Trabajo Fin de Máster

Máster Interuniversitario en Seguridad de las tecnologías de la información y de las comunicaciones –MISTIC–.

Estudio de tecnologías *Bitcoin* y *Blockchain*.

Alumno:
José María Sevillano Acevedo.

Directora del Trabajo Fin de Máster:
D.ª Ángela María García Valdés.

Profesor responsable de la asignatura:
D. Víctor García Font.

Empresa:
Incibe.

Fecha:
4 de junio de 2018.

Dedicatoria y agradecimientos.

Mi agradecimiento, admiración y respeto a las Universidades promotoras y al equipo docente del *Máster Universitario de Seguridad de las tecnologías de la información y las comunicaciones* por hacer posible el sueño de estudiar a tantos profesionales que queremos seguir completando nuestra formación aún después de incorporados a la masa laboral.

Sus conocimientos profesionales y frecuentes aportaciones han sido fundamentales para progresar en el camino del Máster.

A mis compañeros de Máster, grandes referentes en el día a día e interlocutores de apoyo mutuo con sus aportes de diferentes puntos de vista en las herramientas colaborativas como los Foros.

A mi familia, piedra angular de mi vida y apoyo fundamental.

Por último y no menos importante a mi tutora D.ª Ángela María García Valdés por su ayuda y comprensión en la realización y tutorización de este trabajo y al profesor responsable de la asignatura: D. Víctor García Font.

Ficha del trabajo final.

Título del trabajo:	Estudio de tecnologías *Bitcoin* y *Blockchain*.
Nombre del autor:	José María Sevillano Acevedo.
Nombre del consultor/a:	Ángela María García Valdés.
Nombre del PRA:	Víctor García Font.
Fecha de entrega (mm/aaaa):	06/2018.
Titulación:	Máster Interuniversitario en Seguridad de las tecnologías de la información y de las comunicaciones –MISTIC–.
Área del Trabajo Final:	M1.830 - TFM-Ad hoc aula 1.
Idioma del trabajo:	Castellano.
Palabras clave:	*Bitcoin*, *Blockchain*, Criptomoneda.

Tabla 1. Ficha del trabajo final.

Resumen del trabajo.

El objetivo de este Trabajo Fin de Máster es llevar a cabo un estudio sobre las tecnologías *Bitcoin* y *Blockchain*.

Se han estudiado los principios de operación de la red *Bitcoin*, su arquitectura, organización y la estructura básica: transacciones, bloques y cadena de bloques, las ventajas del modelo *peer-to-peer* respecto del modelo tradicional y los beneficios de estas tecnologías y sus aplicaciones actuales y futuras.

Después se ha enfocado el estudio en las tecnologías *blockchain* en general, exponiendo sus aplicaciones actuales y probablemente futuras.

También se ha trabajado sobre el concepto de *Smart Contracts* y los mecanismos de consenso en *blockchain* y sus fortalezas y debilidades.

Se han repasado las diferencias entre *blockchain* público y privado y se ha profundizado en los aspectos de seguridad y criptografía.

Por último, se ha incorporado al estudio información de otros *blockchains*.

Palabras clave: *Bitcoin*, *Blockchain*, Criptomoneda.

Abstract.

The goal of this Master's Final Essay is to accomplish a deeper knowledge about Bitcoin and Blockchain technologies.

For this purpose I studied the principles of the Bitcoin network operational system, its design, organization and basic structure: transactions, blocks and blockchains, the advantages of peer-to-peer system versus the traditional one and the benefits of these technologies and current and future applications.

After that I focused in the blockchain technology in general showing its actual applications and possible future ones.

I also worked about the Smart Contracts concept and the mechanism of agreement in blockchain, its strengths and flaws.

I reviewed the differences between public and private blockchain and investigate deeper in cryptography and security topics.

Finally I completed the essay adding information about other blockchains.

Keywords: *Bitcoin*, *Blockchain*, *Cryptocurrency*.

Tabla de contenidos.

Tabla de ilustraciones.

Tabla de tablas.

1. Introducción y objetivos del proyecto.

Introducción.

Debido al creciente interés en las nuevas tecnologías y las criptomonedas y sus tecnologías afines la finalidad de este Trabajo Fin de Máster es familiarizarnos con los principios de operación de la red *Bitcoin* y su *Blockchain*.

Como aproximación a la cuestión vamos a identificar y exponer los beneficios que genera la tecnología *Blockchain* y sus aplicaciones actuales y posibilidades futuras en *Bitcoin* y otros criptosistemas en general; explicando las ventajas y desventajas de los diferentes mecanismos de consenso de *blockchain* y resumiendo las diferencias entre *blockchain* público y privado.

Nos proponemos conocer la arquitectura y organización de la red *Bitcoin*, exponer los conceptos de transacción, bloque y cadena de bloques y describir el funcionamiento del consenso y su alcance, e introducir los diferentes *blockchains* en uso en varios criptosistemas (*Bitcoin*, *Ethereum*, *Ripple*, *Litecoin*).

Vamos a explicar las ventajas y desventajas de los diferentes mecanismos de consenso de *blockchain* y comparar y exponer las ventajas del modelo *peer-to-peer* y el modelo de transacción tradicional.

Por último, vamos a exponer el concepto de *Smart Contracts* y estudiar los diferentes aspectos de seguridad de *Bitcoin*, *blockchain* y *Smart Contracts*.

Objetivos del proyecto.

- Conocer la arquitectura y organización de la red *Bitcoin*.
- Exponer los conceptos de transacción, bloque y cadena de bloques.
- Comparar y exponer las ventajas del modelo *peer-to-peer* y el modelo de transacción tradicional.
- Introducir los diferentes *blockchains* (*Bitcoin*, *Ethereum*, *Ripple*, *Litecoin*).
- Exponer las aplicaciones actuales y futuribles de la tecnología *blockchain*.
- Describir el funcionamiento del consenso y cómo se alcanza en la red *Bitcoin*.
- Explicar las ventajas y desventajas de los diferentes mecanismos de consenso de *blockchain*.
- Resumir las diferencias entre *blockchain* público y privado.
- Exponer el concepto de *Smart Contracts*.
- Estudiar los aspectos de seguridad de *Bitcoin*, *blockchain* y *Smart Contracts*.

2. Enfoque y método seguido.

Para llevar el trabajo a buen término la estrategia elegida el método es el Estudio Explicativo con la realización de una investigación bibliográfica y documental para aproximar las diferentes premisas que nos facilitan acerca del trabajo, con el fin de tomarlo como base para documentarnos y más adelante concluir la investigación para poder desarrollar el material definitivo del contenido del trabajo; que además debe tener cierto aspecto divulgativo.

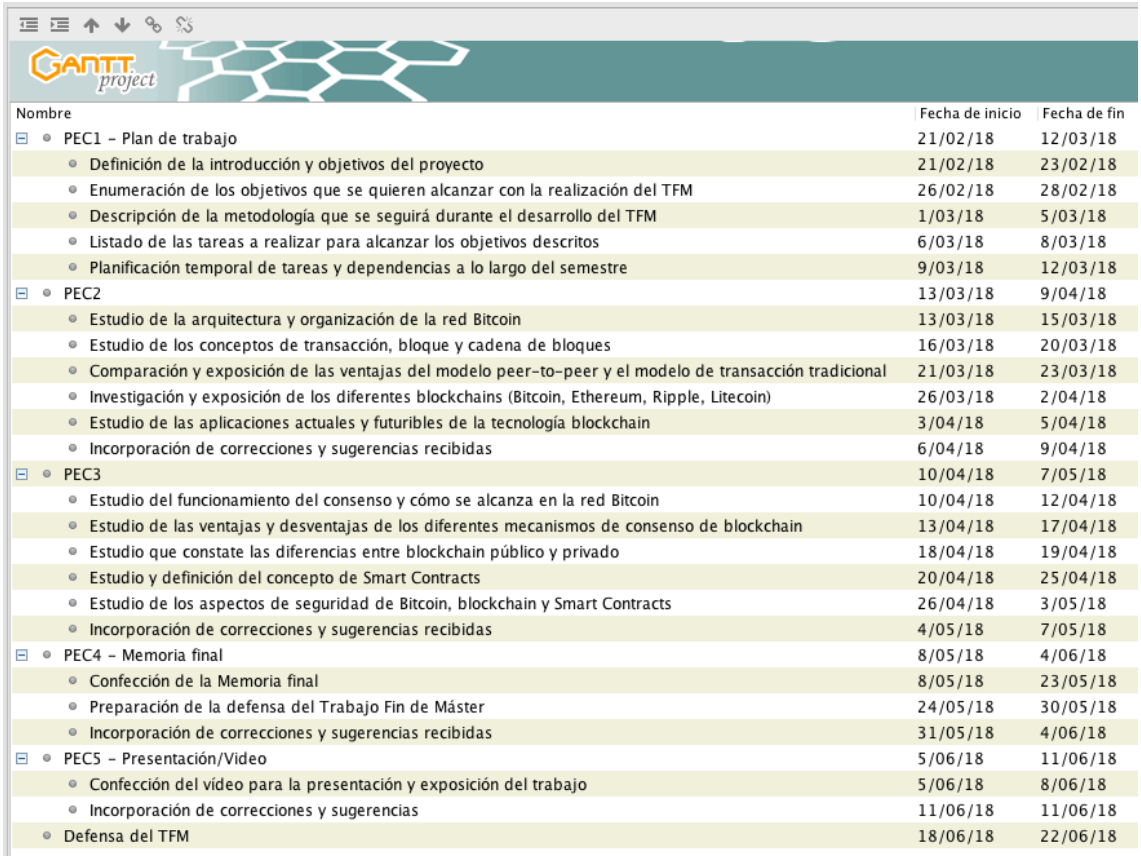
Metodología del trabajo.

- Búsqueda de información e investigación a través de diversas fuentes de materiales orientados a sustentar la confección de documentación relativa a cada objetivo.
- Extracción de conclusiones en función de la información recabada una vez integrada y elaborada.
- Redacción de contenido que dé respuesta a los objetivos del trabajo en función de las conclusiones obtenidas.
- Trabajo en diferentes iteraciones con ciclos de incorporación de correcciones y sugerencias recibidas hasta lograr el resultado deseado.

3. Listado de tareas para alcanzar los objetivos descritos.

- Definición de la introducción y objetivos del proyecto.
- Enumeración de los objetivos que se quieren alcanzar con la realización del TFM.
- Descripción de la metodología que se seguirá durante el desarrollo del TFM.
- Planificación temporal de tareas y dependencias a lo largo del semestre.
- Estudio de la arquitectura y organización de la red *Bitcoin*.
- Estudio de los conceptos de transacción, bloque y cadena de bloques.
- Comparación y exposición de las ventajas del modelo *peer-to-peer* y el modelo de transacción tradicional.
- Investigación y exposición de los diferentes *blockchains* (*Bitcoin*, *Ethereum*, *Ripple*, *Litecoin*).
- Estudio de las aplicaciones actuales y futuribles de la tecnología *blockchain*.
- Estudio del funcionamiento del consenso y cómo se alcanza en la red *Bitcoin*.
- Estudio de las ventajas y desventajas de los diferentes mecanismos de consenso de *blockchain*.
- Estudio que constate las diferencias entre *blockchain* público y privado.
- Estudio y definición del concepto de *Smart Contracts*.
- Estudio de los aspectos de seguridad de *Bitcoin*, *blockchain* y *Smart Contracts*.
- Confección de la Memoria final de acuerdo con las especificaciones recibidas y el documento *P08/89018/00446 Presentación de documentos y elaboración de presentaciones*, teniendo presentes los documentos *Normativa de los trabajos finales de máster de ámbito profesional* y *P08/89018/00445 Redacción de textos científico-técnicos*, además de la información de apoyo incluida en los documentos *Informe_Evaluacion_TFM_es_v3.doc* y *Criterios_Evaluación_TFM_es_v1.doc*.
- Preparación de la defensa del Trabajo Fin de Máster y recursos adicionales para su correcta exposición y resolución de imprevistos.
- Incorporación de correcciones y sugerencias recibidas de todas las PEC's.
- Confección del vídeo para la presentación y exposición del trabajo de acuerdo con las especificaciones recibidas y el documento *PID_00191586 Exposición de contenidos en video*.
- Defensa del TFM.

