podrían aportar a la propiedad intelectual la plataforma para registrar la propiedad de los activos de estos mismos, de forma clara y precisa.

Cualquier disputa sobre el origen de una idea podría resolverse fácilmente refiriéndose a una cadena de bloques a prueba de manipulaciones que podría servir como una marca de tiempo que indicara exactamente cuándo se grabó la idea. Esto también proporciona a los titulares de derechos de propiedad intelectual la capacidad adicional de proteger sus activos de los infractores.

2.7 Especial mención: Ethereum

Ethereum fue creado en 2015 por Vitalik Buterin y actualmente es el líder de Blockchain programable. Utiliza la tecnología Blockchain con la red global de nodos y la verificación por el 51 % de estos.

La plataforma Ethereum puede ser utilizada en diferentes campos de negocios o finanzas. Se garantiza la seguridad y evita cualquier intrusión en el sistema. Empresas y servicios basados en Ethereum pueden hacer negocios con otras empresas y servicios que no conocen, sin riesgo de fraude.

Ethereum permite registrar cualquier tipo de operaciones con cualquier activo sin necesidad de recurrir a procedimientos judiciales. Esto lo hace preferible en comparación con los métodos actuales de registro de marcas.

Ethereum está programado como aplicación ejecutora condicionada, es decir, ejecuta las instrucciones recibidas si se cumplen las condiciones previamente establecidas.

Sobre los contratos inteligentes ya he hecho una exposición en un apartado anterior, al que me remito.

Las D-Apps son aplicaciones, como la apps, pero con una diferencia fundamental: son descentralizadas.

Las miles de apps existentes actualmente y que nos ayudan con una infinidad de utilidades tienen una característica en común, y es que son centralizadas, es decir, hay un desarrollador que pone a disposición de la gente la app de forma habitualmente gratuita, ya que, en unos casos pretenden facilitar la utilización de servicios propios de la empresa o entidad y en otros el incentivo es el cobro de una comisión por la inclusión de publicidad cuando se usa.

Por ejemplo, en el primero de los casos, empresas como El Corte Inglés o el banco BBVA quieren que, al descargarse la gente la aplicación en el móvil o la tableta, la utilice con habitualidad, con lo que consiguen fidelización (en el caso de un uso satisfactorio) y ahorro de personal al popularizar servicios a través de internet sin necesidad de acudir al centro comercial o a las oficinas.

Pero hay un aspecto muy importante a tener en cuenta en este tipo de apps: si en el caso de los ejemplos anteriores las entidades creadoras de la app decidieran cobrar una comisión cada vez que se utilice, los usuarios no tendrían más remedio que aceptarlo, ya que se trata de una app centralizada.

Las DApp son también apps pero con una diferencia fundamental: son los propios usuarios los que la desarrollan y de los que dependen.

Si realizamos una comparativa de las Apps tradicionales con las DApp, en la Apps existe la parte visible, que es la interfaz con la que interactuamos y la parte del servidor, que es donde se encuentran las bases de datos y el software que "traduce" lo que hemos solicitado en la interfaz. Posteriormente, nos devuelve la información solicitada.

En el caso de las DApp, lo solicitado a través de nuestra interfaz va a los smart contracts, descentralizados y verificables, que no dependen de instituciones u organismos.

Ventajas de las DApp frente a las Apps:

- Realizar pagos y cobros sin intermediarios: La multitud de transacciones en dinero que se realizan con instituciones financieras, como VISA, PayPal, etc. se podrían realizar a través de Ethereum, con una seguridad prácticamente absoluta y sin comisiones, o con una comisión mínima, mucho menor que las actuales.
- Facilitar creación y acreditación en cuentas de usuario: Al no ser necesario que los usuarios se registren y tener una única cuenta con llave pública y privada se puede vincular con cualquier DApp y sin el engorro de olvidar alguna de las muchas claves de acceso que hay que memorizar de tantas aplicaciones como utilizamos, y teniendo en cuenta además que en este caso no tendríamos el riesgo del cese del servicio, ya que es una red descentralizada.
- Confianza y tranquilidad: Podemos ver y validar los códigos del contrato inteligente basado en Ethereum, ya que funciona como la parte del software del servidor e una app tradicional. De esta forma nos podemos asegurar de que la ejecución inherente al *smart contract* es la que queremos que sea.

Podríamos resumir las diferencias entre las Apps tradicionales y las DApp en que estas últimas utilizan Blockchain como su parte del servidor, con el software de ejecución y las bases de dato necesarias para su funcionamiento.

Características de las DApp

- Descentralización: lo más importante, todo el poder de decisión lo tiene la comunidad de usuarios, sin intervención de entes controladores.

- Código abierto: Es decir, el software o código fuente que soporta la programación se puede modificar y mejorar por parte de la comunidad de usuarios. Este software ha de ser libre y gratuito e implementado por consenso de los usuarios.
- Blockchain: Aspecto también muy importante, ya que esta tecnología es la que soporta los bloques de información y funcionamiento. La cadena de bloques, en este caso, ha de ser pública.
- Protocolo de verificación: El funcionamiento de Blockchain necesita, no solo el almacenamiento en bloques de información, sino que estos también han de ser verificados.

En el apartado de protocolos de verificación expuse varios de ellos, siendo el más utilizado el PoW (*Proof of Work*, prueba de trabajo). Pues bien, este también es el utilizado habitualmente por las DApp, junto con el PoS (*Proof of Stake*, prueba de participación).

De esto se puede deducir que existen mineros que validan las transacciones, ya que son imprescindibles en estos protocolos de validación. Además, los mineros realizan su trabajo en base a recompensas o probabilidad de recibir recompensas, que normalmente serán en la moneda de Ethereum, los Ether.

Llegados a este punto, cabría preguntarse si a plataforma Ethereum es, en sí misma, una DApp.

Si lo analizamos teniendo en cuenta lo expuesto en el apartado anterior, podemos establecer que es una plataforma descentralizada, basada en la tecnología Blockchain, con un software de código abierto (open source) y que utiliza para el almacenamiento y la validación de los bloques el protocolo *Proof of Work* (habitualmente). En consecuencia, es claro que la plataforma Ethereum es una DApp.

La red de Bitcoin asimismo cumple con los anteriores requisitos como otras criptomonedas, por lo que pueden ser consideradas DApp a todos los efectos.

Tipos de DApp

El criterio para clasificar las DApp se basa en si tiene su propia Blockchain o si utilizan l cadena de bloques de otra DApp. Todas ellas, como ya hemos expuesto, son descentralizadas.

- DApp de tipo I: Estas aplicaciones tienen su propia cadena de bloques independiente. Por lo tanto, conforme a esta definición, Ethereum estaría encuadrada en este tipo, así como Bitcoin y otras menos conocidas como Litecoin.
- DApp tipo II: Este tipo utiliza la Blockchain de una DApp tipo I, es decir, no tienen una propia. Su funcionamiento a su vez se puede dividir en aquellas DApp con tokens de la Blockchain con la que operan o con tokens propios.
- Ejemplos de este tipo de DApp son Omni Layer (utiliza la Blockchain de Bitcoin) o Raiden Network (utiliza Ethereum).
- DApp tipo III: En este caso utilizan el protocolo de una DApp tipo II y, a su vez, pueden dividirse con el mismo criterio anterior, tokens propios o de la cadena de bloques utilizada.
- Como ejemplo de este tipo de DApp es Safe Network, que utiliza el protocolo de Omni Layer.

DApp más conocidas

- *Golem.* Con esta DApp lo que se consigue es un ordenador cuya potencia es igual a la suma de las potencias de multitud de ordenadores que los ceden o alquilan. Es decir, cuando en determinado momento se precisa un suplemento importante de potencia de nuestro ordenador, a través de esta DApp solicitamos a otros usuarios que nos alquilen los suyos y con la misma aplicación se unen para crear, durante un tiempo, un "superordenador". Posteriormente realizaríamos el pago en la moneda (criptomoneda) de la plataforma Golem. Gracias a esta DApp no es preciso adquirir un ordenador con una gran potencia (y por ello más caro) cuando solamente precisamos el suplemento de potencia eventualmente.
- *Augur.* Con esta DApp se apuesta sobre predicciones de eventos futuros reales. El funcionamiento es el siguiente. Primero se designa un evento, que tiene que ser real y verificable, y se nombra lo que se denomina un reportero (casi siempre). Posteriormente se realiza el intercambio de participaciones, que son apuestas sobre posibles resultados del evento. Una vez sucede el evento, el reportero o, en su caso, los tenedores del token de la aplicación determinan el resultado y, por último, se produce la liquidación, en la que los perdedores traspasan a los ganadores el importe de las apuestas.
- *Aragon.* Se trata de una aplicación que pretende facilitar la creación y utilización de estructuras organizativas de todo tipo. Es decir, basado en la plataforma Ethereum, las

personas pueden gestionar las empresas o instituciones sin intermediarios y de forma segura, con el consiguiente ahorro de costes, agilización de cualquier tramitación e incluso para la toma de decisiones. Ha sido creado por un español, Jorge Izquierdo.

Una de las aplicaciones descentralizadas más curiosas y que mayor éxito ha tenido, ha sido un juego, concretamente *Criptokitties*. Se trata de unos gatitos virtuales, que se pueden coleccionar, comprar y vender, siendo en realidad las monedas virtuales o criptomonedas. Además, tienen algunas curiosidades, como que pueden tener descendencia, utilizable también como criptomoneda.

Esta DApp tuvo tanto éxito que colapsó Ethereum, tratándose en realidad de una cadena Blockchain basada en iconos (no monedas), pudiendo ser este aspecto parte de su éxito.

