Universitat Oberta de Catalunya

uoc.edu

Análisis de los distintos tipos de cadenas de bloques

Koldo Pérez de San Román Martínez de Lahidalga
Máster Universitario en Ciberseguridad y Privacidad
Sistemas de Blockchain

Alberto Ballesteros Rodríguez
Víctor García Font

Junio 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Análisis de los distintos tipos de cadenas de bloques*
Nombre del autor:	*Koldo Pérez de San Román Martínez de Lahidalga*
Nombre del consultor/a:	*Alberto Ballesteros Rodríguez*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2021
Titulación:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Sistemas de Blockchain*
Idioma del trabajo:	*Castellano*
Palabras clave	*Blockchain, criptomoneda, transacción*

Resumen del Trabajo:

Las cadenas de bloques son la tecnología detrás de las criptomonedas; una tecnología que ha revolucionado el mundo de los sistemas de información. Las redes de cadenas de bloques permiten mantener registros descentralizados y distribuidos de transacciones digitales en forma de libro mayor de forma segura y transparente. El objetivo principal de este trabajo es exponer, analizar y describir todo aquello que se conozca acerca de los distintos tipos de cadenas de bloques.

Para llevar a cabo este cometido, se ha seguido una metodología que incluye cinco etapas: la planificación del proyecto, una breve introducción a unos conceptos básicos necesarios para entender el funcionamiento de las cadenas de bloques, el análisis de cada uno de los distintos tipos, la realización de comparaciones entre los aspectos más relevantes de estos tipos y, finalmente, la exposición de las conclusiones obtenidas a raíz del análisis.

Abstract:

Blockchain is the technology behind the cryptocurrency; a technology that has revolutionized the world of Information Systems. Blockchain networks allow their users to keep decentralized and distributed records of digital transactions in the form of a ledger, in a secure and transparent way. The main purpose of this paper is to expose, analyze and describe every information known about the different types of blockchains.

In order to achieve this purpose, a five-stage methodology has been followed, which includes: a planning of the project, a brief introduction to some basic concepts necessary to understand how blockchains work, the analysis of each of the different blockchain types, some comparisons between the most relevant aspects of these types and, finally, the conclusions achieved as a result of the analysis.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El reciente auge de la capitalización de las criptomonedas, como el *Bitcoin*, denota una vez más el inexorable crecimiento de la digitalización en nuestra era. Y es que las divisas digitales proporcionan una confianza y seguridad superiores para el usuario en cada transacción, contra las cuales la moneda física no es capaz de competir. Esto se debe, en gran parte, a la tecnología en la que las criptomonedas están basadas: las cadenas de bloques.

Las cadenas de bloques o *blockchain*, basadas en una combinación de criptografía asimétrica, funciones hash, curva elíptica (en algunos casos), etcétera, permiten mantener registros descentralizados y distribuidos de transacciones digitales documentadas en forma de libro mayor, haciendo uso de direcciones donde la identidad de los usuarios no es revelada en momento alguno, resultando así transacciones seguras y transparentes. Esta tecnología se puede considerar como un libro contable (*ledger*), puesto que registra y comparte con todos los nodos de la red todas las transacciones realizadas desde su creación.

No obstante, la aplicabilidad de la tecnología *blockchain* va más allá de las monedas digitales. Conceptos como *Smart Contracts*, voto electrónico, *Internet of Things* (IoT) o almacenamiento en la nube, verbigracia, son ya una realidad de las posibles aplicaciones de esta tecnología y de la revolución que suponen las cadenas de bloques, dado que garantizan que las transacciones, no sólo económicas, sean seguras y fiables, evitan la falsificación de datos y previenen la pérdida de información, desbancando por completo a los sistemas actuales de flujo de datos.

Mediante este proyecto, se analizará en profundidad la tecnología en la que se basan los protocolos de las criptodivisas con más repercusión en la actualidad.

1.2 Objetivos del Trabajo

El objetivo principal de este proyecto es exponer, analizar y describir todo aquello que se conoce acerca de las cadenas de bloques y sus distintos tipos. Para lograr este cometido, se ha dividido en cuatro objetivos generales:

- Exponer los conceptos básicos necesarios para comprender el funcionamiento de la tecnología *blockchain*.

- Analizar en profundidad uno a uno los distintos tipos de cadenas de bloques que existen.

- Realizar una comparación de los aspectos más relevantes entre las distintas cadenas de bloques, como bien pueden ser el acceso, la gobernanza, los algoritmos de consenso, etc.

- Exponer y analizar las conclusiones obtenidas a raíz de los análisis realizados sobre las distintas propiedades de las cadenas de bloques.