4. Planificación del trabajo.



Nombre	Fecha de inicio	Fecha de fin
PEC1 – Plan de trabajo	21/02/18	12/03/18
Definición de la introducción y objetivos del proyecto	21/02/18	23/02/18
Enumeración de los objetivos que se quieren alcanzar con la realización del TFM	26/02/18	28/02/18
Descripción de la metodología que se seguirá durante el desarrollo del TFM	1/03/18	5/03/18
Listado de las tareas a realizar para alcanzar los objetivos descritos	6/03/18	8/03/18
Planificación temporal de tareas y dependencias a lo largo del semestre	9/03/18	12/03/18
PEC2	13/03/18	9/04/18
Estudio de la arquitectura y organización de la red Bitcoin	13/03/18	15/03/18
Estudio de los conceptos de transacción, bloque y cadena de bloques	16/03/18	20/03/18
Comparación y exposición de las ventajas del modelo peer-to-peer y el modelo de transacción tradicional	21/03/18	23/03/18
Investigación y exposición de los diferentes blockchains (Bitcoin, Ethereum, Ripple, Litecoin)	26/03/18	2/04/18
Estudio de las aplicaciones actuales y futuribles de la tecnología blockchain	3/04/18	5/04/18
Incorporación de correcciones y sugerencias recibidas	6/04/18	9/04/18
PEC3	10/04/18	7/05/18
Estudio del funcionamiento del consenso y cómo se alcanza en la red Bitcoin	10/04/18	12/04/18
Estudio de las ventajas y desventajas de los diferentes mecanismos de consenso de blockchain	13/04/18	17/04/18
Estudio que constate las diferencias entre blockchain público y privado	18/04/18	19/04/18
Estudio y definición del concepto de Smart Contracts	20/04/18	25/04/18
Estudio de los aspectos de seguridad de Bitcoin, blockchain y Smart Contracts	26/04/18	3/05/18
Incorporación de correcciones y sugerencias recibidas	4/05/18	7/05/18
PEC4 – Memoria final	8/05/18	4/06/18
Confección de la Memoria final	8/05/18	23/05/18
Preparación de la defensa del Trabajo Fin de Máster	24/05/18	30/05/18
Incorporación de correcciones y sugerencias recibidas	31/05/18	4/06/18
PEC5 – Presentación/Video	5/06/18	11/06/18
Confección del vídeo para la presentación y exposición del trabajo	5/06/18	8/06/18
Incorporación de correcciones y sugerencias	11/06/18	11/06/18
Defensa del TFM	18/06/18	22/06/18

Ilustración 1. Planificación del trabajo. Diagrama de *Gantt*.

PEC1 - Plan de trabajo: del 21/02/2018 al 12/03/2018

- Definición de la introducción y objetivos del proyecto.
- Enumeración de los objetivos que se quieren alcanzar con la realización del TFM.
- Descripción de la metodología que se seguirá durante el desarrollo del TFM.
- Listado de las tareas a realizar para alcanzar los objetivos descritos.
- Planificación temporal de tareas y dependencias a lo largo del semestre.

PEC2: del 13/03/2018 al 09/04/2018

- Incorporación de correcciones y sugerencias recibidas.
- Estudio de la arquitectura y organización de la red *Bitcoin*.
- Estudio de los conceptos de transacción, bloque y cadena de bloques.
- Comparación y exposición de las ventajas del modelo *peer-to-peer* y el modelo de transacción tradicional.
- Investigación y exposición de los diferentes *blockchains* (*Bitcoin*, *Ethereum*, *Ripple*, *Litecoin*).
- Estudio de las aplicaciones actuales y futuribles de la tecnología *blockchain*.

PEC3: del 10/04/2018 al 07/05/2018
Incorporación de correcciones y sugerencias recibidas.

- Estudio del funcionamiento del consenso y cómo se alcanza en la red *Bitcoin*.
- Estudio de las ventajas y desventajas de los diferentes mecanismos de consenso de *blockchain*.
- Estudio que constate las diferencias entre *blockchain* público y privado.
- Estudio y definición del concepto de *Smart Contracts*.
- Estudio de los aspectos de seguridad de *Bitcoin*, *blockchain* y *Smart Contracts*.

PEC4 - Memoria final: del 08/05/2018 al 04/06/2018
Incorporación de correcciones y sugerencias recibidas.

- Confección de la Memoria final de acuerdo con las especificaciones recibidas y el documento *P08/89018/00446 Presentación de documentos y elaboración de presentaciones*, teniendo presentes los documentos *Normativa de los trabajos finales de máster de ámbito profesional* y *P08/89018/00445 Redacción de textos científico-técnicos*, además de la información de apoyo incluida en los documentos *Informe_Evaluacion_TFM_es_v3.doc* y *Criterios_Evaluación_TFM_es_v1.doc*.
- Preparación de la defensa del Trabajo Fin de Máster y recursos adicionales para su correcta exposición y resolución de imprevistos.

PEC5 - Presentación/Vídeo: del 05/06/2018 al 11/06/2018
(preparación del video)

- Incorporación de correcciones y sugerencias recibidas del resto de PEC's.
- Confección del vídeo para la presentación y exposición del trabajo de acuerdo con las especificaciones recibidas y el documento *PID_00191586 Exposición de contenidos en video*.

Defensa del TFM: del 18/06/2018 al 22/06/2018

5. Estado del arte.

Hace tiempo que se viene comentando en los medios de comunicación el auge de las criptomonedas, que en la actualidad ascienden a 1.875.
[1] Recuperado de: `https://es.investing.com/crypto/currencies`, (31/5/2018).

La criptomoneda de mayor volumen de capitalización, sin duda, es el *Bitcoin*.

La popularidad del *Bitcoin* ha traspasado fronteras y en la actualidad se pueden hacer muchos tipos de compras en tiendas físicas y virtuales, pueden comprarse servicios e incluso se pueden comprar y cambiar *Bitcoins* en determinados cajeros automáticos.

La ausencia de una autoridad centralizada, el poder hacer transacciones en muy poco tiempo que atraviesan fronteras, la capacidad de disponer de una moneda que escapa de gobiernos y reguladores centrales es parte de su fortaleza y también de su debilidad, al no estar respaldada por ningún organismo central, solamente por la cadena de bloques.
El sistema para protegerse tiene resuelto en la cadena de bloques el problema del doble gasto y otras capacidades que forman parte del atractivo de la criptomoneda.

La intencionalidad de este trabajo es exponer claramente la información relativa al *Bitcoin* y su estructura y organización, así como los mecanismos que han hecho que sea la criptomoneda más popular. También dedicaremos una parte a la cadena de bloques que lo sustenta: *Blockchain*, y lo contrastaremos con otros *blockchain* de otras criptomonedas para apreciar sus diferencias. Además, vamos a plasmar aspectos relativos a los *Smart Contracts*.

El *Bitcoin* es una criptomoneda que ha llegado para quedarse y sus datos así lo avalan.
A día de hoy cuenta con una capitalización de mercado de `126.031.396.405 USD`, con `17.064.950 monedas` en circulación y un volumen de cambio diario en las principales casas de cambio de `339.813.351 USD`.
Blockchain, también llamada la cadena de bloques, sustenta la tecnología con unos datos imparables. A día de hoy el tiempo medio de confirmación de la transacción se ha reducido a `5,883 minutos` y el número de transacciones diarias confirmadas es de `204.769`.
El tamaño de la cadena de bloques es de `169.365 MB`. y el número de transacciones por bloque es de `1.173`.
[2] Datos recuperados de `blockchain.info`, (31/5/2018).

6. Estudio de la arquitectura y organización de la red *Bitcoin*.

Para disponer de una aproximación rápida al *Bitcoin*, consultamos en sus *Frequently Asked Questions* las cuatro preguntas necesarias para comprender el inicio de esta tecnología.

¿Qué es *Bitcoin*?
Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, *Bitcoin* es como dinero para Internet. *Bitcoin* puede ser el único sistema de contabilidad triple existente.

¿Quién creó *Bitcoin*?
Bitcoin es la primera implementación de un concepto conocido como moneda criptográfica, la cual fue descrita por primera vez en 1998 por *Wei Dai* en la lista de correo electrónico *cypherpunks*, donde propuso la idea de un nuevo tipo de dinero que utilizara la criptografía para controlar su creación y las transacciones, en lugar de que lo hiciera una autoridad centralizada.
La primera especificación del protocolo *Bitcoin* y la prueba del concepto la publicó *Satoshi Nakamoto* en el 2009 en una lista de correo electrónico. *Satoshi* abandonó el proyecto a finales de 2010 sin revelar mucho sobre su persona. Desde entonces, la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en el protocolo *Bitcoin*.

La anonimidad de *Satoshi* a veces ha levantado sospechas injustificadas, muchas de ellas causadas por la falta de comprensión sobre el código abierto en el que se basa *Bitcoin*. El protocolo *Bitcoin* y su *software* se publican abiertamente y cualquier programador en cualquier lugar del mundo puede revisarlo o crear su propia versión modificada del *software*.
Al igual que los programadores actuales, la influencia de *Satoshi* se ha limitado a que los cambios que hizo los adoptaran los demás y, por tanto, no controlaba *Bitcoin*. Así, conocer la identidad del inventor del *Bitcoin* es igual de relevante que saber quién inventó el papel.

¿Quién controla la red *Bitcoin*?
De la misma manera que nadie controla la tecnología detrás del correo electrónico, *Bitcoin* tampoco tiene propietarios. *Bitcoin* lo controlan todos los usuarios de *Bitcoin* del mundo. Aunque los programadores mejoran el software, no pueden forzar un cambio en el protocolo de *Bitcoin* porque todos los demás usuarios son libres de elegir el *software* y la versión que quieran. Para que sigan siendo compatibles entre sí, todos los usuarios necesitan utilizar *software* que cumpla con las mismas reglas. *Bitcoin* sólo puede funcionar correctamente si hay consenso entre todos los usuarios. Por lo tanto, todos los usuarios y programadores tienen un gran aliciente en proteger dicho consenso.

¿Cómo funciona *Bitcoin*?
Desde la perspectiva del usuario, *Bitcoin* no es más que una aplicación móvil o de escritorio que provee un monedero *Bitcoin* personal y permite al usuario enviar y recibir *Bitcoins* con él. Así es como funciona *Bitcoin* para la mayoría de los usuarios.

Detrás de las cámaras, la red *Bitcoin* comparte una contabilidad pública llamada *block chain*. Esta contabilidad contiene cada transacción procesada, permitiendo verificar la validez de cada transacción. La autenticidad de cada transacción está protegida por firmas digitales correspondientes a las direcciones de envío, permitiendo a todos los usuarios tener control total al enviar *Bitcoins* desde sus direcciones *Bitcoin*. Además, cualquiera puede procesar una transacción usando el poder computacional de *hardware* especializado y conseguir una recompensa en *Bitcoins* por este servicio. Esto es comúnmente llamado *mining* o minería.

[3] *Bitcoin*. *Preguntas más frecuentes*.
© Bitcoin Project 2009-2018 Publicado bajo la licencia *MIT*
Recuperado de: `https://bitcoin.org/es/faq` (31/05/2018)

En el inicio su creador *Satoshi Nakamoto* envió un *paper* llamado *Bitcoin: A Peer-to-Peer Electronic Cash System* a la lista de correo de criptografía en *Metzdowd* que se puede leer en el siguiente enlace, explicando el germen de esta tecnología.

[4] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System.*
Recuperado de: `https://bitcoin.org/bitcoin.pdf` (31/05/2018)

El correo electrónico original se puede leer en el siguiente enlace, en *The Mail Archive*.

Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to anothe without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes contr the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basi and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to [EMAIL PROTEC

[5] Recuperado de: `https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html` (31/05/2018)

Ilustración 2. *Satoshi Nakamoto*, correo electrónico original.

Como hemos comentado la arquitectura de red trabaja sobre topología de malla descentralizada, compuesta por nodos *peer to peer* (*P2P*). Esto dota de gran autonomía a la red que puede operar independientemente del fallo o los ataques que puedan sufrir algunos nodos.