Existe en los distintos sistemas operativos lo que se puede denominar una zona de adquisición de aplicaciones, donde descargárselas, bien de forma gratuita, bien pagando. Por ejemplo, en el sistema operativo Android, se llama Play Store.

Lo que sucede en este caso es que se trata de una *appstore* centralizada, gestionada por google. Por tanto, las decisiones y normas de funcionamiento las dicta google

En el caso de la plataforma Ethereum, como ya se ha indicado, todas las DApp están descentralizadas y se ha creado un portal web donde se encuentran todas las que están basadas en esta plataforma. Se denomina State of the DApp. Se agrupan mediante colores en función de su situación operativa, es decir, si son de funcionamiento, demos, fase beta, apagadas, etc.

Todas ellas se caracterizan además por una total transparencia, ofreciendo información acerca de inicio, descripción de funcionamiento, actualizaciones, licencia de software, autores, etc.

Hay una cuestión interesante en relación a la utilización de la plataforma Ethereum por los desarrolladores de aplicaciones. Si pueden utilizar su propia cadena Blockchain libremente, ¿Cuál es la razón de que masivamente utilicen la de Ethereum?

En realidad uno de los principales objetivos era ese precisamente, ofrecerse como plataforma (el otro es el desarrollo de contratos inteligentes), y para ello las DApp buscan dos características que tiene Ethereum:

- Seguridad: Si bien la seguridad absoluta 100 % no existe, pero la DApp soportada en Ethereum y su gran red de nodos hace que sea dificilísimo su crackeo.
- Interoperabilidad: Se trata de operar con la misma red Blockchain y mismo lenguaje. En efecto, si dos aplicaciones funcionan con distinto lenguaje y en redes Blockchain diferentes, si pretenden operar conjuntamente pueden producirse problemas de pérdida de datos u operaciones fallidas.

Al funcionar las DApp basadas en Ethereum, utilizan el mismo lenguaje, denominado Solidity, con lo que el procesado de la información será homogéneo. Asimismo, y no menos importante, al utilizar la misma red de bloques, se pueden aprovechar economías de escala, con la consiguiente reducción de tiempos y costes.

Crear una DApp es más sencillo de lo que parece, basta con seguir las siguientes cuatro fases:

1.- Documento de creación de la DApp, donde se exponen todos los aspectos a tener en cuenta, como objetivos, mecanismos de funcionamiento, etc. Se suele llamar White paper. De este documento suele depender, en gran medida, el éxito de la DApp.

2.- Programar las distintas fases del desarrollo de la DApp, con un criterio amplio en el sentido de admitir sugerencias de distintos ámbitos y la consiguiente posibilidad de modificaciones.

3.- Oferta inicial de moneda (ICO*, Initial Coin Offering*). Este es un paso necesario si no se dispone de financiación suficiente en la fase inicial. Una vez realizada una adecuada promoción de las bondades de la misma, se ofrece la nueva criptomoneda a cambio de otras, siendo el ratio de cambio algo a negociar.

4.- Desarrollo de la DApp, esto es, la parte técnica de su creación.

Algo básico a tener en cuenta es que es preciso familiarizarse con el lenguaje informático que utiliza Ethereum, es decir, *Solidity*. Sin embargo, es bastante parecido a JavaScript (este muy conocido), por lo que no es difícil adaptarse.

Por último, una serie de recursos y herramientas informáticas, como librerías, nodos, compiladores, etc. cuyo desarrollo no voy a exponer por ser algo muy específico para técnicos informáticos.

2.8 Blockchain en Valladolid

Valladolid es una ciudad muy implicada con el aprendizaje conjunto de esta tecnología. Tanto es así que la empresa Blockchain Valladolid ha creado su propia criptomoneda, VaCoin (VLL).

La empresa tiene varios proyectos en marcha para llevarlos a cabo en la comunidad y fomentar el uso y divulgación de Blockchain. Sus metas son:

Experimentar: Utilizarán el token en los próximos meetups para experimentar y realizar pagos entre los asistentes.

Votar: Realizarán diferentes apuestas para ver cómo poder utilizar el token para votar y ver como mejora al sistema tradicional que utilizamos actualmente.

DApp: Ampliarán conocimientos creando sus propias DApp (aplicaciones descentralizadas) que funcionen con la propia moneda de la Valladolid Coin.

Otro ejemplo de la implicación de nuestra ciudad es la cantidad de *meetups* que realizan. El primer evento tuvo lugar el 13 de diciembre de 2017, en la "Agencia de Innovación y Desarrollo Económico de Valladolid, con oradores, al investigador de Blockchain Miguel Martínez Arias" y Carlos Callejo González, fundador de Blockchain Valladolid.

En esta primera reunión se habló de Blockchain como revolución digital y de por qué todo el mundo habla de Bitcoin.

Desde sus inicios no han parado de organizar más y más *meetups* para lograr sus objetivos. Algunos de los temas que han tratado son: Inversión en ICO dentro del mundo de Blockchain, cómo comprar cualquier criptomoneda desde Euros, explicación del entorno de Bitcoin y cómo instalar un nodo y varios más.

También, añadir que el 13 de marzo pasado tuvo lugar en Valladolid (Arroyo de la encomienda) el primer foro nacional de Blockchain, en el cual Blockchain Valladolid fue partícipe.

El "Foro nacional de Blockchain para pymes y empresas" (nombre que se dio al evento) reunió a expertos de Blockchain de todo el país donde trataron las bondades de la tecnología Blockchain, financiación para proyectos Blockchain, ciberseguridad, impulso en las PYMES desde los DIH, los retos en el sector agroindustrial y el impacto social de Blockchain.

3 CRIPTOMONEDAS

Como he explicado antes, las criptomonedas pueden considerarse una moneda digital que funciona como un medio de cambio en la compra y venta de diversos bienes y servicios.

La cadena de bloques puede ser usada para resolver problemas como, enviar dinero internacionalmente de manera costosa y lenta. Por ejemplo, la red Bitcoin tarda diez minutos aproximadamente en realizar las transacciones desde su inicio hasta su liquidación. Pero, otras redes son aún más rápidas, de hecho, hay algunas redes que pretenden reducir el tiempo de liquidación a fracciones de segundo.

Además, también evita la privatización de acceso a servicios bancarios que algunas personas padecen. De esta manera Blockchain sirve como base sobre la cual se pueden construir criptodivisas.

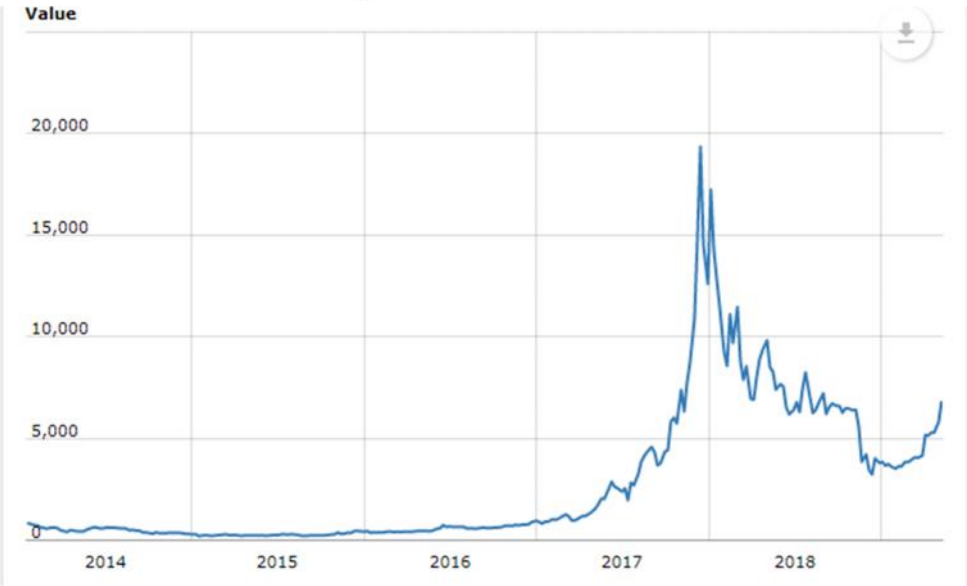
Las criptomonedas tienen más ventajas, por ejemplo, la gestión del riesgo. Usando este tipo de divisas, evitamos tres tipos de riesgo:

- De liquidación: este tipo de riesgo ocurre cuando hay un fallo técnico y nos devuelven la transacción.
- De agentes: este riesgo se da cuando los administradores de una transacción hacen mal uso de los trámites que llevan a cabo y ocultan malas prácticas.
- De la otra parte: este se da cuando tenemos la mala suerte que la otra parte, antes de que la transacción haya podido ser liquidada, quiebre.

3.1 Bitcoin

Como hemos podido ver al inicio de este trabajo, la historia de Blockchain y Bitcoin se fusionan y es así como en 2008, Satoshi Nakamoto presentaba un sistema de dinero electrónico, descentralizado, *peer to peer*, denominado Bitcoin. El 3 de enero de 2009, se realiza el primer bloque de Bitcoin que fue resuelto por Satoshi Nakamoto, obteniendo una recompensa de 50 Bitcoins.

Imagen 5. Valor de Bitcoin



Fuente: (WorldCoin Index, 2019)

El valor de Bitcoin a sus inicios era prácticamente nulo. No fue hasta febrero 2011 donde 1 Bitcoin era equivalente a 1 USD. Desde ese punto su tendencia se convierte en creciente con algún descenso (diciembre 2011). En abril de 2013 el valor era de 266 USD, dato sorprendente teniendo en cuenta que cuatro meses antes era solo de 2 USD.