1.3 Enfoque y método seguido

Para llevar a cabo este trabajo, se ha planteado una metodología que permita cumplir con todos los objetivos previamente establecidos. Esta metodología incluye cinco etapas.

- *Primera etapa: Plan de trabajo*.

En esta primera etapa se estudiará el contexto del tema principal del proyecto. Asimismo, se definirán los objetivos, la metodología y las tareas a realizar para alcanzar los objetivos, así como una planificación temporal para cumplir dichas tareas.

- *Segunda etapa: Análisis de los conceptos básicos*.

La segunda etapa del proyecto consistirá en realizar una introducción sobre los conceptos básicos de las cadenas de bloques y el contexto, sirviendo de introducción para el análisis de los distintos tipos de *blockchain.*

- *Tercera etapa: Análisis de los distintos tipos de cadenas de bloques*.

Una vez se haya introducido el tema, se procederá a analizar los diferentes tipos de cadenas de bloques que existen, explicando en detalle cada una de las características de estas redes.

- *Cuarta etapa: Comparaciones entre los tipos de cadenas de bloques*.

Tras el análisis, se realizarán comparaciones entre los aspectos más relevantes (gobernanza, acceso, etc.) de cada tipo de cadenas de bloques.

- *Quinta etapa: Conclusiones*.

Por último, se expondrán las conclusiones a las que se haya llegado con la realización de este proyecto acerca de las cadenas de bloques.

1.4 Planificación del Trabajo

Para realizar este proyecto y cumplir con los objetivos planteados anteriormente, se han definido doce tareas:

1. Realizar la planificación del proyecto.
2. Recopilar información sobre las cadenas de bloques y sus distintos tipos.
3. Realizar una introducción a los conceptos básicos sobre la tecnología *blockchain.*
4. Realizar y redactar un análisis sobre las cadenas de bloques públicas.
5. Realizar y redactar un análisis sobre las cadenas de bloques privadas.
6. Realizar y redactar un análisis sobre las cadenas de bloques de consorcio.
7. Realizar y redactar un análisis sobre *permissioned blockchain*.
8. Realizar y redactar un análisis sobre *permissionless blockchain*.
9. Comparar los tipos de cadenas de bloques.
10. Obtener conclusiones.
11. Redactar la memoria final del proyecto.
12. Preparar la presentación.

En la figura 1 se puede apreciar la planificación temporal de todas estas tareas. La memoria final ha sido redactada en paralelo al análisis realizado de cada uno de los tipos.

Nombre de la tarea	Fecha de inicio	Fecha de fin	Duración en días
Realizar la planificación del proyecto	17/2/21	2/3/21	13
Recopilar información sobre las cadenas de bloques y sus distintos tipos	3/3/21	15/3/21	12
Realizar una introducción a los conceptos básicos sobre la tecnología *blockchain*	10/3/21	25/3/21	15
Realizar un análisis sobre las cadenas de bloques públicas	26/3/21	10/4/21	15
Realizar un análisis sobre las cadenas de bloques privadas	10/4/21	20/4/21	10
Realizar un análisis sobre las cadenas de bloques de consorcio	20/4/21	27/4/21	7
Realizar un análisis sobre *permissioned blockchain*	27/4/21	5/5/21	8
Realizar un análisis sobre *permissionless blockchain*	5/5/21	10/5/21	5
Comparar los tipos de cadenas de bloques	10/5/21	27/5/21	17
Obtener conclusiones	15/5/21	31/5/21	16
Redactar la memoria final del proyecto	10/3/21	31/5/21	82
Preparar la presentación	1/6/21	5/6/21	4

Figura 1: Planificación temporal del trabajo.

Las primera tarea, donde se ha realizado la planificación del proyecto, ha sido la primera entrega, correspondiente a la *PEC 1*. Las tareas de recopilación de información, introducción a conceptos básicos y parte del análisis de las cadenas de bloques públicas han correspondido a la entrega de la segunda *PEC*. La tercera entrega ha introducido el análisis de las cadenas de bloques privadas y de consorcio. Y, por último, la última entrega englobaba el resto de tareas de análisis, comparaciones y obtención de conclusiones para la redacción definitiva de la memoria final.

Mediante el diagrama de Gantt (figura 2), se proporciona una vista general de la planificación del proyecto y representa de una manera más visual la organización de las fechas de inicio y finalización de cada una de las tareas.