Servidores y clientes disponen de mecanismos para el descubrimiento de nodos en la red a través de intercambio de listas. Las conexiones de los diferentes nodos gestionan su optimización para mejorar el rendimiento de la red.

Conceptos.

Bitcoin.
Se refiere a la tecnología.

bitcoin.
Se refiere a la criptomoneda.

Un *bitcoin* es simplemente un saldo en una cuenta en *bitcoins* mas allá de un propio *token* criptográfico y este saldo está en una cuenta en *bitcoins*, creada por el usuario con una clave privada y una pública.

Los *bitcoins* funcionan con criptografía de curvas elípticas.

En una criptografía de clave pública, de curvas elípticas, todo el mundo tiene una clave pública y una privada y lo que hace la clave privada lo deshace la pública y viceversa.

[6] Transcrito de:
Herrera, Jordi. *Congrés de Seguretat informàtica UOC-CON*. 15/5/2017.
WannaCry: un mal ejemplo de gestión de pagos con *bitcoins.*
Bitcoin and ransomware: la caída de *Wannacry*
Recuperado de: https://www.youtube.com/watch?v=ixdhXQhYx4A (31/05/2018).

Dirección *Bitcoin*.

Es la dirección virtual de un usuario que contiene monedas *Bitcoin* y se utiliza para pagar y recibir pagos, similar a una cuenta de banco.
Un mismo usuario puede tener tantas direcciones *Bitcoin* como necesite y se identifican con una clave pública.
Una dirección *Bitcoin* es, básicamente, una transcripción de una clave pública.
La clave privada asociada sirve para firmar las transacciones y la clave pública sirve para identificar la dirección y validar las firmas.

[7] *INCIBE. Bitcoin: Una moneda criptográfica.* (página 17, Direcciones *Bitcoin*, Monederos).
Recuperado de:
`https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf` (31/05/2018)

La clave privada es aquel elemento que solo conoces tú y lo que haces con ella es una firma digital y permitir que una transacción sea correcta.

Un punto muy importante es que con las criptomonedas las claves se vuelven dinero. Es decir, tu clave privada es directamente dinero.

[8] Transcrito de:
Herrera, Jordi. *Congrés de Seguretat informàtica UOC-CON*. 15/5/2017.
WannaCry: un mal ejemplo de gestión de pagos con *bitcoins.*
Bitcoin and ransomware: la caída de *Wannacry*
Recuperado de: https://www.youtube.com/watch?v=ixdhXQhYx4A (31/05/2018).

Monedero (*Wallet*).

Espacio virtual, equivalente a un monedero físico, donde se almacenan y gestionan direcciones *Bitcoin* de un usuario y los pagos que se realizan con ellas.

[9] *INCIBE. Bitcoin: Una moneda criptográfica.* (página 17, Direcciones *Bitcoin*, Monederos). Recuperado de: `https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf` (31/05/2018)

Minero.

Son usuarios que dedican potencia de cómputo procesar nuevas transacciones. La minería de *Bitcoin* ofrece una recompensa a cambio de servicios útiles que son necesarios para que la red de pagos funcione de manera segura. Es bastante habitual que los mineros se agrupen en *pools* para sumar capacidad de cálculo y acceder más fácilmente a la solución de los retos.

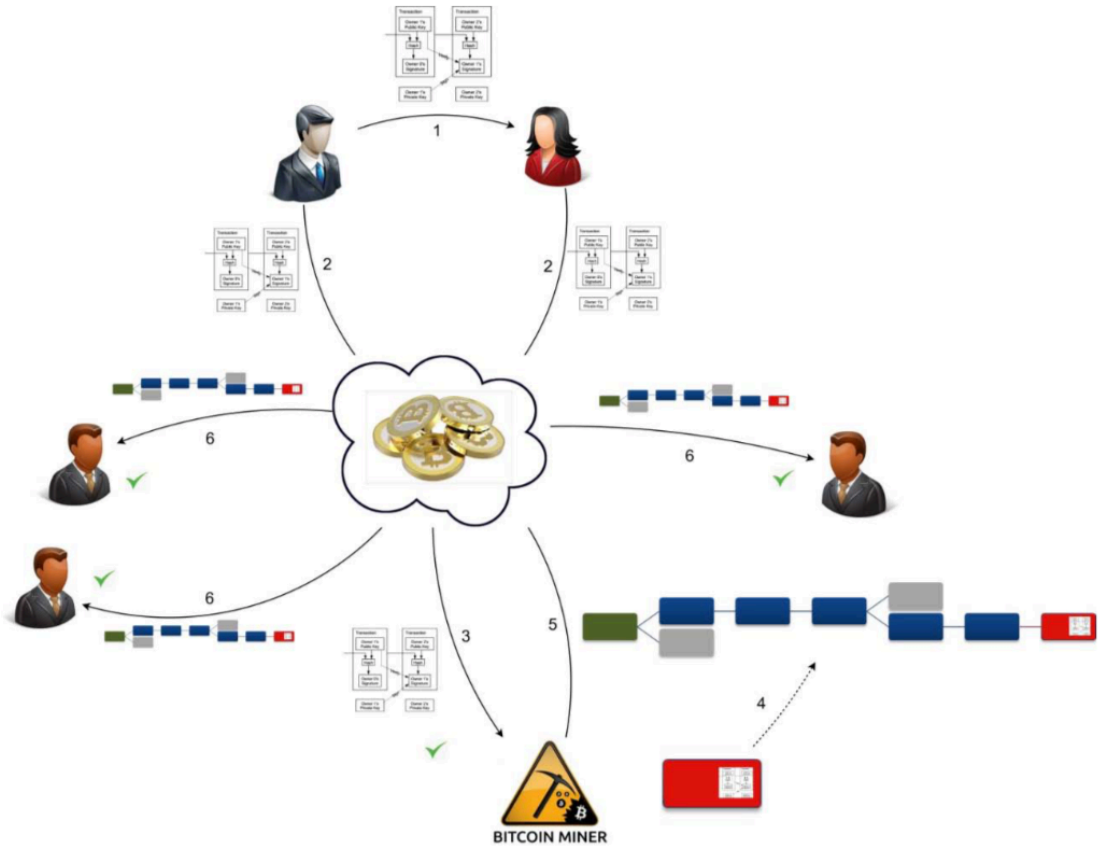
[10] Elaborado de:
Bitcoin. Preguntas más frecuentes.
© *Bitcoin Project 2009-2018* Publicado bajo la licencia MIT
Recuperado de: `https://bitcoin.org/es/faq` (31/05/2018)

Minería.

La minería es un sistema de consenso distribuido que se utiliza para confirmar las transacciones pendientes a ser incluidas en la cadena de bloques. Hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un acuerdo entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones, deberán ser empacadas en un bloque que se ajuste a estrictas normas de cifrado y que será verificado por la red. Estas normas impiden que cualquier bloque anterior se modifique, ya que hacerlo invalidaría todos los bloques siguientes. La minería también crea el equivalente a una lotería competitiva que impide que cualquier persona pueda fácilmente añadir nuevos bloques consecutivamente en la cadena de bloques. De esta manera, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para revertir sus propios gastos.

[11] Elaborado de:
Bitcoin. ¿Cómo funciona *Bitcoin*?.
© *Bitcoin Project 2009-2018* Publicado bajo la licencia *MIT*.
Recuperado de: `https://bitcoin.org/es/como-funciona` (31/05/2018)

Funcionamiento genérico de *Bitcoin*.



1. *Bob hace un pago en bitcoins a Alice.*
2. *Alice y Bob envían la transacción a la red P2P de Bitcoin.*
3. *Un minero recibe la nueva transacción y la verifica.*
4. *El minero crea un conjunto de transacciones nuevas, incluyendo la transacción del paso 1, y trabaja para confirmarla.*
5. *El minero envía el nuevo bloque de transacciones confirmadas a la red P2P de Bitcoin.*
6. *El resto de usuarios de Bitcoin actualizan su estado incluyendo el nuevo bloque de transacciones, verificando que dicho bloque es válido.*

Ilustración 3. Funcionamiento genérico de *Bitcoin*.
[12] INCIBE. *Bitcoin: Una moneda criptográfica.* (página 18).
Recuperado de:
`https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf` (31/05/2018)

Enrutamiento.
Es la funcionalidad básica de cualquier cliente.
Con ella se integra en la red y participa de las conexiones, pudiendo operar determinados tipos de transacciones.

Transacciones, bloques, cadena de bloques (*blockchain*).
Conceptos objeto de estudio en el siguiente apartado de este trabajo.

7. Estudio de los conceptos de transacción, bloque y cadena de bloques.

Transacción.

Una transacción es una sección de datos con firma digital que se transmite a la red y se almacena en los bloques. Este conjunto de datos incluye una referencia a una transacción anterior e indica una cantidad de *bitcoins* que pasan a estar disponibles para una dirección *Bitcoin* de destino.
Al igual que el resto de datos que se almacenan en la cadena de bloques, la información no está cifrada.
Un explorador de la cadena de bloques es un sitio *web* en el que se pueden visualizar todas las transacciones incluidas en los bloques. Esto resulta muy útil para ver los detalles técnicos de la transacción y para poder verificar los pagos.

[13] *bitcoin* wiki. *Transacción*.
Recuperado de: `https://es.bitcoin.it/wiki/Transacción` (31/05/2018).

Una transacción, dicho de otra forma, es una transferencia de dinero de una dirección *Bitcoin A* hacia otra dirección *B*. Para componer una transacción, el propietario de la dirección *A* firma una transcripción de la dirección *B* (entre otros datos) con la clave privada asociada a la dirección *A*, de forma que la red sabrá que el nuevo propietario legítimo es el dueño de la dirección *B*.

[14] Adaptado de:
INCIBE. Bitcoin: Una moneda criptográfica. (página 17, Transacciones).
Recuperado de:
`https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf` (31/05/2018).

Las transacciones de *Bitcoin* están aseguradas mediante criptografía militar. Nadie puede cobrarle dinero o hacer un pago en su nombre. Tan pronto como tome los pasos requeridos para proteger su monedero, *Bitcoin* podrá darle control sobre su dinero y un fuerte nivel de protección contra muchos tipos de fraude.

[15] *Bitcoin. bitcoin para personas.*
© *Bitcoin Project* 2009-2018 Publicado bajo la licencia *MIT*
Recuperado de: `https://bitcoin.org/es/bitcoin-para-personas` (31/05/2018).

¿Porqué tengo que esperar 10 minutos?

La recepción de un pago es casi instantánea con *Bitcoin*. Sin embargo, hay un retraso de 10 minutos de media antes de que la red empiece a confirmar esa transacción al incluirla en un bloque y antes de que se puedan gastar los *bitcoins* recibidos. Una confirmación significa que hay un consenso en la red en que los *bitcoins* recibidos no han sido enviados a alguien más y son ahora de tu propiedad. Una vez que tu transacción ha sido incluida en un bloque, esta irá siendo enterrada con más confirmaciones por los siguientes bloques que van añadiéndose a la cadena, lo que hará consolidarse este consenso y disminuir el riesgo de una revocar la transacción. Cada usuario es libre de determinar en qué punto se puede considerar una transacción como confirmada, pero normalmente 6 confirmaciones es considerado tan seguro como esperar 6 meses tras un pago con tarjeta de crédito.

¿Cuánto costará la comisión por una transacción?

La mayoría de las transacciones se pueden ejecutar sin comisiones, pero se anima a los usuarios a pagar una pequeña comisión voluntaria para obtener confirmaciones más rápidas y para remunerar a los mineros. Cuando las tasas son obligadas, generalmente no superan unos pocos céntimos. Tu cliente *Bitcoin* normalmente intentará estimar una comisión adecuada siempre que esta sea requerida.

Las comisiones se usan como protección frente a usuarios que intenten enviar gran número de transacciones con la intención de sobrecargar la red.
La manera exacta en que funcionan las comisiones todavía está desarrollándose y evolucionará con el tiempo.
Como el importe de la comisión no está relacionada a la cantidad de *bitcoins* que se envían, puede ser extremadamente baja (0.0005 BTC para una transferencia de 1000 BTC) o injustamente alta (0.004 BTC para un pago de 0.02 BTC).
La comisión se calcula en relación a propiedades como la cantidad de datos en la transacción y su recurrencia. Por ejemplo, si estás recibiendo un gran número de cantidades pequeñas, las comisiones por envíos serán más altas. Este tipo de pagos se pueden comparar con pagar en un restaurante usando solo céntimos. Gastar pequeñas fracciones de tus *bitcoins* de forma rápida también requerirá una comisión. Si tus actividades siguen el patrón habitual de transacciones normales, las comisiones deberían ser muy bajas.