El máximo histórico de Bitcoin es registrado el 11 de diciembre de 2017, alcanzando el valor de 19.798 USD. Esto posiblemente se deba a la venta de Bitcoins por parte de la CME (Chicago Mercantile Exchange).

Desde ese punto, su valor ha caído, con altibajos y parece ser, por ahora, lleva un ritmo creciente (a día 11 de mayo de 2019, ya que el valor de Bitcoin está en constante cambio).

3.1.1 Definición

Satoshi Nakamoto (2008) lo definió en el documento original de Bitcoin como una forma de dinero en efectivo electrónico puramente *peer-to-peer* que permite enviar pagos online directamente entre las partes y sin pasar a través de una institución financiera.

Pensemos en Bitcoin como en cualquier otro tipo de dinero solo que este tipo de moneda, consiste en una moneda digital que solo existe en la red Blockchain que la

soporta y gracias a un complejo proceso de verificación de transacciones, no puede gastarse más de una vez ni necesita ninguna entidad que la gobierne, pues son los propios usuarios los que se encargan de ello.

3.1.2 Carteras Bitcoin

Las transacciones realizadas en la Cadena Bloques son la base del sistema Bitcoin.

Toda transacción se tiene que llevar a cabo de una cuenta a otra, las cuales son denominadas carteras. Estas *wallets* funcionan como cuentas bancarias donde ocurren las transacciones.

Una cartera de Bitcoins es un fichero informático encriptado que te permite almacenar tu dinero Bitcoin.

Para interactuar entre las carteras se usa una clave o dirección pública única para todas las carteras. Cada cartera, además de tener esta llave, también tiene una dirección privada que actúa como un PIN para realizar transacciones con tu cartera.

Para poder llevar a cabo una transacción es necesario saber la clave pública de la cartera del usuario al que se quiere enviar dinero.

El siguiente paso, es utilizar la llave privada y así poder autorizar la transacción. Es aquí cuando se envía la transacción a la Cadena de Bloques donde los mineros de la red se encargan de verificarlo.

Existen tres tipos de carteras:

Carteras Software:

Este tipo permite el almacenamiento de tus Bitcoin en el dispositivo donde el usuario decida instalarla.

Ventajas: Enviar y recibir fácilmente monedas

Desventaja: Posibilidad de pérdida o intrusión por parte de hackers

Carteras hospedadas:

Estos monederos son administrados por terceras empresas. Para acceder a ellas se suele hacer a través de una aplicación o navegador web.

Ventajas: Proporcionan seguridad elevada aunque el grado de seguridad dependerá de la empresa que proporcione el servicio.

Desventaja: La posibilidad que la empresa desaparezca y por lo tanto también desaparezcan los Bitcoins de los usuarios.

Carteras físicas:

Estas carteras almacenan tu dinero de "forma física", normalmente en forma de papel o medio electrónico, sin conexión.

Ventajas: Útiles para la recepción de monedas.

Desventajas: No se pueden enviar, ya que necesitas conectarte a Internet para ello.

3.1.3 Características

Las características de Bitcoin son mayoritariamente comunes con las de Blockchain, ya que es la tecnología que hace posible el funcionamiento de esta criptomoneda.

- **Transparente**: Bitcoin usa una red Blockchain pública, por lo que todos los usuarios tienen acceso a todos los bloques pudiendo comprobar el estado actual y el historial de las transacciones.
- **Seguro**: Ya que, si alguien quisiese corromper la red, debería modificar todos los datos almacenados en cada nodo de la red hasta llegar al bloque génesis de Blockchain.
- **Descentralizado**: Quiere decir que no existe una autoridad o tercera parte que lo controle o que sea indispensable para su funcionamiento. Bitcoin funciona gracias a los usuarios actúan simultáneamente como clientes y servidores.
- **Rápido**: La transacción tardará lo que tarden los usuarios en verificar la información. El tiempo medio es de 10 minutos para Bitcoin. Además, también en cuestión de segundo puedes obtener tu monedero o cartera Bitcoin y empezar a operar.
- **Privado:** Los usuarios poseen claves que están asociadas a monederos, es decir, no aparece el nombre del usuario, pero el anonimato no es total, ya que se puede rastrear la dirección y descubrir quién está realizando las operaciones.
- **Limitado:** Esta característica la comparte con Blockchain.

Satoshi Nakamoto decidió limitar la creación de Bitcoin a 21 millones, que deberían estar en circulación hasta 2140. De esta manera, Nakamoto cree que no podrá haber hiperinflación ni devaluación, al menos no como las que causan las burocracias incompetentes o corruptas.

3.1.4 Funcionamiento

Bitcoin, como bien sabemos en este punto del trabajo, funciona gracias a la tecnología Blockchain. En este apartado aplicaré la información ya expuesta en el apartado del funcionamiento del Blockchain (página 12) en el caso del Bitcoin.

Supongamos que un usuario (con su monedero ya descargado) quiere enviar 10 Bitcoins a otro usuario (con su correspondiente monedero también).

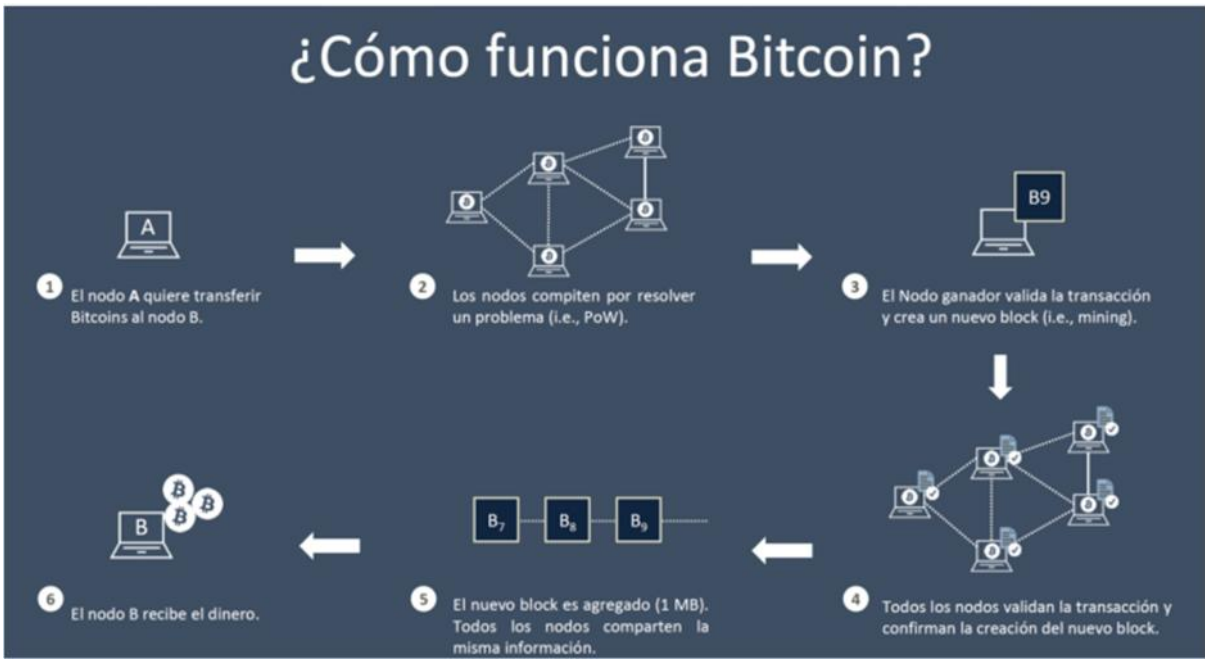
Pues bien, el primer usuario ordena la transferencia manualmente o a través del sitio web donde tiene descargada su cartera y firma la transacción con su clave privada.

Una vez la transacción está firmada, los nodos compiten por resolver la operación matemática y obtener la recompensa. Después, la red tiene que verificar dicha transacción. Como bien sabemos, los mineros de la red Blockchain se encargan de este proceso de verificación.

Una vez esta transacción es corroborada, queda reflejada en cada nodo de la cadena de bloques, sin posibilidad de eliminación o modificación.

En este punto, el usuario destinatario recibe el dinero y puede hacer uso de él.

Imagen 6. Blockchain y contratos inteligentes



Fuente: (Cervera, 2018)

3.2 Ether (ETH)

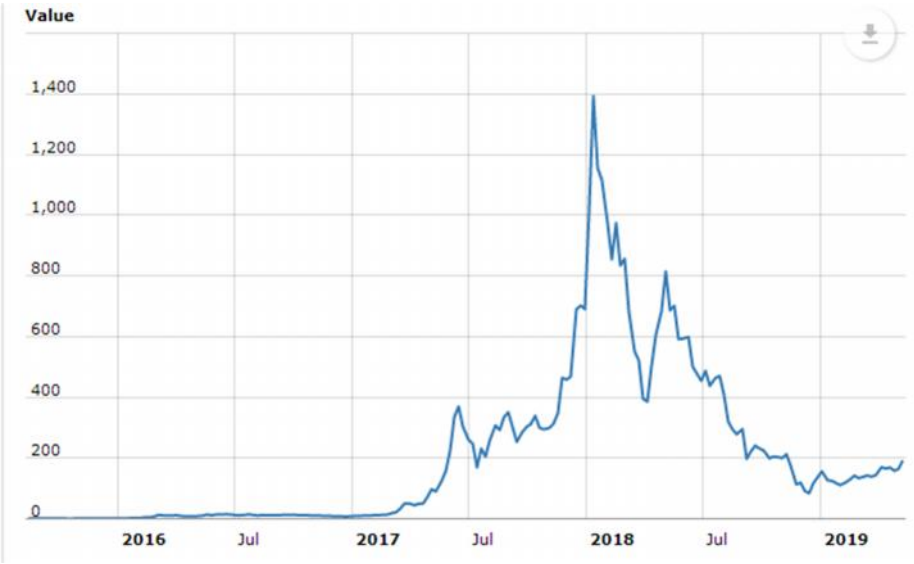
Cuando en 2015 se lanzó Ether, su valor era de 2,68 USD. Desde entonces se ha vuelto más y más popular.