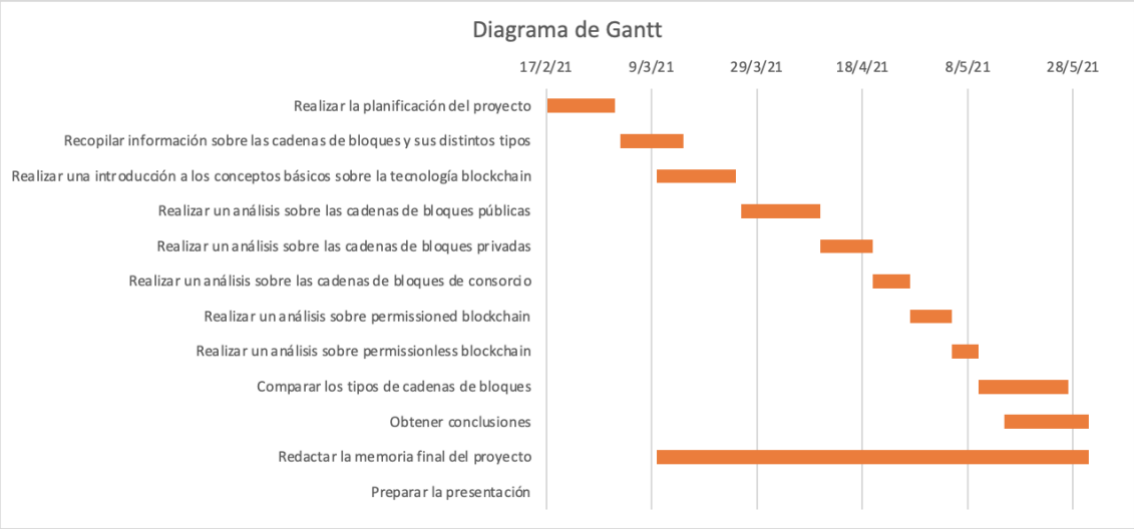

Figura 2: Diagrama de Gantt de la planificación.

1.5 Breve descripción de los otros capítulos de la memoria

En este apartado se realizará una breve explicación de los contenidos de cada capítulo del presente trabajo y su relación con los objetivos del mismo.

- **Capítulo 1: Introducción.** En este capítulo se proporciona toda la información relativa a la realización del proyecto, empezando por el contexto y justificación del Trabajo y los objetivos principales, seguido de la metodología y el enfoque utilizados y la planificación temporal.

- **Capítulo 2: Conceptos básicos.** En este segundo capítulo, se introduce al lector algunos de los conceptos más relevantes y necesarios sobre las cadenas de bloques para la propicia comprensión del trabajo.

- **Capítulo 3: Redes según acceso: públicas, privadas y de consorcio.** En este apartado se realiza un análisis de las cadenas de bloques en función de su acceso. Se explican las características principales de los

distintos tipos, así como du funcionamiento y algunos ejemplos de estos tipos de redes.

- **Capítulo 4: Redes según privilegios: *permissioned* y *permissionless.*** Este capítulo ofrece otro análisis de los distintos tipos de cadenas de bloques, esta vez desde el punto de vista de los privilegios. Al igual que en el anterior, en este capítulo se ofrece una explicación de las características y el funcionamiento de estas redes, además de varios ejemplos de cada tipo.

- **Capítulo 5: Clasificación de distintas *blockchains*.** Una vez analizado cada uno de los distintos tipos de cadenas de bloques, se procede a clasificar y comparar estos tipos, explicar las posibles combinaciones, ventajas y desventajas de cada tipo, etcétera.

- **Capítulo 6: Conclusiones y trabajo futuro.** Este capítulo culmina el análisis de las cadenas de bloques proporcionando las conclusiones que se han alcanzado durante la realización del trabajo y se mencionan los posibles futuros trabajos a realizar.

- **Capítulo 7: Glosario.** Este apartado recoge todos los tecnicismos o términos relevantes que han sido utilizados en el presente trabajo, seguidos de una breve definición.

- **Capítulo 8: Bibliografía.** En esta última sección se recogen todas las referencias bibliográficas utilizadas para la redacción de la memoria final.

2. Conceptos básicos

Las cadenas de bloques o *blockchain* son una tecnología basada en una combinación de funciones hash, criptografía asimétrica, curva elíptica, etc. que permite mantener registros descentralizados y distribuidos de transacciones digitales. Esta estructura de datos funciona como una red P2P (*Peer-To-Peer*) donde el nodo emisor y el nodo receptor de la transacción, los cuales son independientes, participan simultáneamente como cliente y como servidor, eliminando la necesidad de un intermediario. Dichas transacciones quedan documentadas en forma de libro contable (*ledger*) sin revelar en ningún momento la identidad de los usuarios y se comparten con el resto de nodos de la red, que guardan una copia actualizada en tiempo real de todas las transacciones realizadas desde la creación de la *blockchain*.