[16] Elaborado de:
Bitcoin. Preguntas más frecuentes.
© *Bitcoin Project* 2009-2018 Publicado bajo la licencia *MIT*
Recuperado de: `https://bitcoin.org/es/faq` (31/05/2018).

Bloque.

Un bloque es un registro que contiene confirmaciones de transacciones que se encontraban pendientes.
Aproximadamente cada 10 minutos, en promedio, un nuevo bloque que incluye nuevas transacciones se anexa a la cadena de bloques a través de la minería.

Campo	Descripción
Magic no	Valor establecido siempre a 0xD9B4BEF9
Blocksize	Número de bytes que siguen, hasta el final del bloque
Blockheader	Cabecera con metainformación sobre el bloque y la cadena
Transaction counter	Número de transacciones en la siguiente lista
Transactions	Lista de transacciones contenidas en el bloque

Tabla 2. Campos de un bloque.
[17] INCIBE. *Bitcoin: Una moneda criptográfica.* (página 25).
Recuperado de:
`https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf` (31/05/2018).

De los campos anteriores, destaca en primer lugar la lista de transacciones que incluye las transacciones nuevas que el minero que ha calculado el bloque ha decidido incluir en el mismo. Qué transacciones se incluyen depende

principalmente de su prioridad. Dentro de la cabecera se incluyen los campos mostrados en la Tabla 3.

Campo	Descripción
Version	Versión de bloque
hashPrevBlock	Hash del bloque anterior
hashMerkleRoot	Hash de la raíz del árbol Merkle
Time	Marca de tiempo de creación del bloque
Bits	Especificiación de la complejidad del bloque
Nonce	Nonce que resuelve la prueba de trabajo

Tabla 3. Cabecera de bloque.
[18] Adaptado de: *INCIBE. Bitcoin: Una moneda criptográfica.* (página 25).
Recuperado de:
https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf (31/05/2018).

Cadena de bloques.

Una cadena de bloques es un registro inmutable de transacciones a las cuales solo puedes añadir transacciones y que estas transacciones quedan ordenadas desde el punto de vista secuencial.
...
Es decir, es un sistema para prevenir el doble gasto en criptomonedas.
...
El concepto de *blockchain* se estableció con *los bitcoins*, por lo tanto, estos crearon la *blockchain*.

[19] Transcrito de:
Herrera, Jordi. *Congrés de Seguretat informàtica UOC-CON*. 15/5/2017.
WannaCry: un mal ejemplo de gestión de pagos con *bitcoins.*
Bitcoin and ransomware: la caída de *Wannacry*
Recuperado de: https://www.youtube.com/watch?v=ixdhXQhYx4A (31/05/2018).

La cadena de bloques o *block chain* es una contabilidad pública compartida en la que se basa toda la red *Bitcoin*. Todas las transacciones confirmadas se incluyen en la cadena de bloques. De esta manera los monederos *Bitcoin* pueden calcular su saldo gastable y las nuevas transacciones pueden ser verificadas, asegurando que el cobro se está haciendo al que realiza el pago. La integridad y el orden cronológico de la cadena de bloques se hacen cumplir con criptografía.

[20] Elaborado de:
Bitcoin. ¿Cómo funciona *Bitcoin*?.
© *Bitcoin Project 2009-2018* Publicado bajo la licencia MIT
Recuperado de: https://bitcoin.org/es/como-funciona (31/05/2018).

El primer registro se hizo el 3 de enero de 2009, a partir de aquí en orden cronológico cuando un nodo de la red consigue crear un nuevo bloque, éste lo transmite al resto de nodos, los cuales verifican que el bloque es correcto, en caso que se confirme, se añade a la cadena y se difunde, se asegura la seguridad porque todas las transacciones son públicas y difícil de falsificar, automatizado por algoritmos matemáticos en la cual la comunidad puede hacer de 'notarios' que certifican el documento.

Un usuario no puede reutilizar monedas que ya usó, puesto que la red rechazará la transacción porque las transacciones se hacen públicas, imposibilitando una reutilización, de hecho, en la página de *Blockchain* se

puede observar casos de reutilización de monedas que se han detectado y bloqueado.

El *blockchain* es creado por el minero y mantenido por el resto de usuarios, el minero envía un bloque de transacciones confirmadas a la red *peer to peer* (*P2P*) de *Bitcoin*, el resto de usuarios actualizan su estado incluyendo el nuevo bloque de transacciones verificando que dicho bloque es válido.

Construcción de la cadena.

Cada vez que se hace una transferencia de una dirección *bitcoin* a otra, el propietario de la dirección origen firma una transcripción de la dirección destino, esto crea una estructura que contiene tanto claves como otros datos, los cuales están pendientes de confirmar. Estos datos se agrupan en bloques y sobre cada bloque se aplica la minería. Una vez validados y confirmados los bloques pasan a formar parte de la cadena denominada *blockchain*.

Como hemos visto anteriormente el tiempo medio de generación de un bloque es de 10 minutos. Por defecto cada cliente debería esperar 6 bloques, es decir, hasta que no se hayan validado 6 bloques desde que se comenzó la transacción, porque de lo contrario no se considera realmente efectuado el pago. Por otro lado, la red trata de crear 6 bloques por hora, y cada 2016 bloques (Aprox. dos semanas), todos los clientes comparan el número real creado con este objetivo y modifican el porcentaje que ha variado, lo cual aumenta (o disminuye) la dificultad de generación de bloques.

[21] Medina Reyes, María Fernanda. (2016) *Análisis y comparación de monedas criptográficas basadas en la tecnología Blockchain* (páginas 10 y 11).
Barcelona: Editorial Universitat Oberta de Catalunya. Reconocimiento-NoComercial- SinObraDerivada 3.0 España de Creative Commons
Recuperado de: `http://openaccess.uoc.edu/webapps/o2/handle/10609/56344` (31/05/2018).

8. Comparación y exposición de las ventajas del modelo *peer-to-peer* y el modelo de transacción tradicional.

Como aspectos relevantes, las principales diferencias y a la vez ventajas del modelo *peer-to-peer* contra el modelo de transacción tradicional son: el carácter irreversible de las transacciones y el nivel de privacidad de los usuarios y las operaciones que realizan.

Irreversibilidad de las transacciones.

En el modelo *peer-to-peer* (*P2P*) de *Bitcoin* se asume que cuando una transacción se asienta en el bloque es legítima. Una vez asentado, no existe riesgo de que la moneda recibida sea falsa o se destine a otra transacción, porque la cadena de bloques dispone de mecanismos para evitar el problema del doble gasto.

El riesgo de fraude, de hecho, es menor al riesgo de fraude con cualquier otra forma de dinero fiduciario.

El uso del modelo *peer-to-peer* (*P2P*) mejora la fiabilidad del modelo de transacción tradicional.

Privacidad.

El modelo tradicional logra su nivel de privacidad al limitar el acceso a la información a las partes involucradas y a la tercera parte confiable.

En el modelo *peer-to-peer* (*P2P*) la necesidad de anunciar todas las transacciones públicamente se opone a este método, pero la privacidad aún se puede mantener rompiendo el flujo de información manteniendo anónimas las claves públicas.

Cualquier usuario puede ver que alguien está enviando una cierta cantidad a otra persona, pero sin información que relacione la transacción con nadie en particular.
Esto es similar al nivel de información que se muestra en las bolsas de valores, donde el tiempo y el tamaño de las transacciones individuales (la “cinta”), son públicos, pero sin decir quiénes son las partes.

Esto explica por qué *Bitcoin* se ha utilizado para llevar a cabo transacciones ilegales ya que, a pesar del acceso público y libre al libro mayor, la identidad y privacidad de sus usuarios está garantizada si así se requiere.
No obstante, son inevitables algunos tipos de asociación con transacciones de múltiples entradas, las que pueden revelar que sus entradas pertenecen al mismo dueño. El riesgo estaría en que, si el dueño de una clave se revela, entonces el enlazado podría revelar otras transacciones que pertenecieron al mismo dueño.

[22] Elaborado sobre una idea de:
Acuña, Héctor. (noviembre 2017). *Estudio sobre Bitcoin y Tecnología Blockchain.*
Cuadernos CEF - ESE Business School.
Recuperado de: `http://www.ese.cl/wp-content/blogs.dir/1/files_mf/1510073019CUADERNOS_CEF_1_EstudiosobreBitcoinytecnolog%C3%ADaBlockchainv2003.pdf` (31/05/2018)

9. Investigación y exposición de los diferentes *blockchains* (*Bitcoin*, *Ethereum*, *Ripple*, *Litecoin*).

Blockchain.

Una *blockchain* es un libro de contabilidad digital que se distribuye entre varias ubicaciones para garantizar la seguridad y facilidad de acceso a nivel mundial, permitiendo a consumidores y proveedores conectarse directamente, eliminando la necesidad de un tercero.

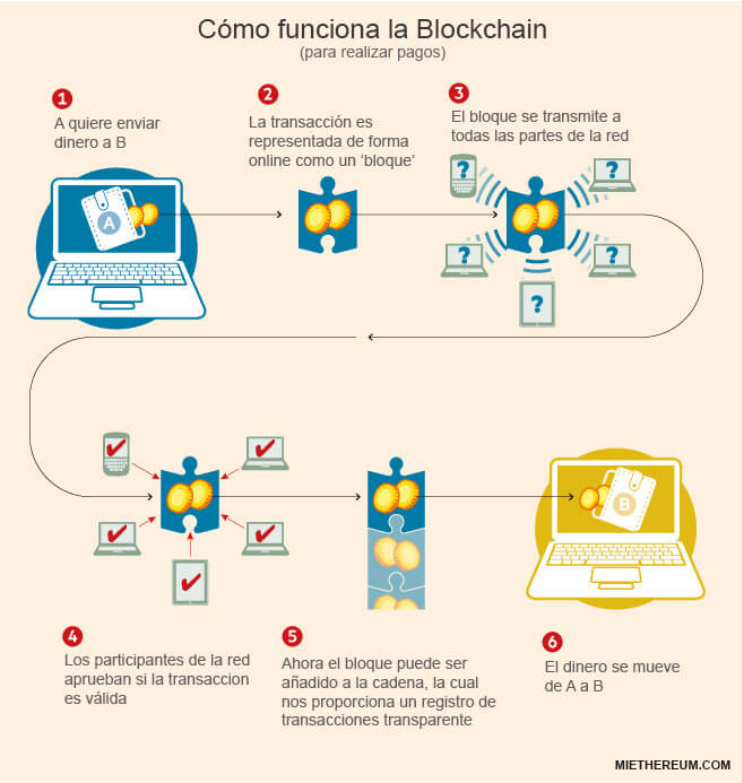


Ilustración 4. Cómo funciona la Blockchain (para hacer pagos).
[23] Recuperado de: `https://miethereum.com/blockchain/#toc3` (31/05/2018)

Propiedades de *blockchain*.

Replicación *P2P* (*peer-to-peer*).

Cada usuario que forme parte de la plataforma tendrá una copia íntegra y actualizada de toda la *blockchain*, y según se vaya añadiendo información a la misma, también se irá sincronizando en el resto de ordenadores de los participantes.

Descentralización.

Las cadenas de bloques están políticamente descentralizadas (no hay nadie que las controle) y arquitectónicamente descentralizadas (no hay punto central de fallo de infraestructura) pero están lógicamente centralizadas (hay un estado comúnmente acordado y el sistema se comporta como una sola computadora).

`Vitalik Buterin, creador de Ethereum`

Irreversibilidad e inmutabilidad.
Una vez que se ha grabado un dato o se ha realizado una transacción en la cadena de bloques, es imposible de eliminar, o mejor dicho, es extremadamente fácil darse cuenta de que alguien intenta modificar alguna información.