En 2017 Ether comenzó a crecer rápidamente, pero no fue hasta enero de 2018 donde alcanzó su máximo histórico de 1.385,02 USD. Desde que alcanzó dicho máximo su valor ha disminuido mucho y a pesar de sus altibajos, actualmente se encuentra en 249, 36 (a día 26 de mayo de 2019, pues este dato está en constante cambio).

Esta moneda de Ethereum es sólo superada por Bitcoin en la capitalización de las criptomonedas.

Es importante no confundir esta criptomoneda con Ethereum Classic, que fue fruto de un *Hard Fork* (al igual que Bitcoin Cash de Bitcoin), y es autónoma del original de Ethereum.

Imagen 7. Evolución valor Ether



Fuente: (World Coin Index, 2019)

3.2.1 Definición

Ether es el nombre que recibe la criptomoneda de Ethereum.

La propia página Ethereum lo define como: “ETH Es dinero puramente digital, y puede ser enviado a cualquier persona en cualquier parte del mundo al instante. El suministro de ETH no está controlado por ningún gobierno o empresa, sino que está descentralizado y es limitado”.

Ether soporta contratos inteligentes y DApps que son llevados a cabo en la red Ethereum.

3.2.2 Monederos Ethereum

Los monederos Ethereum nos permiten enviar, recibir o guardar Ethers.

Cada monedero posee una dirección pública y una privada. Para enviar dinero necesitaré la clave pública de la persona que recibirá mi transacción y para poder realizar dicha transferencia, necesitaré mi clave privada.

Como ya hemos visto las carteras Bitcoin, quiero resaltar que, por lo general, en un mismo monedero o cartera no puedes hospedar diferentes tipos de monedas. De hecho, si se intenta transferir un tipo de moneda a una cartera no compatible, dicha cantidad de dinero se perdería.

Sin embargo, Ethereum sí que permite generar otros tokens o criptomonedas en su plataforma (como veremos más adelante durante la creación de mi criptomoneda). Es decir, yo puedo crear mi token, y que éste tenga un precio propio y que funcione en la red Ethereum.

Tipos de monederos Ethereum:

Online: Dentro de este tipo de monederos podemos diferenciar dos clases dependiendo de quién tiene el control de las claves.

Si prefiero que la dificultad de uso sea menor, entonces podré acceder al tipo de monedero donde yo no gestiono mi clave privada, pero por lo contrario, puedo registrarme y comprar criptomonedas con mi tarjeta del banco o por transferencia.

El problema de este tipo es que, si la empresa que lleva el control de mi clave cierra, yo no podría acceder a mi cartera, pero por lo demás no hay diferencia.

Si por el contrario prefiero tener el control total de mis criptomonedas, podré optar por la segunda opción de carteras online. Este tipo, es más complejo de usar pero aporta ese control total sobre tu dinero.

Extensión: Este tipo de cartera es el que usaré para crear mi criptomoneda más adelante.

Para usar este tipo, necesitaremos descargarnos (de manera gratuita) una extensión para Chrome o Firefox. Una vez descargado, nos darán 12 palabras que sirven para poder recuperar tu monedero cuando quieras usarlo desde otro navegador distinto.

Para este tipo, no hace falta facilitar ningún dato personal y además, te permite acceder a las DApp pero, no permite el intercambio con euros o dólares.

Software: Este monedero consiste en descargarse un programa que se instalará en el escritorio de tu ordenador. No hará falta proporcionar ninguna información y tendrás automáticamente tu monedero.

No puedes intercambiar criptomonedas por Euros, Dólares o demás tipos de dinero fiduciario.

Son seguras y sencillas, pero si alguien accediese a tu ordenador podría usar tus fondos y no puedes usarlo para todo tipo de criptomonedas.

Físicos: La manera más sencilla de explicar este tipo, es pensando que son *pen drives* que su función es guardar criptomonedas. Es el tipo más seguro de monedero, aunque su dificultad de uso es algo mayor.

También están los monederos de papel que son un registro donde almacenas todas tus claves para poder llevar a cabo transacciones.

En Exchange: Estos son como una casa de cambio web. Este tipo, aporta análisis y distintas herramientas para la compraventa, además, puedes comprar y guardar cualquier criptomoneda. El problema es que no puedes comprar las criptomonedas a partir de euros o dólares y que no existe el anonimato pues te tienes que registrar ni tampoco serás el dueño de tus claves privadas.

3.2.3 Características y Diferencias con BTC

Las características de Ether son las mismas que Bitcoin, y que a su vez de Blockchain pero, como bien hemos visto antes siempre hay alguna peculiaridad.

Pues sí, Ether es segura pues necesitas el protocolo de consenso y la información está repartida entre todos los nodos de la red. También es descentralizada pues no hay una entidad que la gobierne ni regule. Es *Peer to Pee*r por lo que también es distribuida y es transparente, dado que es una red Blockchain pública que todo el que forma parte de ella posee toda la información de todas las transacciones que hayan ocurrido en la red.

Entonces, ¿qué le diferencia de Bitcoin? Pues bien, yo veo dos grandes diferencias entre estas criptomonedas.

La primera es que la oferta de Bitcoin es de 21 millones en total, mientras que la de Ether es de 18 millones al año.

La segunda, es que Ether su función principal es operar dentro de Ethereum, crear y ejecutar contratos inteligentes. La función principal de Bitcoin es ser un sistema de pago.

Otro dato a añadir respecto a ambas criptomonedas es la recompensa que reciben los mineros de las distintas redes. Mientras que en Bitcoin es de 12,5 Bitcoins, en Ether es de 3, además del tiempo que tardan en procesarse los bloques, en Ether son 16 segundos mientras que en Bitcoin son aproximadamente 10 minutos.

Por último, en Ether el coste de las transacciones depende de la velocidad que quieras dar a tu transacción y en Bitcoin el coste de dicha transacción es siempre el mismo.

3.2.4 Funcionamiento

Ether, funciona en la plataforma Ethereum y, por lo tanto, a través de Blockchain.

Ethereum, a diferencia de Bitcoin, lanzó una preventa de Ether en 2014, con la que recaudó 18 millones de USD lo cual fue la causa impulsora de que la oferta inicial de Ether fuera de 72 millones.

Ethereum se basa en el protocolo de *Proof of Work* y los mineros que consiguen crear el nuevo bloque, lo que ocurre cada 16 segundos aproximadamente, reciben una recompensa de 3 ETH. Anteriormente, esta recompensa era de 5 y a los mineros que intentaban resolverlo, pero no lo conseguían, recibían una recompensa menor, llamada *Mining uncle reward* que era de 2 o 3 Ether.

La configuración de la red Blockchain es muy parecida a la de Bitcoin, pues es un registro distribuido del historial de todas las transacciones y cada nodo almacena una copia.

La mayor diferencia con Ether es que sus nodos guardan el estado más reciente de los contratos inteligente, además de las transacciones que se realicen de Ether.

Para cada posible aplicación de Ethereum, la red necesita hacer un seguimiento del estado actual de esas aplicaciones, incluyendo el saldo de todos los usuarios, el código completo del *Smart Contract* y también, dónde está almacenado.

Bitcoin usa las salidas de transacciones no utilizadas para reconocer quién tiene dicha cantidad de Bitcoin. Para realizar transacciones futuras, la red Blockchain de Bitcoin debe calcular todas las piezas de cambio, que se clasifican como "gastadas" o "no gastadas".

Ethereum, sin embargo, usa cuentas.

Así como los fondos de las cuentas bancarias, los tokens de Ether aparecen en una billetera y se pueden portar a otra cuenta. Los fondos siempre están en alguna parte, pero no tienen lo que se podría llamar una relación continua.

3.3 Otras criptomonedas

3.3.1 Monero

La principal característica que destaca de Monero es la capacidad de minería. Esto se debe a que en vez de usar el protocolo *Proof of Work*, utiliza *CryptoNote*, que permite minar con ordenadores de menor potencia, como un portátil.

La cadena de bloques detrás de esta criptomoneda no es como la de Bitcoin, pues no podemos ver todas las transacciones que han ocurrido con Monero.

3.3.2 Dash

Una de las peculiaridades de Dash es la alta seguridad del sistema pues no solo posee 11 algoritmos, además proporciona anonimato.

Respecto a este último punto, creo importante recordar que con Blockchain, por lo general, no es necesario registrarse ni dar información personal pero sí que las transacciones quedan registradas y con grandes procesadores se pueden rastrear.

3.3.3 Ripple

Esta criptomoneda pretende facilitar la gestión de créditos a los bancos, tanto en tiempo como en dinero, pues les permite evitar los controles transfronterizos.

Puede sonar extraño que una criptomoneda pueda ser especialmente usada por los bancos, pues una de las ventajas de estas es que evita la necesidad de entidades bancarias. Pero, no es extraño, pues grandes bancos ya usan criptomonedas para abaratar y agiliza sus operaciones.

3.3.4 Litecoin

Si hemos entendido el concepto de Bitcoin entonces no tendremos problemas en entender Litecoin, pues funcionan igual.

Eso sí, existen dos cosas que las diferencian. La primera es la oferta total, mientras que en Bitcoin son 21 millones, en Litecoin es de 84 millones.