Entre las características de las cadenas de bloques destaca notoriamente su carácter descentralizado, puesto que no depende de una entidad u organismo central de confianza. Asimismo, es una tecnología distribuida, abierta y de consenso, ya que parte de unas normas claras y consensuadas sobre la validez y el estado de las transacciones y que permite a cualquier usuario hacer uso de ella [1]. Gracias a los mecanismos criptográficos, la descentralización y las normas de consenso, las cadenas de bloques están dotadas de un innegable alto nivel de seguridad.

Las cadenas de bloques son una estructura de datos con forma de lista lineal y ordenada de bloques de transacciones y con referencia anterior, puesto que cada bloque guarda la referencia del bloque que le precede (figura 3, [11]).

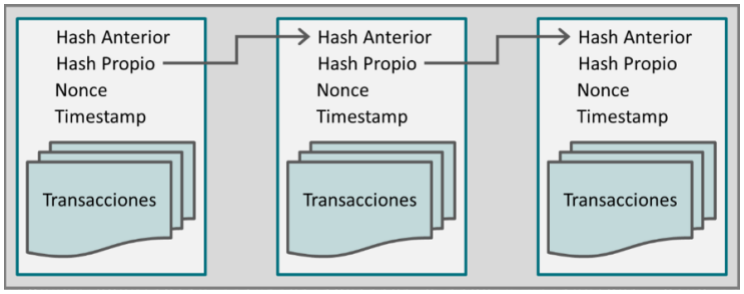

Figura 3: Esquema de la cadena de bloques.

2.1 Componentes de las cadenas de bloques

La tecnología *blockchain*, por lo general, se basa en los siguientes componentes [2]:

- Una **red P2P** (*Peer-To-Peer*) que conecta entre sí a todos los participantes y que propaga las transacciones realizadas y los bloques

de las transacciones verificadas por la *blockchain*. Esta red está basada en un protocolo *gossip* estandarizado, obteniendo así una red eficiente, segura y de baja latencia.

- Mensajes, en forma de **transacción**, que representan transiciones de estado. Las transacciones no tienen por qué ser necesariamente económicas, como en el caso de las criptomonedas. Pueden ser sencillamente transacciones de datos.

- Un conjunto de **reglas de consenso** previamente establecidas y aprobadas que rigen lo que constituye una transacción y lo que hace que una transición de estado se considere válida.

- Una **máquina de estado** que se encarga de procesar las transacciones de acuerdo con las reglas de consenso.

- Una **cadena de bloques**, protegida criptográficamente, que actúa como un diario o un libro contable (*ledger*) de todas las transiciones de estado verificadas y aceptadas. Los bloques están compuestos por un conjunto de transacciones verificadas por el sistema e información relevante sobre el bloque, como un hash de referencia al bloque que le precede, un hash propio, una marca temporal (*timestamp*) etc.

- Un **algoritmo de consenso** que descentraliza el control sobre la cadena de bloques. De esta manera, se obliga a los participantes a tomar parte y cooperar en la aplicación de las reglas de consenso.

- Un **esquema de incentivación** teóricamente sólido (p. ej. costes *proof-of-work* más recompensas por bloque) para asegurar económicamente la máquina de estado en un entorno abierto.

- Uno o más puntos de conexión (físicos o virtuales) donde se ejecute el software de código abierto que hace funcionar la red. También llamados **nodos**, son dispositivos conectados a la red que participan en los procesos previamente mencionados.

Los componentes listados pueden variar en función del tipo de cadena de bloques. Dado que se trata de una tecnología que evoluciona, avanza y mejora constantemente, es probable que algunos de los componentes mencionados sean sustituidos en un futuro próximo por otros componentes más eficaces o que se añadan más a la lista.

2.2 Funcionamiento de las cadenas de bloques

Las redes *blockchain* desde su creación establecen una reglas de consenso que rigen cómo va a funcionar la red y qué se considerará una

transacción válida. Son reglas que todo participante debe aceptar y cumplir para poder formar parte de la red.

Los nodos que se unen a la red participan en conjunto para validar todas las transacciones que cumplan con las reglas de consenso y rechazar el resto. Las transacciones aceptadas se agrupan y se guardan en bloques que, una vez validados, se añaden a la cadena de bloques. Esta acción es definitiva, puesto que una vez en la cadena de bloques, ya no se podrá eliminar o modificar dicho bloque.

Los mensajes en forma de transacciones que se forman en las redes *blockchain* los generan los propios nodos al comunicarse con otros nodos. No tienen por qué ser transacciones económicas, puesto que puede tratarse simplemente de transacciones de datos.