Criptografía y seguridad.
En la cadena de bloques, la red puede verificar que una transacción fue enviada por la persona que posee la clave privada sin que esta revele su identidad.

Carácter público.
El carácter público de la cadena de bloques hace que las transacciones y las validaciones de bloques puedan ser vistas por todos y cada uno de los participantes de la red.

Privacidad y transparencia.
La cadena de bloques proporciona verificabilidad pública de su estado general sin filtrar información sobre el estado de cada participante individual.

Integridad.
En la cadena de bloques, para poder “hacer trampas” al resto de la red, se necesitaría que el resto de la red aceptase esas trampas.

Cronología.
En la cadena de bloques, cada bloque tiene una marca de tiempo que dota a todas las transacciones de ese bloque con ese registro temporal.

Rapidez a bajo coste.
La *blockchain* hace posible que las transacciones se realicen de forma más rápida que a través de una entidad central. Al poder realizar más transacciones, en menos tiempo y directamente entre las partes interesadas, sin intermediarios, se agiliza todo el proceso.

[24] Elaborado sobre una idea de:
`https://miethereum.com/blockchain/#toc3` (31/05/2018)

Respecto a las particularidades de la *blockchain* de *Ethereum*.
Ethereum es una plataforma *blockchain* donde se realizan transacciones de cualquier cosa, permite transaccionar cualquier cosa que sea programable.

Los contratos inteligentes son aplicaciones que operan como programas informáticos y se ejecutan a través de *blockchain*, de forma descentralizada. La plataforma de *Ethereum* es una red de dispositivos/ordenadores a nivel mundial que desarrollan estos contratos inteligentes bajo unas inmutables reglas de consenso compartido.

Un *Smart Contract* es un código *software* que se ejecutará por sí mismo bajo ciertas circunstancias acordadas entre las partes de antemano. Normalmente incluyen una transacción financiera. Por ejemplo, si el valor del petróleo baja

hasta un precio fijado se invierte una cantidad de dinero en una determinada acción.

Los contratos inteligentes aportaran en un futuro servicios financieros sin necesidad de intermediarios. Tienen un sinfín de posibilidades: sistemas de votación online, seguros, etc.

El lenguaje de programación de la plataforma es el "*Turing* completo", en él puede programarse contratos para cualquier tipo de transacción o aplicación. En resumen, *Ethereum* utiliza *Blockchain* para convertirse en una plataforma informática mundial descentralizada capaz de crear contratos inteligentes.

[25] Elaborado de: https://nuevofinanciero.com/ethereum-blockchain-ether-bitcoin/ (31/05/2018)

Respecto a las particularidades de la *blockchain* de *Ripple*.

Ripple sostiene una *blockchain* empresarial que soporta casos de pagos transfronterizos, y el sistema está diseñado especialmente para bancos y proveedores de pagos de todo el mundo que necesiten una liquidez más eficiente y un mayor acceso a los mercados emergentes.

[26] Recuperado de: https://www.criptonoticias.com/aplicaciones/blockchain-privada-ripple-encamina-descentralizacion/ (31/05/2018)

Respecto a las particularidades de la *blockchain* de *Litecoin*.

El tiempo de generación de bloques es de 2 minutos y 30 segundos en lugar de 10 minutos en promedio. El número de criptomonedas a emitir hasta 84 millones de unidades sin necesidad de reducir a la mitad la recompensa cada cierto tiempo, como sí ocurre en el caso de *Bitcoin*. Utiliza el algoritmo *hash scrypt* en su método de prueba de trabajo, en lugar de *SHA-256*. Dicha función criptográfica exige mayor capacidad de almacenamiento y memoria para proteger al *hardware* de minería de ataques, por lo que este *hardware* es más complejo de fabricar en comparación con los *ASIC* de *Bitcoin*.

[27] Recuperado de: https://www.criptonoticias.com/informacion/blockchains-criptomonedas-fundamentos-caracteristicas/ (31/05/2018)

	Bitcoin	*Ethereum*	*Ripple*	*Litecoin*
Descripción	Primera criptomoneda. Descentralizada, transacciones *p2p*. Sin autoridad central.	Permite que las aplicaciones descentralizadas (*DApps*) se construyan en la capa superior. Tiene una máquina virtual completa de *Turing* en la que se ejecutan *DApps*. Permite la ejecución de contratos inteligentes. Utiliza el protocolo *GHOST* para resolver conflictos que surgen cuando hay tiempos de transacción más rápidos.	No hay mineros; Los 100 mil millones de monedas de *XRP* que existen se crearon cuando la red se lanzó en 2012. Basado en un algoritmo de consenso único.	Moneda electrónica alternativa a *Bitcoin*. Procesa un bloque cada 2,5 minutos. Producirá 84 millones de *Litecoins*. Utiliza la función *scrypt*.
Creación	enero de 2009	julio de 2015	2012	octubre de 2011
Permisos y desarrollo	Pública. *Open source*.	Pública. *Open source*.	Semi - pública. *Open source*.	Pública. *Open source*.
Aplicaciones	Criptomoneda.	*DAPP's*.	Ayudar a liquidar pagos transfronterizos más rápido y más barato.	Confirmación más rápida de transacciones y facilidad de minería.
Algoritmo de consenso	Prueba de trabajo	Prueba de trabajo	*Ripple Protocol Consensus Algorithm* (*RPCA*) basado en un sistema de votación donde los votos de los nodos en la lista de nodos únicos de cada nodo (validadores de confianza) se toma en consideración para que un nodo decida el siguiente bloque en el *blockchain*.	Prueba de trabajo

Tabla 4. Comparativa de *blockchains*.
[28] Elaboración propia sobre una idea de: `https://www.xoken.org/blog/features-of-various-blockchains-a-comparison/` (31/05/2018).

10. Estudio del funcionamiento del consenso y cómo se alcanza en la red *Bitcoin*.

Un algoritmo de prueba de trabajo, (del inglés *Proof-Of-Work*), es un protocolo de consenso distribuido para redes distribuidas. Los sistemas que los usan, como *Bitcoin*, son sistemas de prueba de trabajo.

Hashcash fue el primer sistema de prueba de trabajo. La idea fundamental es que los nodos no confiables que intervienen en un sistema deben aportar una prueba de su interés en el sistema. Para ello tienen que demostrar que han dedicado cierta cantidad de recursos (prueba de trabajo). Además, el coste de la verificación de dicha prueba tiene que ser reducida.

Bitcoin es la primera implementación ampliamente usada de un sistema de dinero electrónico *peer-to-peer* que no requiere tener confianza en los pares. Se reemplaza la firma del servidor central con un mecanismo de firma consensuada, realizada por nodos no confiables a los que se llama mineros, basada en pruebas de trabajo donde los firmantes son incentivados para que actúen cooperativamente y de forma honesta.

La remuneración a los firmantes hace que a priori estén dispuestos a tener un comportamiento honesto para conseguir el consenso. Como la contribución a la firma está ponderada por el poder computacional, si un grupo de firmantes tiene alguna motivación para ser deshonestos, tiene que competir computacionalmente con el resto de firmantes que siguen siendo honestos. Por eso cuantos más firmantes haya más difícil será que un grupo deshonesto tenga cierto éxito. Por esta razón se dice que es una solución al Problema de los generales bizantinos.

[29] Adaptado y recuperado de: `https://es.wikipedia.org/wiki/Prueba_de_trabajo_(algoritmo_de_consenso_distribuido)` (31/05/2018).

La prueba de trabajo es un método para establecer un consenso entre un número de personas interesadas, ninguna de las cuales está subordinada a otra, y existen incentivos considerables para resistirse a dicho consenso.

Antes de que un bloque nuevo sea generado, puede que haya muchos pagos pululando por la red sin existir respuesta objetiva acerca de qué pagos deberían ser validados. Algunos podrían ser inválidos, así que todos deben ser comprobados. Algunos pueden no incluir una tasa de transacción, así que debe decidirse si dejar estas anotaciones pasar, o si ignorarlos. Finalmente, podría haber un conjunto de 2 o más pagos que no pueden ser válidos simultáneamente. Por ejemplo, si alguien intenta gastar los mismos *bitcoins* en dos transacciones que aún no han sido confirmadas, habría que tomar una decisión sobre qué pago permitir.

De este modo, para un conjunto de pagos dado, pueden existir muchos bloques posibles que pueden construirse con ellos, ninguno de los cuales es objetivamente el más correcto. Tampoco habrá necesariamente un acuerdo acerca de qué resultado es preferible, porque los distintos bloques posibles benefician a distintas personas. Primeramente, está el beneficio que surge de generar un bloque en forma de nuevos *bitcoins*. Esto es necesario porque, si no existiera, habría muy poco incentivo para hacer la contabilidad para empezar. Con esta recompensa, cada minero naturalmente prefiere que el nuevo bloque sea su propuesta, y no la de cualquier otro.

Para evitar que se hagan manipulaciones interesadas, *Bitcoin* añade requerimientos extra al protocolo que incrementan enormemente el coste de la deserción. Los bloques se generan aleatoriamente mediante un cálculo muy difícil, que requiere muchos recursos computacionales, y sólo se propone un único bloque a la vez. Es anunciado y verificado por la mayoría de otros nodos (lo cual es fácil verificando los *hashes*). Cuando un bloque ha sido propuesto, los mineros tienen la opción de continuar buscando un bloque alternativo que les sea más favorable, o aceptar la propuesta (dar por verificado) y luego pasar a buscar el siguiente. Alguien que acepta el último bloque propuesto entiende que está siguiendo un proceso de consenso natural y que, si tiene la suerte de generar el siguiente bloque, será probablemente aceptado por las mismas razones que él aceptó el anterior. Por el otro lado, la opción de esperar e intentar encontrar un bloque más favorable para él es muy arriesgada, porque entonces tendría que convencer a un número suficiente de mineros de que podrá establecer un nuevo consenso, para que le sigan.

[30] Preukschat, Alexander, (2017) *Blockchain: la revolución industrial de internet*. Gestión 2000.
Recuperado de: `http://libroblockchain.com/consenso/` (31/05/2018).

Reglas de consenso.

Las reglas de consenso establecen la cantidad de *bitcoins* incluidos en la recompensa minera (*coinbase*), la dificultad de minado, el tipo de prueba de trabajo (*proof-of-work*) requerido, y, también, el límite del tamaño de los bloques.

Determinan qué bloques son considerados válidos por todos los nodos completos. Si todos los nodos completos aplican las mismas reglas de consenso, se asegura que todos ellos mantienen una copia idéntica de la cadena de bloques (*blockchain*).

Si los diferentes nodos aplican diferentes reglas de consenso, se corre el riesgo de que unos acepten unos bloques y otros los rechacen, lo que implicaría que los nodos de la red mantienen versiones completamente incompatibles de la cadena de bloques (*blockchain*), lo que supondría que la red *Bitcoin* quedaría dividida.

Las reglas del consenso de *Bitcoin* se pueden modificar de dos maneras:

1) A través de un cambio que añade reglas adicionales al protocolo (haciendo que los bloques actuales sean inválidos). Es lo que se conoce como *soft fork* o bifurcación blanda. Se requerirá súper mayoría del 95 por ciento de la potencia de *hash* para ponerse de acuerdo en los *soft forks*.

2) A través de un cambio que elimina las reglas del protocolo (haciendo que los bloques que antes no eran válidos, sí lo sean ahora). Es lo que se conoce como *hard fork* o bifurcación dura. Un *hard fork* requiere que todos los nodos completos de la red actualicen el software.

[31] Elaborado de: `https://www.oroyfinanzas.com/2016/03/4-capas-red-bitcoin-por-que-importante-consenso-cambios/` (31/05/2018).

Funcionamiento.

Bitcoin en el fondo no es más que un registro inmutable con la historia de todos los *tokens* desde su creación inicial.

En vez de usuarios con una identidad física el sistema utilizaría claves digitales, claves asimétricas (pública y privada) creadas por los propios

usuarios. Las claves son las que luego permiten hacer transacciones mediante un sencillo sistema de firma electrónica. Como el historial de todas las transacciones es público se facilita que cualquiera pueda verificar tanto el origen válido de cada *token* como el cumplimiento de las normas.