La segunda diferencia es el tiempo necesario para crear nuevos bloques, en Bitcoin es de aproximadamente 10 minutos y en esta criptomoneda es de 2,5 minutos, reduciendo la potencia necesaria de los nodos para resolver la operación aleatoria.

3.4 Creando mi criptomoneda

A la hora de crear una criptomoneda tenemos dos opciones, crear nuestra propia red, como puede ser Bitcoin o Ethereum o usar una red de la segunda generación de Blockchain.

Puesto que no poseo los conocimientos ni existe la necesidad de ello, yo utilizaré la red Ethereum.

Para empezar, debemos descargarnos la extensión de Google Chrome llamada *Metamask*. Esta extensión es el puente que permite ejecutar Ethereum DApp directamente en el navegador sin necesidad de ejecutar un nodo Ethereum completo.

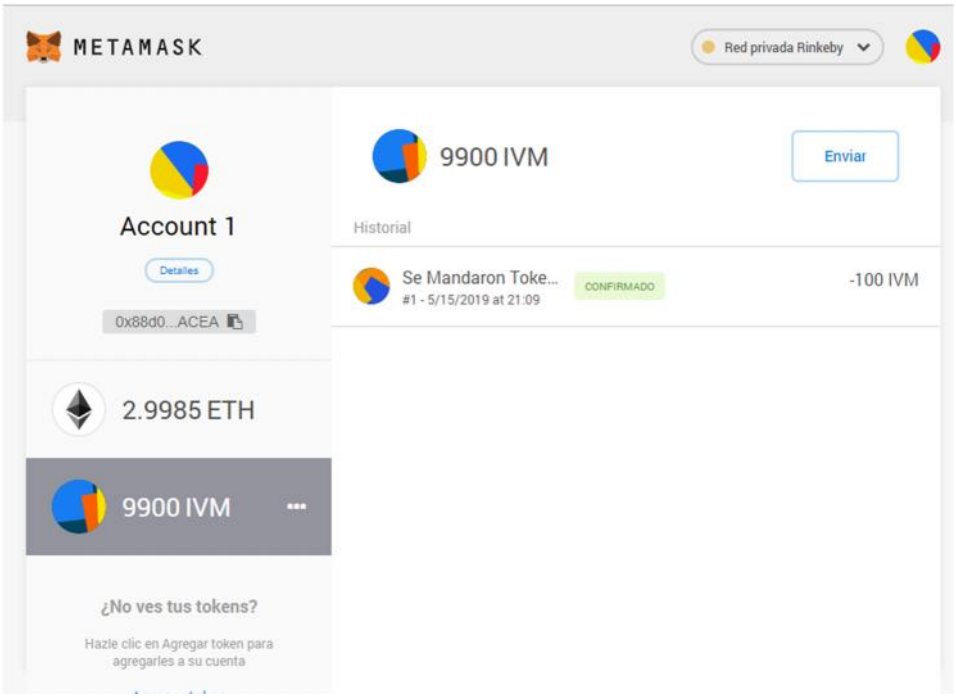
En ella no nos preguntan ningún dato respecto a nuestra información personal, simplemente te dan la opción de insertar o crear una cartera.

Como yo aún no tenía ninguna, lo primero que hice fue descargarme el monedero.

Una vez dentro, te dan tu clave privada, que no puedes perder ya que si la pierdes lo que poseas en dicha cartera no podrá volver a usarse.

Como dato curioso, existen 21 millones de Bitcoins de los cuales 17 están en funcionamiento y 4 han desaparecido por esta razón.

Imagen 8. Aspecto de una cartera Metamask



Fuente: Elaboración propia

Un aspecto que quiero aclarar es que cuando me refiero a que voy a usar Ethereum, no utilizaré la red principal de Blockchain en sí, ya que para ello tendría que pagar. Para mi criptomoneda utilizaré *Rinkeby,* que es una red que funciona igual que la principal (con menos ordenadores) y de manera gratuita.

Este tipo de redes se llaman *Testing nets* (redes de prueba).

¿Para qué usamos Ethereum?

La respuesta es, porque tenemos que crear un contrato inteligente (*Smart contract*) donde podamos escribir la información de nuestra moneda, como, por ejemplo, la cantidad de monedas que queremos emitir, el nombre, los decimales, etc.

Para poder escribir esta información utilizaremos el lenguaje *Solidity*, que es el que soporta los *Smart Contracts. Solidity*, es otro tipo de lenguaje informático como puede ser Java Script o HTML.

Esto puede parecer complejo, pero, no hay necesidad de saber utilizar *Solidity*, pues en *Github* (una página web) lo tienes ya escrito.

Primero buscamos *Github ConsenSys*. Una vez hemos accedido a ello, buscamos tokens y como primera opción nos aparecerá *ConsenSys/Tokens Ethereum tokens contract*s, pinchamos ahí.

Una vez dentro, veremos distintas carpetas. Nosotros nos fijaremos en la primera, *Contracts*. Dentro de *contracts* pulsaremos eip20.

Por ahora dejamos esa ventana abierta, porque primero, tenemos que llevar a cabo otros pasos.

Lo siguiente que debemos hacer es pedir Ether de prueba. Para conseguirlo hay distintas formas. En este caso, accederemos a *Rinkeby Authenticated Faucet*, y en una de tus redes sociales (Facebook o Twitter) deberás escribir tu dirección pública (la cual tienes en tu cartera *Metamask*), copiar el link de ese post y pegarlo en *Rinkeby Authenticated Faucet.*

Esto es así porque si no la misma persona podría pedir muchos Ether de prueba.

Una vez hemos hecho ese paso, deberíamos tener los Ether que hemos pedido en nuestra cartera *Metamask*. Debemos tener cuidado cuando busquemos en nuestra cartera ya que por defecto nos va a salir Red principal Ethereum y no es ahí donde debemos buscar, en este caso es en *Rinkeby*.

Ahora, debemos acceder a Remix de Ethereum y a la vez a la página abierta anteriormente de *Github.*

En la parte superior izquierda de Remix encontraremos un signo más, debemos clicar ahí para crear un nuevo *Smart Contract*. Lo primero que vas a tener que hacer es darle un nombre al nuevo contrato. En mi caso lo he llamado IVMtoken.

Una vez nombrado, veremos una página en blanco donde podemos escribir. Es aquí donde entra en juego la página ya abierta de *Github*, con el lenguaje *Solidity* ya escrito.

Entramos en EIP20.sol y copiamos todo lo que venga escrito y lo pegamos en nuestra página remix.

Imagen 9. Lenguaje Solidity en Smart Contract de Ethereum

```
pragma solidity ^0.4.21;

import "./EIP20Interface.sol";


contract EIP20 is EIP20Interface {

    uint256 constant private MAX_UINT256 = 2**256 - 1;
    mapping (address => uint256) public balances;
    mapping (address => mapping (address => uint256)) public allowed;
    /*
    NOTE:
    The following variables are OPTIONAL vanities. One does not have to include them.
    They allow one to customise the token contract & in no way influences the core functionality.
    Some wallets/interfaces might not even bother to look at this information.
    */
    string public name;                   //fancy name: eg Simon Bucks
    uint8 public decimals;                //How many decimals to show.
    string public symbol;                 //An identifier: eg SBX

    function EIP20(
        uint256 _initialAmount,
        string _tokenName,
        uint8 _decimalUnits,
        string _tokenSymbol
    ) public {
        balances[msg.sender] = _initialAmount;               // Give the creator all initial tokens
        totalSupply = _initialAmount;                        // Update total supply
        name = _tokenName;                                   // Set the name for display purposes
```

Fuente: Elaboración propia

Una vez lo tengamos pegado, debemos cambiar el nombre del contrato, de EIP20 a IVMtoken, así como el nombre de la función. Es decir, el nombre del contrato y de la función tiene que ser el mismo (IVMtoken) porque es la función constructora.

Si nos fijamos al principio de este documento de *Solidity*, veremos que en esta función hay otra integrada. Esto significa que necesitamos el lenguaje *Solidity* de esta segunda función. Para conseguir este documento, volvemos a la página de *Github* y en vez de coger el primer documento de la carpeta *contracts*, usaremos el tercero, EIP20interface.sol.

Copiamos como hicimos con EIP20 y en una pestaña nueva de nuestra página remix, pegamos. Esta vez cuando creemos la nueva página, la llamaremos como el documento que acabamos de copiar, EIP20interface.sol.

Volviendo al documento IVMtoken, en la función que hemos cambiado el nombre, veremos que contiene cuatro apartados. Ahí es donde diremos la cantidad inicial de tokens, el nombre del token, cuantos decimales y, por último, el símbolo.

La función, depositará en la cartera del creador del contrato todos los tokens que haya decidido crear.

En este punto, ya tenemos el contrato escrito, ahora solo queda ponerlo en funcionamiento. Para este paso, debemos acceder a la pestaña Run, dentro de la página remix, donde tenemos IVMtoken.

Una vez en Run, veremos la palabra *Environmen*t y una pestaña con tres opciones, de las cuales elegiremos *Injected 3.*

Ahora, más abajo, ya podemos seleccionar IVMtoken en vez de EIP20interface.sol y empezar a dar los cuatro valores que he mencionado antes (la cantidad inicial de tokens, el nombre del token, cuantos decimales y el símbolo).

En el caso de mi criptomoneda los valores que he dado han sido los siguientes:

- Cantidad inicial de tokens: 10.000
- Nombre del token: IVMtoken
- Decimales: 0
- Símbolo: IVM

Estos valores se escriben entre comillas en el apartado donde pone *Create*. Una vez escritos, pulsamos *Create*.

La ventana de *Metamask* se abrirá automáticamente. Es aquí cuando entran en juego los Ether de prueba que pedimos a través de nuestras redes sociales. ¿Por qué? Porque para llevar a cabo cualquier transacción en el sistema Ethereum, hay que gastar Ether.