En una cadena de bloques basada en pruebas de trabajo se podrían crear situaciones de conflicto en las reglas de consenso cuando alguien con suficiente potencia de minado quisiera atacar la red modificando las reglas sin antes alcanzar un consenso, o cuando una actualización del protocolo produzca un cambio imprevisto en esas reglas.

En cualquiera de estos casos los usuarios de la red se podrían llegar a encontrar con dos registros (*blockchains*) distintos. La *blockchain* más votada será aquella que tenga acumulada un mayor número de pruebas de trabajo.

Los nodos son los encargados de validar los bloques y las transacciones, y de actualizar la *blockchain*.

Los *wallets* generan las transacciones, las firman y las envían a los nodos para ser validadas y puestas en una lista de espera (*mempool*) a disposición de los mineros.

Los mineros generan los bloques de la cadena.
Para ello obtienen el *Merkle tree* de las transacciones que quieran escoger entre aquellas que se ya se encuentran en la lista de espera. El *root hash* de ese árbol de *Merkle* lo usan como parte del mensaje a *hashear* con un algoritmo de prueba de trabajo tipo *hashcash*.
El minero que logra encontrar el *hash* válido se lo comunica a los demás nodos, que lo verifican y actualizan la *blockchain*. Sólo entonces los mineros reinician sus procesos y comienzan a generar el siguiente bloque incentivados por los nuevos *bitcoins* que obtendrán si logran dar con el *hash* requerido por el nivel de dificultad.

En caso de encontrarnos con dos cadenas, la “real” será la más larga, la respaldada o votada por la mayoría al igual que en el supuesto de los *generales Bizantinos* en el dilema resuelto por *Satoshi*.

Mientras los mineros honestos mantengan la mayor parte de la capacidad de proceso (*hashrate*), su cadena crecerá más rápido que cualquier otra. Si un atacante llegara a tener más potencia que todos los demás juntos, podría cambiar las reglas de forma unilateral, pero en ese mismo momento o probablemente mucho antes, el sistema se devaluará hasta el punto en el que dicho ataque no sea rentable. Los inversores habrán abandonado el sistema hasta que la situación se solucione.

Los mineros son quienes obtienen las pruebas de trabajo y por tanto los únicos con “derecho” a voto. Es su potencia de cálculo y el gasto que realizan para obtenerla la que les otorga ese derecho. Pero los mineros no están sólos en la red, dependen también de los nodos para validar las transacciones de los usuarios y mantener la *blockchain*.
Los usuarios por su lado son quienes dan valor al servicio y por tanto quienes ponen precio a los *tokens*.

[32] Preukschat, Alexander, (2017) *Blockchain: la revolución industrial de internet*. Gestión 2000.
Recuperado de: `http://libroblockchain.com/consenso/` (31/05/2018).

11. Estudio de las ventajas y desventajas de los diferentes mecanismos de consenso de *blockchain*.

La innovación en el terreno de las *blockchains* no ha sido exclusivamente de tipo técnica. También se han propuesto mejoras para reemplazar las pruebas de trabajo basadas en *SHA256*, pero también se han diseñado y puesto en marcha *blockchains* alternativas que exploran distintos aspectos sociales y económicos. Algunas como *Ethereum* se orientan a la ejecución de contratos complejos, otras a los mercados de valores o de predicciones y otras como *Monero* o *Dash* a la privacidad. En todas ellas se necesita definir la forma en la que se establece un consenso sobre el estado de la *blockchain*.

Para poder llegar a un consenso en un sistema descentralizado de tipo *blockchain* se necesita conocer con anterioridad cuáles serán las reglas de consenso, es decir, las que deberán cumplir los bloques para ser admitidos en una cadena. En este punto sería interesante recordar el dilema de los generales Bizantinos.

Los nodos que forman la red son los responsables de actualizar la *blockchain* y son ellos quienes verifican los bloques antes de incorporarlos a la cadena. Los mineros por su lado son los encargados de crear los bloques y por tanto quienes ostentan el poder último para decidir cuál es la cadena legítima en caso de discrepancia.

En el caso de las *blockchains* públicas cualquiera puede ser minero y bastará con reunir los requisitos y recursos necesarios. En las *blockchains* privadas en cambio el consenso depende de las instituciones participantes, que actuarán como partes de un contrato privado que es el que en última instancia regula las relaciones entre ellos.

El consenso en cadenas públicas es en donde encontramos un cambio de paradigma capaz de transformar todo aquello que conocemos hasta el momento. Como en el consenso descentralizado no existe ninguna autoridad a la que recurrir, son las propias reglas del juego las que deben incorporar los incentivos necesarios para lograr que a las partes les compense actuar de forma honesta. Mejor dicho, hay que partir de la presunción de que los participantes en la red no se comportarán de forma “honesta” y tomarán sus decisiones pensando únicamente en maximizar su rentabilidad. Si los incentivos están bien planteados, será su propio interés quien les lleve a actuar de forma honesta. Este principio tiene su base en la teoría de juegos y en el equilibro de *Nash*, y es la clave para la estabilidad de todo el sistema. Cualquier cambio que se realice en las reglas de consenso y concretamente en aquellos que establecen los incentivos es por tanto sumamente delicado.

En una *blockchain* privada no se requiere un consenso mayoritario y basta con que intervengan exclusivamente las partes intervinientes con arreglo al estatuto o contrato que hubieran firmado. En una *blockchain* de consenso descentralizado todos los cambios requieren la aceptación de la mayoría, y en consecuencia se necesita un protocolo que defina en qué consiste esa mayoría.

Algoritmos de consenso.

- Pruebas de trabajo (*Proof of Work*), en donde tienen más voto los que realizan una mayor cantidad de trabajo. Es el sistema *hashcash* y el principal mecanismo de consenso en las *blockchains* públicas más conocidas como *Bitcoin* y *Ethereum*.
- Pruebas de participación (*Proof of Stake*) , en donde tienen más voto quienes poseen un mayor porcentaje de los *tokens* emitidos. Se utiliza por *Nxtcoin*, *Peercoin*, *Bitshares* y otras criptomonedas.
- Pruebas de importancia (*Proof of Importance*) , en donde el que más dinero mueve, más puntos recibe.

[33] Preukschat, Alexander, (2017) *Blockchain: la revolución industrial de internet*. Gestión 2000.
Recuperado de: `http://libroblockchain.com/consenso/` (31/05/2018).

Proof-of-Work.

Proof-of-Work consiste en problemas matemáticos con dificultad avanzada. De esta forma se requiere de equipos avanzados y un elevado consumo de electricidad para resolverlos. Los equipos y la electricidad que requieren forman una cantidad abismal de recursos desperdiciados. *PoW* es perjudicial para el medio ambiente.

Otro problema del costo elevado que implica participar en el trabajo de un sistema *PoW* es que cada vez menos personas pueden adquirir los equipos necesarios y por lo tanto la comunidad se vuelve más exclusiva.

Proof-of-Stake.

En *PoS* los participantes sólo pueden contribuir a la computación en la proporción en la cual poseen recursos en el sistema.

PoS no solo es más seguro según teoría de juegos, si no que también es más sustentable y mejor para el medio ambiente. Los cálculos criptográficos en *PoS* son mucho más fáciles de computar y por lo tanto no requieren de equipos especializados. Sólo requieren probar que posees cierto porcentaje de monedas en una moneda. El consumo de energía como resultado también es muy leve.

PoS es más justo y democrático porque invita a participar a cualquiera, no solamente los que pueden adquirir equipos especializados con un costo elevado (más descentralización).

Proof-of-Importance.

Proof-of-Importance es un mecanismo de consenso del *blockchain* que asigna un puntaje a los participantes basado en su participación en el sistema, en vez de asignarlo sólo en sus recursos (cantidad de monedas). Esto previene que los participantes del sistema se dediquen a acumular dinero. En *PoI*, el que más dinero mueve, más puntos recibe.

[34] Elaborado de: `https://www.karlbooklover.com/consensos-del-blockchain/` (31/05/2018).

12. Estudio que constate las diferencias entre *blockchain* público y privado.

Una *blockchain* puede clasificarse de muchas maneras, pero básicamente puede hacerlo según dos propiedades importantes:
quién puede leer la información y quién puede escribirla.

Si todo el mundo puede leer la información decimos que esta *blockchain* alcanza un máximo de transparencia.

Según quién pueda escribir podemos ver en dicha *blockchain* que si todos pueden escribir en ella consigue un máximo nivel de *anticensorship*. Nadie puede censurar las cosas que aparecen en la *blockchain*.

Entonces en función de una cosa y otra, dependiendo de quién puede escribir y leer en una *blockchain* podemos definir tres niveles:

Una *blockchain* totalmente abierta, donde todo el mundo puede leer la información (*Bitcoin*, *Ethereum*).

Una *blockchain* parcialmente transparente donde puede leerse toda la información, pero hay alguna que está cifrada (*Zcash*).

Zcash es una criptomoneda parecida a los *bitcoins*, pero que permite hacer transacciones anónimas, por lo tanto en estas transacciones hay información que no puede leerse.

También puedes tener una *blockchain* totalmente cerrada donde solo pueden acceder usuarios autorizados.

En cuanto a quién puede escribir en la *blockchain*, simplemente hay dos opciones:
la *permisionless blockchain* o *blockchain* abierta donde todo el mundo puede escribir y una privada o *permissioned* donde solo pueden escribir una parte de usuarios autorizados.

De las abiertas hay *bitcoins*, *ethereums*, *zcash*, *litecoins* todas las criptomonedas que hay hoy en día y de las cerradas hay menos conocidas. Quizá las más conocidas son *Hyperledger*, detrás de la cual está *IBM* y *Corda* que está desarrollada por un conjunto de bancos, por una asociación de bancos y también es una *blockchain* cerrada.

Teniendo en cuenta que una *blockchain* es esto:
un registro de transacciones donde vas añadiendo información, ¿qué es una *blockchain technology*?
Esto es como añadir una cosa más redundante.

Una *blockchain technology* son todos los mecanismos y técnicas que permiten que pueda lograrse esta propiedad de integridad y de no modificación.

¿De acuerdo?

Es decir, esto es muy dispar en función de si son *blockchains* abiertas o cerradas.

En una *blockchain* cerrada, prevenir que escriba según quién puede ser más fácil que en una abierta.
Prevenir que según quién escriba algo inapropiado.

El concepto de *blockchain technology* cuando se habla en genérico es un concepto algo etéreo y muchas veces se habla de *blockchain technology* en ciertos ámbitos y se hace referencia a propiedades de una cosa y otra y se mezclan.

Esto puede derivar en conceptos erróneos según el escenario.

Entonces, desde el punto de vista de la dicotomía sobre *blockchain* privadas y públicas, desde el punto de vista científico, que es a lo que nos dedicamos en las universidades, creemos que las *blockchains* abiertas son más integrantes porque cuando tú tienes una *blockchain* pública asumes que está completamente distribuida y lograr que sea una *blockchain* donde solo pueda añadirse información y que no pueda cambiarse la añadida es un problema complicado en cuanto a la seguridad.

Cuando has limitado quién puede escribir y quién no y tienes un sistema jerárquico hacer estas limitaciones resulta bastante trivial.

Aun así, desde el punto de vista comercial es interesante el tema de las *blockchain* privadas porque puede definir un sistema jerárquico de usuarios donde uno tiene más privilegios que otro y puedes tener información privada, lo cual es interesante según el ámbito empresarial.

[35] Transcrito de:
Herrera, Jordi. *Congrés de Seguretat informàtica UOC-CON*. 15/5/2017.
WannaCry: un mal ejemplo de gestión de pagos con *bitcoins.*
Bitcoin and ransomware: la caída de *Wannacry*
Recuperado de: https://www.youtube.com/watch?v=ixdhXQhYx4A (31/05/2018).

13. Estudio y definición del concepto de *Smart Contracts*.

Si lo que incluimos en la *blockchain* son programas, tendríamos lo que llamamos *Smart Contracts*: una *blockchain* como la de *Ethereum*, que permite ejecutar programas.

[36] Transcrito de:
Herrera, Jordi. *Congrés de Seguretat informàtica UOC-CON*. 15/5/2017.
WannaCry: un mal ejemplo de gestión de pagos con *bitcoins.*
Bitcoin and ransomware: la caída de *Wannacry*
Recuperado de: https://www.youtube.com/watch?v=ixdhXQhYx4A (31/05/2018).