Tenemos tres opciones: que la transacción sea rápida, media o lenta y con ello, cambiará la comisión que tienes que pagar, de mayor a menor respectivamente.

Yo seleccioné media, por lo que pagué 0,00001 Ether. Y tardó unos segundos en realizar la operación.

Una vez hecha la transacción, en esa misma página de remix, podemos comprobar el balance copiando nuestra dirección pública y pegándola donde pone Balance, entre comillas.

Para poder ver nuestro token en nuestra cartera *Metamask*, debemos pulsar en el menú izquierdo de *Metamas*k y agregar token.

Añadimos token personalizado, pegando la dirección del contrato que hemos creado, y el símbolo de la moneda. Nos aparecerá en pantalla y daremos a agregar.

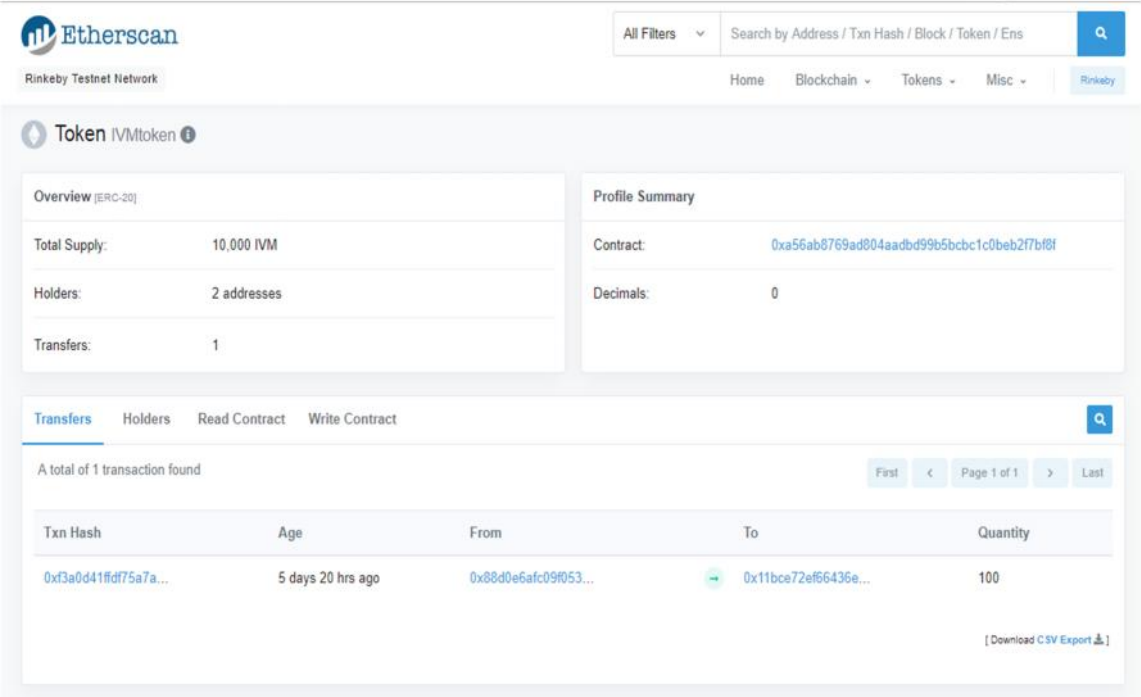
Ahora IVMtoken ya está en mi cartera (importante mirar siempre en la red *Rinkeby*) y puedo hacer transacciones dentro de esta red de prueba.

Llegados a este punto, si queremos comprobar el estado de la criptomoneda, podemos hacerlo a través de Etherscan, que es una plataforma donde te permite explorar y buscar en la cadena de bloques de Ethereum las transacciones, direcciones, fichas, precios y otras actividades que tienen lugar en Ethereum.

Para poder encontrar IVMtoken, no podemos olvidarnos que debemos buscar en la red *Rinkeby*. Esto en Etherscan se selecciona en el símbolo de Ethereum que suele situarse en la esquina de arriba a la derecha, justo al lado de la opción de iniciar sesión.

Una vez estemos ahí, al escribir el nombre en el buscador deberá aparecernos la criptomoneda con la siguiente información:

Imagen 10. Seguimiento de criptomonedas en Ethereum



Fuente: (EtherScan, 2019)

Como podemos ver en la imagen tenemos *Total supply* de 10.000 IVMtokens, eso es la cantidad de suministro total que previamente se determinó.

Holders se refiere a la cantidad de usuarios que poseen esta criptomoneda. En este caso somos dos, pues para comprobar que la criptomoneda funcionaba, realicé una transferencia a un amigo. De hecho, esta transferencia es el siguiente dato que aparece, *transfers*.

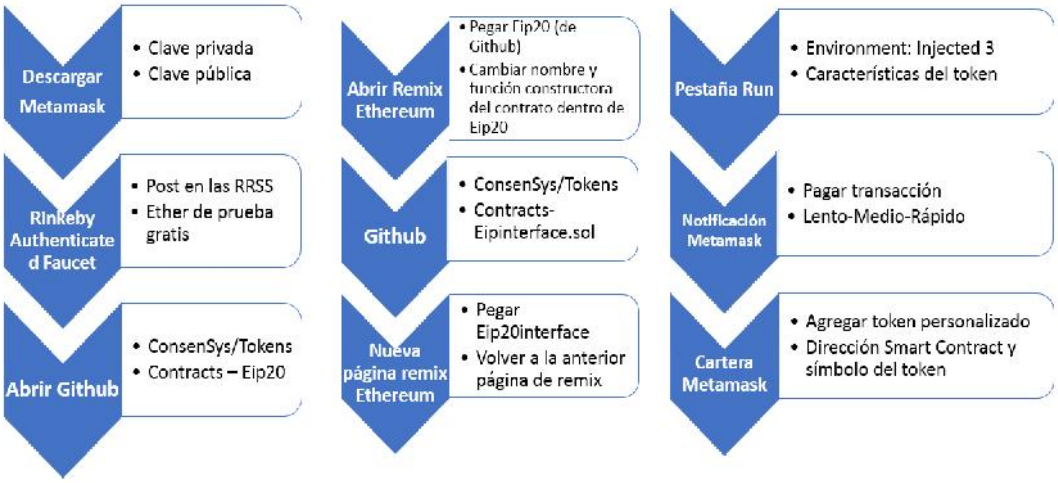
A la derecha, en *profile summary* podemos ver la dirección pública del *Smart contract* que creé previamente para poder llevar a cabo mi criptomoneda. Debajo de esto, observamos que tiene decimales como definí anteriormente.

Por último, en la parte inferior de la imagen podemos ver la transferencia, es decir a la izquierda, está el *hash* de la transacción, seguido de la dirección pública de mi cartera, y a su vez seguido del momento de la transferencia. Después la clave pública de la persona a la que hice la transferencia y finalizando, a la derecha, la cantidad de tokens que envié en dicha transacción.

Llegados a este punto, la criptomoneda ya está creada y comprobado su funcionamiento.

Esto quiere decir que, si yo quisiese lanzar mi criptomoneda a la red principal de Ethereum y que mi token tuviese un valor, simplemente tendría que pagar las tasas necesarias, y eso sería todo, pues los demás pasos necesarios son los puestos en marcha en este apartado del trabajo.

Imagen 11. Pasos creación criptomoneda



Fuente: Elaboración propia

4 CONCLUSIONES

Actualmente dependemos de terceras partes que aporten confianza y verifiquen nuestra identidad en distintos tipos de transacciones. Sin embargo, gracias al sistema de cadena de bloques podemos rebajar e incluso eliminar dicha confianza. Asimismo, esta revolucionaria tecnología hace posible que los usuarios puedan poseer una identidad verificable y segura criptográficamente generando de esta manera la confianza necesaria.

Además, reduce mucho los costes, el tiempo y los riesgos de las transacciones y, a su vez, estimula el crecimiento.

Blockchain evita la dependencia actual que tenemos hacia los bancos ya que proporciona este nuevo tipo de cuenta corriente y de ahorro y, además, aporta a instituciones un mecanismo más eficaz para la compra-venta y el almacenamiento de activos financieros.

También, con el ejemplo de IVMtoken se muestra su funcionamiento, con su rapidez y, además, muestra realmente como es el mundo de las criptomonedas, dando un enfoque práctico y no teórico de lo que es.

En mi opinión, Blockchain va a cambiar (y ya está empezando) el modo en el que vivimos, cómo compramos, cómo realizamos y firmamos contratos, cómo votamos, cómo pedimos un crédito y mil posibilidades más que esta tecnología nos ofrece.

Además, cada día se estudian más escenarios en los que se puede aplicar y, en todos, implicaría una mejoría.