Smart Contract es un contrato capaz de ejecutarse o hacerse cumplir por sí mismo.
Tradicionalmente en la ejecución de un contrato es necesaria la implicación de terceros. El *Smart Contract* nos permite omitir estos terceros.

Es decir, el término *Smart Contract* hace referencia cualquier contrato que se ejecuta por sí mismo automáticamente sin necesidad de que terceros intervengan entre los participantes del contrato.

Los *Smart Contracts* se escriben en lenguajes de programación que permiten definir reglas y consecuencias, prescindiendo del lenguaje legal. El software debe ser capaz de definir reglas y consecuencias estrictas, de la misma forma que quedaría especificado en un contrato tradicional. El *Smart Contract* puede tomar información como entrada para procesarla según las reglas definidas y actuar en consecuencia.

Un ejemplo claro donde aplicar los *Smart Contracts* podría ser en los sistemas de *crowdfunding* (micromecenazgo), que consiste en conseguir donaciones colectivas para un propósito determinado. Habitualmente se especifica una cantidad mínima de dinero a la que llegar para llevar a cabo el proyecto. Una vez llegado a realizar el proyecto, los mecenas pueden recibir o no la recompensa.
En el ámbito de los contratos inteligentes se podrían automatizar muchos procesos fácilmente, como por ejemplo si no se llega a la cantidad de dinero deseada revertir las transferencias o imponer medidas de seguridad para que quien reciba el dinero no lo utilice a su antojo.

Ventajas.

- Automatización.
  Muchas tareas manuales no son necesarias en un contrato inteligente ya que él mismo se encarga de la ejecución.
- Rapidez.
  La automatización conlleva mayor rapidez en la ejecución.
- Ausencia de terceros.
- Disminución de gastos.

Inconvenientes.

- Acceso y fiabilidad de los datos de entrada.
  El *Smart Contract* debe ser capaz de adquirir fuentes fiables de datos para no cometer ni errores ni fraudes.
- Lenguaje legal.
  Es difícil especificar claramente sin ambigüedades todas las condiciones de un contrato.
- Aceptación.
  Es muy difícil conseguir la aceptación jurídica de los *Smart Contracts*.
- Anulaciones y modificaciones.
  Es muy habitual en un contrato querer cambiar las condiciones actuales o incluso anular ese *software* si todas las partes están de acuerdo. Los contratos inteligentes deben prever todas estas vicisitudes para realmente ser una alternativa a los contratos.

[37] Traducido y elaborado sobre documentación de Andreu, Josep Miquel. (2016) *Smart Contracts sobre Bitcoin*.
Barcelona: Editorial Universitat Oberta de Catalunya. Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons
Recuperado de: `http://openaccess.uoc.edu/webapps/o2/handle/10609/46043` (31/05/2018).

Cómo funciona.

El código que constituye el contenido del contrato se almacena en la cadena de bloques. El código debe basarse en reglas lógicas (si pasa X, entonces Y) y condiciones (que pueden interactuar con dispositivos autónomos como sensores de *IOT*). El resultado es un acuerdo virtual blindado con todas las eventualidades cubiertas, de manera que si todas las partes entregan lo acordado, no existirá posibilidad de fraude.

En ocasiones resulta imprescindible acudir a agentes externos que verifiquen el cumplimiento de una condición. A estos agentes se les denomina oráculos. Los oráculos son instrumentos informáticos que permiten validar las condiciones previstas en los *Smart Contracts*.
Generalmente hacen referencia a información externa para decidir si una cláusula del contrato ha sucedido o no. De esta manera, una vez que el oráculo obtiene la información y la contrasta, el contrato se ejecuta y la transacción se produce.
...
Los *Smart Contracts* aumentarán la velocidad de la ejecución de las transacciones, lo que se traducirá eventualmente en la posibilidad de cerrar un mayor volumen de acuerdos con menor riesgo al cumplimiento.

[38] Recuperado de:
`https://retina.elpais.com/retina/2017/12/22/tendencias/1513937575_114270.html` (31/05/2018).

Contratos sobre *blockchains*.

Estos tipos de *Smart Contracts* probablemente sean los más conocidos hoy en día. Gracias al nacimiento de *Bitcoin* como moneda descentralizada se introdujeron nuevos elementos y herramientas como *blockchains* que se pueden utilizar para la creación de *Smart Contracts*.

En todas las monedas basadas en *blockchain*, todos los nodos que forman parte de la red correspondiente mantienen una lista común de todas las transacciones conocidas (cadena de bloques).

Los nodos generadores de la moneda (mineros) crean los bloques añadiendo un *hash* del último bloque creado de la cadena más larga y de las nuevas transacciones acumuladas desde la creación del último bloque.
Cuando un minero encuentra un bloque, lo comparte con el resto de nodos.

Esta forma de comunicar transacciones sin necesidad de una entidad central, permite transacciones distribuidas entre usuarios y garantiza que no haya doble gasto de la moneda.

Bitcoin incorpora un lenguaje de *scripting* basado en un lenguaje llamado *Forth* que permite realizar algunas acciones e implementar *Smart Contracts*.
Este lenguaje de *scripting* es un lenguaje de instrucciones simples, basado en pila y procesado de izquierda a derecha. Se considera un lenguaje *Turing* no completo, sin la opción de ejecutar bucles.

[39] Traducido y elaborado sobre documentación de Andreu, Josep Miquel. (2016) *Smart Contracts sobre Bitcoin*.
Barcelona: Editorial Universitat Oberta de Catalunya. Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons
Recuperado de: `http://openaccess.uoc.edu/webapps/o2/handle/10609/46043` (31/05/2018).

14. Estudio de los aspectos de seguridad de *Bitcoin*, *blockchain* y *Smart Contracts*.

Bitcoin, aspectos de seguridad.

Los sistemas como *Bitcoin* están respaldados por un conjunto de primitivas avanzado. Las primitivas criptográficas de las que *Bitcoin* hace uso son las responsables de que se consigan las propiedades de seguridad.

Firmas digitales.

Bitcoin utiliza el algoritmo *ECDSA* (*Elliptic Curve Digital Signature Algorithm*) –algoritmo de firma digital de curva elíptica– para firmar las transacciones, utilizando los parámetros recomendados por el *Standards for Efficient Cryptography Group* (*SECG*), *secp256k1*.

Las firmas utilizan la codificación *DER* para empaquetar sus componentes en un único flujo de bytes.

ECDSA ofrece ventajas frente a otros esquemas de firma que lo hacen ideal para su utilización en un protocolo distribuido en Internet, como son:
• Longitudes de clave y de firma muy cortas.
• Generación y verificación de firmas muy rápidas.

Hashes criptográficos.

En los cálculos de *hashes* realizados en *Bitcoin* se utilizan los estándares *SHA-256* y, cuando se requiere que el *hash* sea más corto, *RIPEMD-160*. Normalmente el cálculo de *hashes* se realiza en dos fases: la primera con *SHA-256* y la segunda, dependiendo de las necesidades de longitud del resultado, con *SHA-256* o *RIPEMD-160*.

Números aleatorios y *nonces*.

Los números aleatorios y su generación son pilares fundamentales de la criptografía. Los *nonces* son números aleatorios “especiales” que sólo se utilizan una vez.
En *Bitcoin*, los números aleatorios y *nonces* se utilizan de forma directa para la generación de bloques. Para obtener un nuevo bloque es necesario encontrar un número aleatorio que satisfaga ciertos requisitos.

Pruebas de trabajo.

Las pruebas de trabajo son el principal componente de *Bitcoin* responsable de garantizar que la red mantiene un comportamiento legítimo. Calcular nuevos bloques de transacciones conlleva un coste computacional muy elevado, de forma que para hacerse con el control de la red un atacante necesitaría una potencia de cómputo extremadamente difícil de conseguir. El principal precursor de esta idea es el método *Hashcash*.
El control se realiza obligando a que el *hash* de cada nuevo bloque deba comenzar con un número determinado de ceros. Para el cálculo de este *hash* se combinan datos de bloques anteriores y un *nonce*. Como las funciones *hash* criptográficas no son invertibles, para encontrar un bloque válido la única alternativa será ir obteniendo diferentes *nonce* hasta encontrar uno que cumpla el requisito preestablecido.

[40] INCIBE. *Bitcoin: Una moneda criptográfica.* (páginas 20 y 21). Recuperado de: `https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf` (31/05/2018).

La seguridad del *Bitcoin* depende de la custodia de las claves privadas.

Como consideraciones iniciales a tener en cuenta:

- No revele su clave privada.
- Si se sospecha que alguien la podría haber obtenido genere otra dirección y transfiera sus *bitcoins*.
- Utilice distribuciones *live* tipo *Tails* para sus conexiones.
- Use una contraseña larga.
- No use carteras *online* en las que no confía.

En cuanto al *wallet*:

- No olvide su contraseña.
- Haga una copia de seguridad.

Desconfíe de vendedores probablemente ilegítimos.

Seguridad gracias a un servicio de fideicomiso.
Lo ofrecen cada vez más páginas especializadas en venta de segunda mano con *bitcoins*. Realice el pago a la página y esta no lo procesa al vendedor hasta que el producto ha llegado a su destino.

Blockchain, aspectos de seguridad.

Blockchain es una tecnología disruptiva con un enorme potencial de mercado. Tiene el potencial de cambiar la forma en que se llevan a cabo los esfuerzos de ciberseguridad de sistemas industriales, y puede generar nuevas industrias enteras o nuevos segmentos en las industrias existentes, garantizando la integridad.

La seguridad de *Blockchain*.

Las características de descentralización y *peer-to-peer* de la tecnología hacen que sea más difícil de indisponibilizar que las arquitecturas de aplicaciones distribuidas convencionales (como cliente-servidor), pero también están sujetas a ataques *DDoS* y es por esto que se deben implementar medidas de protección adicionales, tanto a nivel de red como de aplicación.

Blockchain no tiene un único punto de falla, lo que disminuye considerablemente las posibilidades de un ataque *DDoS* basado en *IP* que interrumpa el funcionamiento normal. Si se baja un nodo, los datos siguen siendo accesibles a través de otros nodos dentro de la red, ya que todos ellos mantienen una copia completa del libro mayor en todo momento.

La integridad es el atributo destacable de *Blockchain*. La tecnología de *Blockchain* no proporciona confidencialidad y privacidad, por eso cuando hablamos de que *Blockchain* es "seguro", estamos refiriéndonos al aspecto de la integridad. Lo que crea confusión porque tiende a significar confidencial. La confidencialidad y la integridad de las claves privadas utilizadas por los participantes, o debilidades en los algoritmos criptográficos utilizados también son potenciales problemas de seguridad.

Un riesgo de integridad específico de *Blockchain* con un potencial impacto a gran escala se conoce como el ataque del 51%. Este ataque se plantea a menudo cuando se cuestiona la seguridad de *Blockchain*. En este caso en

particular, si un atacante controlara el 51% del poder de computo de toda la red de participantes, existiría el potencial de que el atacante llegue al "consenso" por sí mismo y por lo tanto impacte en la integridad de los datos. Peor aún, llamarlo el ataque del 51% es un nombre incorrecto, en realidad, el porcentaje de potencia informática necesaria puede ser mucho menor, tal vez incluso tan bajo como un 40% . En el caso de *Blockchain* respaldando una criptomoneda, tal ataque podría potencialmente permitir al atacante gastar los mismos fondos dos veces.

Es importante entender que mientras *Blockchain* proporciona una excelente solución para la integridad de la información, no es irrompible. También debemos tener en cuenta que, si bien hay avances en torno a la privacidad de *Blockchain*, por el momento no hay nada intrínsecamente seguro, en términos de confidencialidad, en el uso de la tecnología *blockchain*. Cualquiera sea nuestro caso de uso, si decidimos implementar la tecnología, tenemos que considerar todos los aspectos de seguridad de la información e incorporar los controles de seguridad adecuados en nuestra implementación.

[41] Elaborado de: `https://es.linkedin.com/pulse/la-seguridad-de-blockchain-y-para-alfredo-cammarota` (31/05/2018).

Smart Contracts, aspectos de seguridad.

Los contratos inteligentes son programas que se ejecutan en el *Blockchain*. Una de las grandes bondades del *Blockchain* es su inmutabilidad.
La seguridad en los contratos inteligentes es algo a tomarse muy en serio en el momento en que comenzamos a pensar en nuestro proyecto. Este tipo de tecnologías tienen la seguridad en el desarrollo de *software* como un tema crítico que no se puede dejar pasar por alto.

Recomendaciones
Para poder alcanzar un nivel de seguridad adecuado en nuestros contratos inteligentes, deberíamos incluir la seguridad dentro de todo el ciclo de vida del desarrollo de estos proyectos. Si no es incluida desde un principio, es muy probable que luego nos olvidemos de añadir controles necesarios. Olvidarse algo aquí es muy crítico, ya que no tenemos luego posibilidad de cambiar el contrato. Tendríamos entonces que finalizar el contrato actual y publicar uno nuevo, con todo lo que eso implica.

Desde el punto de vista técnico, más detalladamente, *Consensys* ha desarrollado diferentes recomendaciones con los conocimientos mínimos que debería tener un programador de *Solidity*:

- Llamadas externas: utilizarlas con mucha precaución.
- Marcar los contratos no confiables: cuando interactuamos con contratos externos hay que tener especial manejo en las interacciones con funciones, métodos, variables externas, y realizar los controles necesarios.
- No realizar cambios de estados después de realizar llamadas externas: debemos asumir que ante una llamada externa se podría estar ejecutando código malicioso que luego nos podría afectar en nuestro contrato.
- Realizar manejo de errores en las llamadas externas.
- Recordar que todo lo que está en *Blockchain* es público.
- No realizar devoluciones o otro tipo de operaciones después de llamadas externas, ya que podrían no terminar de ejecutarse.
- No asumir que los contratos son creados con balance cero.

También, en la página de *Solidity*, encontraremos recomendaciones de seguridad que se deberían seguir:

- Información privada y aleatoriedad: toda la información que pongamos en el *Blockchain* es pública, hay que tener especial cuidado con la implementación de funciones aleatorias.
- Reentradas: tener en cuenta que una función de un contrato podría volver a ser invocada por el mismo usuario antes de que la misma finalizara. Podría tener impactos graves, por ejemplo, en la transferencia de *Ethers*.
- Bucles y límites de gas: siempre que utilicemos bucles tenemos que poner límites a los mismos para que no consuma todo el gas.
- Aplicar controles en el envío y recepción de *Ethers*.

Recuerda siempre mantener los contratos inteligentes escritos de forma simple y pequeños, pero sobre todo, realizarle pruebas y verificar su seguridad de manera periódica.

[42] Elaborado de: `http://blog.elevenpaths.com/2018/03/smarts-contracts-ciberseguridad.html` (31/05/2018).

15. Conclusiones.

Se ha abordado la ejecución de este proyecto como un trabajo que permita poner en orden el conocimiento adquirido de las tecnologías *Bitcoin* y *Blockchain*.

Cabe destacar la ingente cantidad de material disponible en internet, que nos ha obligado a leer una y mil veces los conceptos base con mayor o menor acierto y a seleccionar y sintetizar el material que queríamos incluir en el resultado final, que implica en la mayoría de los casos intervenir combinando varias opciones para intentar mejorar el discurso sobre la materia a comunicar, intentando favorecer su capacidad divulgativa como era requerido.

No menos importante es también tener claro que las criptomonedas son un ecosistema en constante cambio y evolución, lo que hace reevaluar, gestionar y cuestionar la información recabada prácticamente cada semana para llevar el proyecto a buen puerto. El desarrollo de este trabajo nos ha demostrado que *Bitcoin* y *Blockchain* son tecnologías que han llegado aquí para quedarse.

Como directrices claves en el desarrollo futuro de este trabajo, sería interesante profundizar en la parte de *DApps*, y observar la evolución de las *blockchain* privadas y sus nuevas funcionalidades y usos emergentes.

16. Glosario.

Bitcoin: es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, *Bitcoin* es como dinero para Internet. *Bitcoin* puede ser el único sistema de contabilidad triple existente.

Blockchain: es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade metainformación relativa a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas la información contenida en un bloque sólo puede ser repudiada o editada modificando todos los bloques posteriores.

Bloque: es un registro que contiene confirmaciones de transacciones que se encontraban pendientes.

Cadena de bloques: traducción al castellano de *blockchain*.

Consenso: determina cuáles son las transacciones correctas con el fin principal de evitar el problema del doble gasto.

Creative Commons: es una organización sin ánimo de lucro dedicada a promover el acceso y el intercambio de la cultura.
Desarrolla un conjunto de instrumentos jurídicos de carácter gratuito que facilitan usar y compartir tanto la creatividad como el conocimiento.

Criptomoneda: es un medio digital de intercambio.

Ethereum: es una plataforma *Open Source*, descentralizada, basada en el modelo *blockchain*, que permite la creación de acuerdos de contratos inteligentes entre pares.

Incibe: es un organismo dependiente de Red.es y del Ministerio de Energía, Turismo y Agenda Digital de España. Tiene su sede oficial en la ciudad de León.

Litecoin: `(LTC)` es una criptomoneda sustentada por la red *P2P*, y un proyecto de software de código abierto publicado bajo la licencia *MIT*. Es prácticamente idéntica en su aspecto técnico a *Bitcoin* `(BTC)`.

Minería: es el proceso de invertir capacidad computacional para procesar transacciones, garantizar la seguridad de la red, y conseguir que todos los participantes estén sincronizados. Podría describirse como el centro de datos de *Bitcoin*, excepto que este ha sido diseñado para ser completamente descentralizado con mineros operando en todos los países y sin que nadie tenga el control absoluto sobre la red.

Peer-to-peer: `(P2P)` es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

Las redes *P2P* permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Ripple: (XRP) es un proyecto basado en *software* libre que persigue el desarrollo de un sistema de crédito basado en el paradigma de extremo a extremo. Cada nodo de *Ripple* funciona como un sistema de cambio local, de tal manera que todo el sistema forma un banco mutualista descentralizado. Llevado al extremo, la red *Ripple* es un servicio de red social distribuido basado en el honor y en la confianza entre las personas existentes en las redes sociales del mundo real. De esta manera, el capital financiero se sustenta en el capital social. Una versión reducida de la red *Ripple* consistiría en una extensión del sistema bancario jerárquico existente, en el cual existirían rutas de pago alternativas que no pasarían por un banco central.

Smart Contracts: es un programa informático que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes (por ejemplo, personas u organizaciones). Como tales ellos les ayudarían en la negociación y definición de tales acuerdos que causarán que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas.

Transacción: son entendidas como los envíos de *bitcoins*. Son registros guardados en la cadena de bloques (*blockchain*).

[43] Definiciones recuperadas de:
https:// es.wikipedia.org/, (31/5/2018).
https://bitcoin.org/es/faq, (31/5/2018).
https://blog.bit2me.com/es/transacciones-bitcoin/, (31/5/2018).

17. Referencias bibliográficas.

[1] https://es.investing.com/crypto/currencies (31/5/2018).

[2] http://blockchain.info (31/5/2018).

[3], [10], [16] Bitcoin. *Preguntas más frecuentes*.
© Bitcoin Project 2009-2018 Publicado bajo la licencia *MIT*
Recuperado de: https://bitcoin.org/es/faq (31/05/2018).

[4] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*.
Recuperado de: https://bitcoin.org/bitcoin.pdf (31/05/2018).

[5] Recuperado de:
https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html
(31/05/2018).

[6], [8], [19], [35], [36] Transcrito de:
Herrera, Jordi. *Congrés de Seguretat informàtica UOC-CON*. 15/5/2017. *WannaCry*: un mal ejemplo de gestión de pagos con *bitcoins*. *Bitcoin and ransomware*: la caída de *Wannacry*
Recuperado de: https://www.youtube.com/watch?v=ixdhXQhYx4A
(31/05/2018).

[7], [9], [12], [14], [17], [18], [40] INCIBE. *Bitcoin: Una moneda criptográfica*.,
(páginas 17, 18, 19, 20, 21, 22).
Recuperado de:
https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf (31/05/2018).

[11], [20] Elaborado de:
Bitcoin. ¿Cómo funciona Bitcoin?. © *Bitcoin Project* 2009-2018.
Publicado bajo la licencia *MIT*. Recuperado de:
https://bitcoin.org/es/como-funciona (31/05/2018).

[13] *bitcoin* wiki. Transacción.
Recuperado de: https://es.bitcoin.it/wiki/Transacción
(31/05/2018)

[15] *Bitcoin*. *bitcoin* para personas.
© Bitcoin Project 2009-2018 Publicado bajo la licencia *MIT*.
Recuperado de: https://bitcoin.org/es/bitcoin-para-personas
(31/05/2018).

[21] Medina Reyes, María Fernanda. (2016) *Análisis y comparación de monedas criptográficas basadas en la tecnología Blockchain* (páginas 10 y 11).
Barcelona: Editorial Universitat Oberta de Catalunya. Reconocimiento-NoComercial- SinObraDerivada 3.0 España de Creative Commons
Recuperado de:
http://openaccess.uoc.edu/webapps/o2/handle/10609/56344
(31/05/2018)

[22] Elaborado sobre una idea de:
Acuña, Héctor. (noviembre 2017). *Estudio sobre Bitcoin y Tecnología Blockchain*. Cuadernos CEF - ESE Business School.
Recuperado de: http://www.ese.cl/wp-content/blogs.dir/1/files_mf/1510073019CUADERNOS_CEF_1_EstudiosobreBitcoinytecnolog%C3%ADaBlockchainv2003.pdf (31/05/2018).

[23], [24] Recuperado de: https://miethereum.com/blockchain/#toc3 (31/05/2018).

[25] Elaborado de:
https://nuevofinanciero.com/ethereum-blockchain-ether-bitcoin/ (31/05/2018).

[26] Recuperado de:
.....https://www.criptonoticias.com/aplicaciones/blockchain-.....privada-ripple-encamina-descentralizacion/ (31/05/2018).

[27] Recuperado de:
.....https://www.criptonoticias.com/informacion/blockchains-.....criptomonedas-fundamentos-caracteristicas/ (31/05/2018).

[28] Elaborado propia sobre una idea de:
https://www.xoken.org/blog/features-of-various-blockchains-a-comparison/ (31/05/2018).

[29] Adaptado y recuperado de:
https://es.wikipedia.org/wiki/Prueba_de_trabajo_(algoritmo_de_consenso_distribuido) (31/05/2018).

[30], [32], [33] Preukschat, Alexander, (2017) *Blockchain: la revolución industrial de internet*.
Gestión 2000.
Recuperado de: http://libroblockchain.com/consenso/ (31/05/2018).

[31] Elaborado de:
https://www.oroyfinanzas.com/2016/03/4-capas-red-bitcoin-por-que-importante-consenso-cambios/ (31/05/2018).

[34] Elaborado de:
https://www.karlbooklover.com/consensos-del-blockchain/ (31/05/2018).

[37], [39], Traducido y elaborado sobre documentación de:
Andreu, Josep Miquel. (2016) *Smart Contracts sobre Bitcoin*.
Barcelona: Editorial Universitat Oberta de Catalunya.
Reconocimiento-NoComercial- SinObraDerivada 3.0 España de Creative Commons
Recuperado de:
http://openaccess.uoc.edu/webapps/o2/handle/10609/46043 (31/05/2018).

[38] Recuperado de:
https://retina.elpais.com/retina/2017/12/22/tendencias/1513937575_114270.html (31/05/2018).

[41] Elaborado de:
https://es.linkedin.com/pulse/la-seguridad-de-blockchain-y-para-alfredo-cammarota
(31/05/2018).

[42] Elaborado de:
http://blog.elevenpaths.com/2018/03/smarts-contracts-ciberseguridad.html (31/05/2018).

[43] Definiciones recuperadas de:
https:// es.wikipedia.org/ (31/05/2018).
https://bitcoin.org/es/faq (31/05/2018).
https://blog.bit2me.com/es/transacciones-bitcoin/ (31/05/2018).