5 BIBLIOGRAFÍA

Allende, M. (2018a). *¿Pública, federada o privada? Explora los distintos tipos de Blockchain.* Recuperado el 3 de mayo de 2019, de https://cutt.ly/2iyBhr

Allende, M. (2018b). *Cómo desarrollar confianza en entornos complejos para generar valor de impacto social.* Recuperado el 17 de abril de 2019, de https://cutt.ly/ViyL4b

Binance Academy. (2018). *La Historia de Blockchain* [vídeo online]. Recuperado de https://cutt.ly/NiyZUY

Bitcoin Project. (2019). *Cómo empezar a usar Bitcoin.* Recuperado el 15 de abril de 2019, de https://cutt.ly/YiqcuP

Blockchain Luxembourg. (2019). *Bitcoin para principiantes.* Recuperado el 12 de mayo de 2019, de https://cutt.ly/DiynBy

Cervera, G. (22 de febrero de 2018). *Blockchain y contratos inteligentes* [SlideShare]. Recuperado el 8 de junio de 2019, de https://cutt.ly/bivMPJ

Criptocampus. (2018). *Introducción al Bitcoin (Parte I).* Recuperado el 11 de abril de 2019, de https://cutt.ly/iiyGvu

Criptonoticias. (2019). *Qué es Bitcoin.* Recuperado el 14 de mayo de 2019, de https://cutt.ly/viyK1B

Crypto Español. (2017a). *Cómo funciona Bitcoin. Wallets, mineros, forks, Blockchain. Explicación sencilla y completa español* [Vídeo online]. Recuperado el 10 de abril de 2019, de https://cutt.ly/oiyRND

Crypto Español. (2017b). *Cómo funciona Blockchain. Explicación sencilla visual en español* [Vídeo online]. Recuperado el 10 de abril de 2019 de https://cutt.ly/RiyWxs

Ethereum Team. (2014). *Ethereum for beginners.* Recuperado el 25 de abril de 2019, de https://cutt.ly/Eiqmfd

EtherScan. (2019). *Ethereum Blockchain Explorer*. Recuperado el 20 de junio de 2019, de https://cutt.ly/toVo3g

García, A. (2018). *Peer to Peer (P2P) Juntos somos poderosos porque somos muchos.* Recuperado el 10 de abril de 2019, de https://cutt.ly/PiyKsq

Gutiérrez, B. (8 de abril de 2012). *De las redes centralizadas a las distribuidas* [Blog]. Recuperado el 8 de junio de 2019, de https://bit.ly/2wGOj8l

Haber, S. y Scott, W. (1991). How To Time-Stamp a Digital Document. *Journal of Cryptology*, 3, pp. 99-111.

Ivan on Tech. (2018). *How to create your OWN cryptocurrency in 15 minutes - Programmer explains.* Recuperado el 15 de mayo de 2019, de https://cutt.ly/5iyTI0

Ladrero, I. (15 de diciembre de 2017). *Blockchain: qué es y para qué sirve* [Blog]. Recuperado el 5 de mayo de 2019, de https://cutt.ly/JiyNiu

Nakamoto, S. (2008). *Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer.* Recuperado de https://cutt.ly/yo0n9g

Olóndriz, P. (2018). *Ethereum wallet/Monedero. Guía completa sobre monederos online y físicos para guardar tus Ether.* Recuperado el 27 de abril de 2019, de https://cutt.ly/fiqQCW

Oro y Finanzas–Portal Oro. (2016). *¿Qué debe saber un inversor antes de comprar Ether, la criptomoneda de Ethereum?* Recuperado el 29 de abril de 2019, de https://cutt.ly/CiqWma

Pastor J. (2017). *Qué es Blockchain: la explicación definitiva para la tecnología más de moda*. Recuperado el 20 de abril de 2019, de https://cutt.ly/viqx04

Redes informáticas Agustin. (2012). *Redes entre iguales y redes cliente-servidor.* Recuperado el 10 de abril de 2019, de https://cutt.ly/ViyJiP

Rodríguez, N. (2018). *Historia de la tecnología Blockchain: Guía definitiva.* Recuperado el 1 de mayo de 2019, de https://cutt.ly/viqxs6

Simondrl y Maurelian. (2019). *Tokens/contracts/eip20/.* Recuperado el 19 de junio de 2019, de https://cutt.ly/CoVpgs

Tapscott, D. y Tapscott A. (2016). *Blockchain Revolution*. New York: Portfolio Penguin.

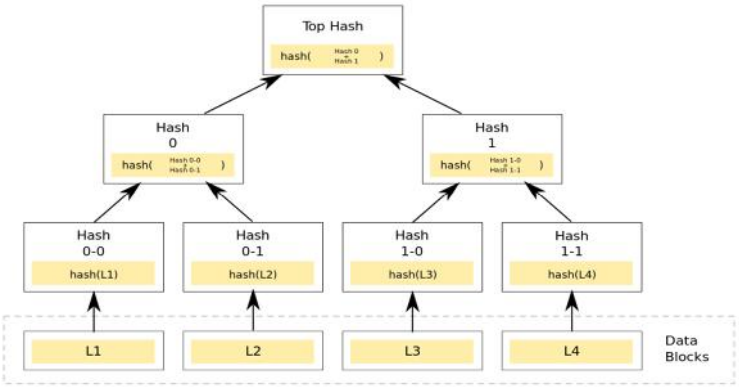
World Coin Index. (2019). *Cotización criptomonedas con dólar*. Recuperado el 21 de junio de 2019, de https://cutt.ly/RoVocC

6 ANEXOS

Anexo I. Glosario de términos

Árbol de Merkle: Estructura que toman los datos en forma de árbol jerárquico. Es decir, agrupa datos separados ligándolos a un único valor hash.

Imagen 12. Árbol de Merkle



Fuente: Imágenes de Google

Hash: es el código alfanumérico que se obtiene aplicando una función matemática, conocida como función hash (codificando una entrada con un algoritmo determinado), a un conjunto de datos concatenados. A cada conjunto de datos le corresponde un único hash.

Los hash tienen una particularidad muy especial: es un proceso de un solo sentido. Si el algoritmo de este tipo está correctamente desarrollado debe ser casi imposible obtener el texto de entrada a partir de la salida hash.

Nonce: El nonce es un código alfanumérico totalmente aleatorio. Se añade ara que el hash no solo sirva para identificar un bloque sino que añada seguridad. Si simplemente usáramos un conjunto fijo de elementos (las transacciones, la firma y el hash del bloque previo) al aplicar la función matemática siempre obtendríamos el mismo hash, por lo que no sería seguro.

PoW: Proof of Work (prueba de trabajo) consiste en un protocolo de consenso respecto a la respuesta la operación matemática para la creación de los siguientes bloques de la cadena. Satoshi Nakamoto “El trabajo medio que hace falta es exponencial

en el número de cero bits requeridos y puede verificarse ejecutando un único hash".

Token: Es una unidad de valor, emitida por una entidad privada, que tiene el valor que se le otorga dentro de una comunidad. Por lo tanto, todas las criptomonedas son consideradas tokens.

Anexo II. Lenguaje Solidity (EIP20.sol) para el Smart Contract de la criptomoneda

Imagen 13. EIP.sol

```
/*
        Implements EIP20 token standard:
        https://github.com/Ethereum/EIPs/blob/master/EIPS/eip-20.md
        .*/



        pragma Solidity ^0.4.21;


        import "./EIP20Interface.sol";



        contract EIP20 is EIP20Interface {


            uint256 constant private MAX_UINT256 = 2**256 - 1;
            mapping (address => uint256) public balances;
            mapping (address => mapping (address => uint256)) public allowed;
            /*
            NOTE:
            The following variables are OPTIONAL vanities. One does not have to
        include them.
            They allow one to customise the token contract & in no way influences the
        core functionality.
            Some wallets/interfaces might not even bother to look at this information.
            */
            string public name;                   //fancy name: eg Simon Bucks
            uint8 public decimals;                //How many decimals to show.
            string public symbol;                 //An identifier: eg SBX
```

```
    function EIP20(
        uint256 _initialAmount,
        string _tokenName,
        uint8 _decimalUnits,
        string _tokenSymbol
    ) public {
        balances[msg.sender] = _initialAmount;              // Give the
creator all initial tokens
        totalSupply = _initialAmount;                       // Update total
supply
        name = _tokenName;                                  // Set the name
for display purposes
        decimals = _decimalUnits;                           // Amount of
decimals for display purposes
        symbol = _tokenSymbol;                              // Set the symbol
for display purposes
    }


    function transfer(address _to, uint256 _value) public returns (bool
success) {
        require(balances[msg.sender] >= _value);
        balances[msg.sender] -= _value;
        balances[_to] += _value;
        emit Transfer(msg.sender, _to, _value); //solhint-disable-line indent,
no-unused-vars
        return true;
    }


    function transferFrom(address _from, address _to, uint256 _value) public
returns (bool success) {
        uint256 allowance = allowed[_from][msg.sender];
        require(balances[_from] >= _value && allowance >= _value);
        balances[_to] += _value;
        balances[_from] -= _value;
        if (allowance < MAX_UINT256) {
            allowed[_from][msg.sender] -= _value;
```

```
        }
        emit Transfer(_from, _to, _value); //solhint-disable-line indent, no-
unused-vars
        return true;
    }


    function balanceOf(address _owner) public view returns (uint256 balance) {
        return balances[_owner];
    }


    function approve(address _spender, uint256 _value) public returns (bool
success) {
        allowed[msg.sender][_spender] = _value;
        emit Approval(msg.sender, _spender, _value); //solhint-disable-line
indent, no-unused-vars
        return true;
    }


    function allowance(address _owner, address _spender) public view returns
(uint256 remaining) {
        return allowed[_owner][_spender];
```

Fuente: (Simondrl y Maurelian, 2019)

Anexo III. Lenguaje Solidity (EIP20interface.sol) para la función del Smart Contract

Imagen 14. EIP20interface.sol

```
//
Abstract
contract
for the
full ERC
20 Token
standard
            // https://github.com/Ethereum/EIPs/blob/master/EIPS/eip-
            20.md
            pragma Solidity ^0.4.21;

// https://github.com/Ethereum/EIPs/blob/master/EIPS/eip-20.md
pragma Solidity ^0.4.21;




contract EIP20Interface {
    /* This is a slight change to the ERC20 base standard.
    function totalSupply() constant returns (uint256 supply);
    is replaced with:
    uint256 public totalSupply;
    This automatically creates a getter function for the totalSupply.
    This is moved to the base contract since public getter functions are
not
    currently recognised as an implementation of the matching abstract
    function by the compiler.
    */
    /// total amount of tokens
    uint256 public totalSupply;


    /// @param _owner The address from which the balance will be retrieved
    /// @return The balance
```

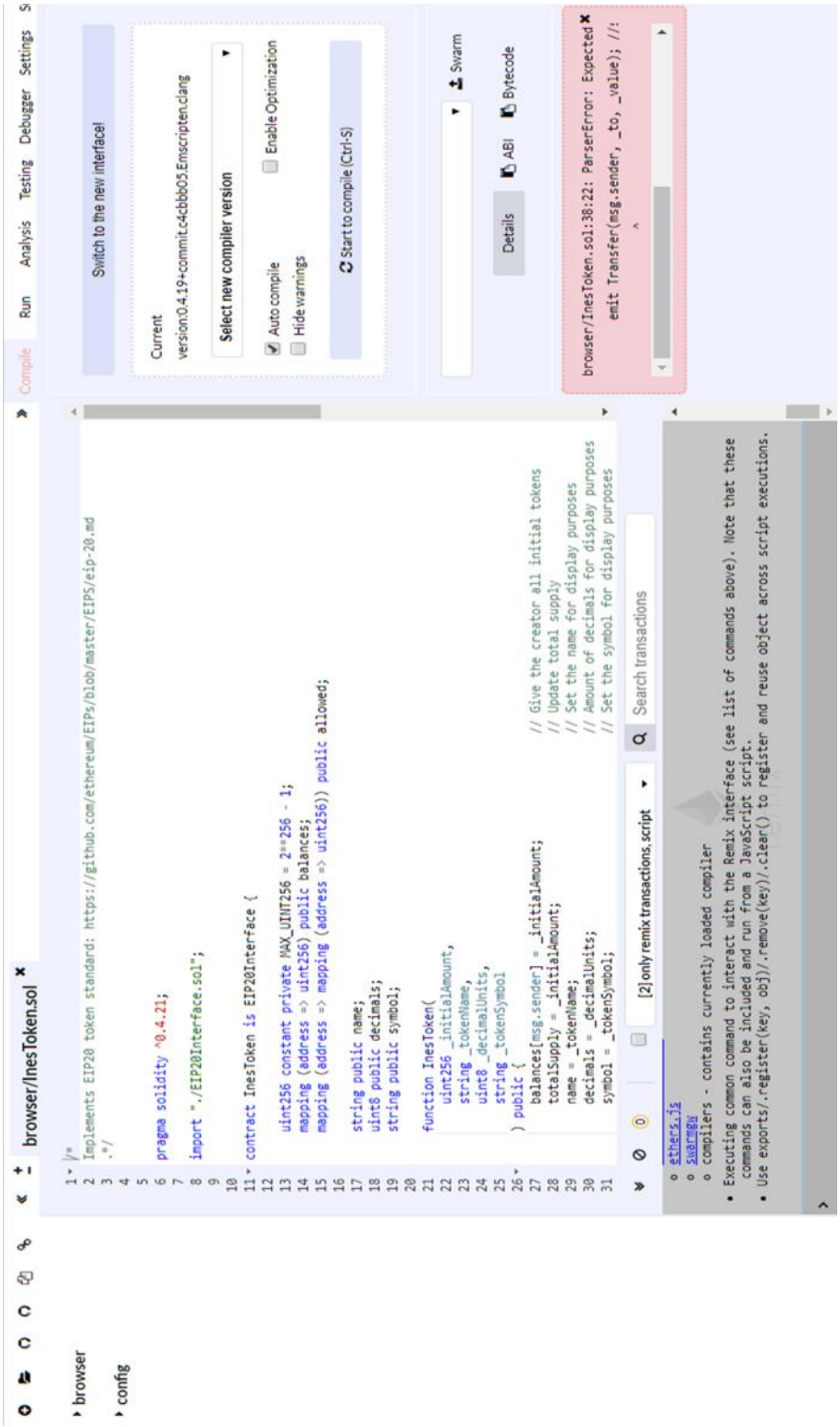
```
    function balanceOf(address _owner) public view returns (uint256
balance);


    /// @notice send `_value` token to `_to` from `msg.sender`
    /// @param _to The address of the recipient
    /// @param _value The amount of token to be transferred
    /// @return WhEther the transfer was successful or not
    function transfer(address _to, uint256 _value) public returns (bool
success);


    /// @notice send `_value` token to `_to` from `_from` on the condition
it is approved by `_from`
    /// @param _from The address of the sender
    /// @param _to The address of the recipient
    /// @param _value The amount of token to be transferred
    /// @return WhEther the transfer was successful or not
    function transferFrom(address _from, address _to, uint256 _value)
public returns (bool success);


    /// @notice `msg.sender` approves `_spender` to spend `_value` tokens
    /// @param _spender The address of the account able to transfer the
tokens
    /// @param _value The amount of tokens to be approved for transfer
    /// @return WhEther the approval was successful or not
    function approve(address _spender, uint256 _value) public returns
(bool success);


    /// @param _owner The address of the account owning tokens
    /// @param _spender The address of the account able to transfer the
tokens
    /// @return Amount of remaining tokens allowed to spent
    function allowance(address _owner, address _spender) public view
returns (uint256 remaining);
```

```
    // solhint-disable-next-line no-simple-event-func-name
    event Transfer(address indexed _from, address indexed _to, uint256
_value);
    event Approval(address indexed _owner, address indexed _spender,
uint256 _value);
}
```

Fuente: (Simondrl y Maurelian, 2019)

Anexo IV. Apariencia página Remix de Ethereum

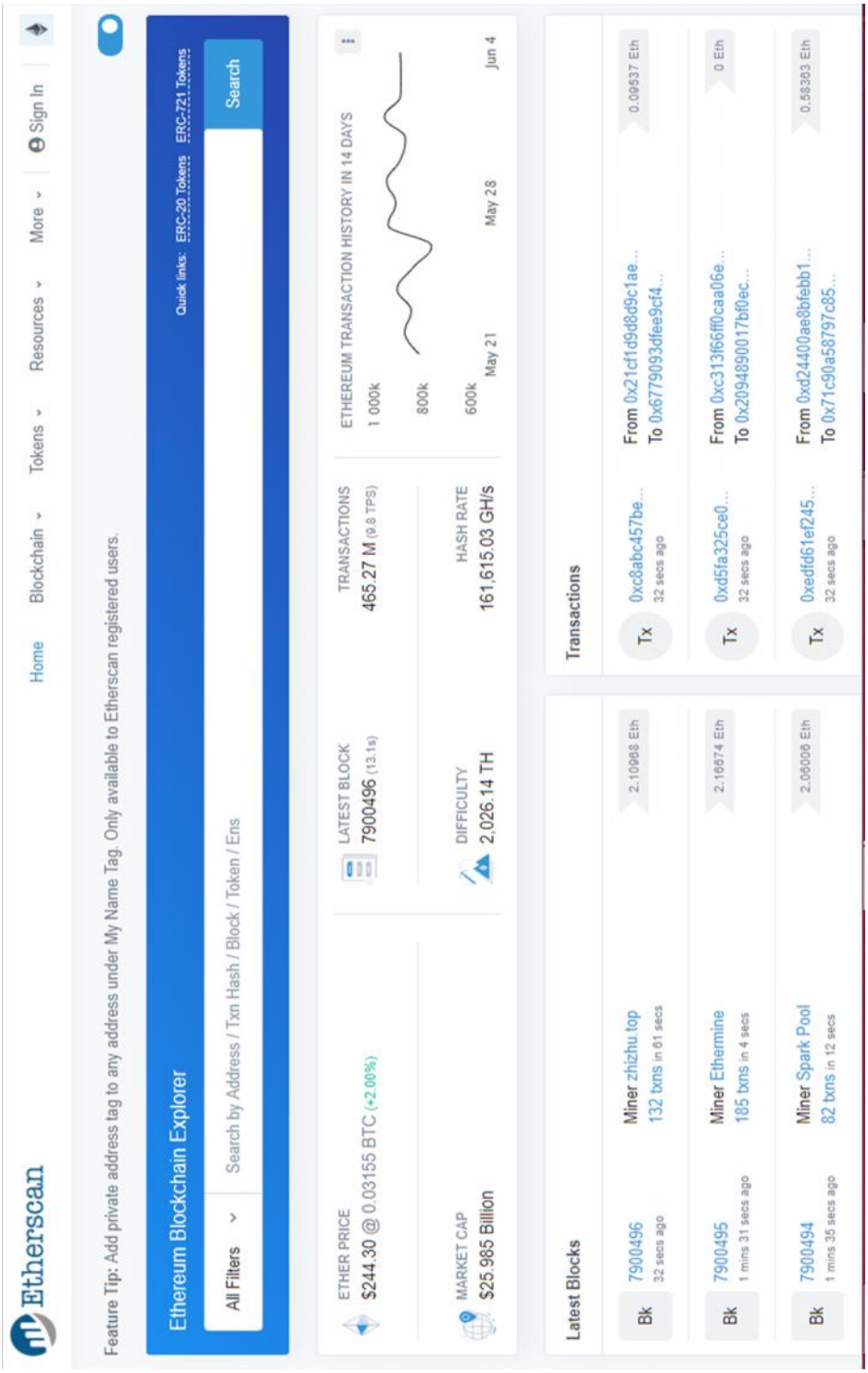
Imagen 15. Remix



Fuente: (Remix Ethereum, 2019)

Anexo V. Apariencia Etherscan

Imagen 16. Etherscan



Fuente: (Etherscan, 2019)