Cada nodo guarda una copia actualizada en tiempo real de la *blockchain*, de tal manera que se garantiza la disponibilidad de la información en todo momento y que la eliminación de un nodo no supone la pérdida de la cadena de bloques de la red. Por otro lado, los nodos, al unirse a la red, descargan e implementan el software que hace funcionar a la red *blockchain* (reglas y algoritmo de consenso). Es así como se consigue que sea una red descentralizada y no dependa de entidades de confianza para funcionar, ya que son los nodos de la red los que hacen que funcione.

Se dice que las cadenas de bloques funcionan como un libro mayor (*ledger*) porque se documentan todas las transacciones validadas desde la creación de la *blockchain*, sin revelar la identidad de los usuarios en momento alguno. Es una forma segura de documentar y evidenciar todas las transiciones de estado, lo cual garantiza una confianza y transparencia para los usuarios contra la que muchos sistemas y aplicaciones actuales no pueden competir.

2.3 Aplicaciones de las cadenas de bloques

Cuando se habla de *blockchain*, a menudo se confunde con *Bitcoin*. Esta criptodivisa, siendo la primera aplicación de las cadenas de bloques y la más conocida, ha supuesto una revolución en la economía y en el mundo en general. No obstante, esta tecnología va más allá, y es que *Bitcoin* no es más que un simple ejemplo de las múltiples posibilidades que ofrece la tecnología *blockchain*. En este apartado, se explicarán algunas de las aplicaciones más destacables de las cadenas de bloques:

- Las **criptomonedas**, a diferencia de las monedas físicas, son enteramente virtuales y están implícitas en las transacciones que transfieren valor de un emisor a un receptor en la mayoría de las redes *blockchain*.

Los propietarios de estas monedas poseen claves que les permiten demostrar su propiedad. Con estas claves se pueden firmar transacciones que desbloquean el valor y gastarlo transfiriéndolo a un nuevo propietario. De esta forma, se pone el control por completo en las manos de cada usuario [3].

Las claves a menudo se almacenan en billeteras digitales en el ordenador o *smartphone* del usuario o incluso en las llamadas "*cold wallets*". Estas últimas se consideran más seguras ante ciberataques, dado que no están conectadas a la red.

Las criptomonedas han logrado crear incertidumbre acerca del futuro del dinero físico. Y es que, al hacer uso de la tecnología de las cadenas de bloques, se elimina la necesidad de un intermediario para realizar las transferencias económicas. Esta aplicación simplifica el sistema actual de las transferencias bancarias y es transparente, lo cual cuestiona la necesidad de la existencia de entidades bancarias.

- Los ***Smart Contracts*** son la segunda aplicación de las cadenas de bloques más relevantes en la actualidad. Plataformas como la conocida *Ethereum* hacen uso de la tecnología *blockchain* para los contratos inteligentes por la alta disponibilidad, transparencia y neutralidad que proporciona [2]. Su objetivo es brindar una seguridad mayor a la que ofrecen los contratos tradicionales y reducir costes de transacción asociados a la contratación.

  Los *Smart Contracts* son programas que viven en un sistema no controlado por ninguna de las partes firmantes y que ejecutan automáticamente la cláusula contractual correspondiente en cuanto se cumple con una condición pre-establecida. No están sujetos a ningún tipo de valoración humana. Por este motivo, se dice que proporcionan un mayor nivel de seguridad y confianza y que eliminan la necesidad de un intermediario de confianza que valore el cumplimiento de los términos del contrato [5].

  Por otro lado, los contratos inteligentes se utilizan a su vez para controlar el derecho de la propiedad inteligente. Se trata de la afirmación digital de que un usuario de una red *blockchain* es el propietario de un activo (y de su clave). Por lo tanto, si el usuario decide vender el activo, el contrato inteligente se encarga de completar el proceso de entregar la clave del vendedor al comprador (nuevo propietario). La propiedad inteligente puede ser aplicable a derechos de autor, marcas, patentes, etc.

- De la mano de los *Smart Contracts*, cabe mencionar la aplicación de las cadenas de bloques a los **bienes inmuebles**. El sistema de confianza inherente de las cadenas de bloques las convierte en la tecnología ideal para el sector inmobiliario. Los contratos inteligentes y las capacidades de contabilidad de las *blockchain* facilitan de manera transparente y eficiente el alquiler, la compra, la inversión e incluso los préstamos [6].

- Las cadenas de bloques pueden ser la mejor opción para la gestión del **proceso de votación**, ya que son transparentes, seguras y rápidas. El sistema de seguridad de las *blockchain* previene las falsas identidades y duplicaciones de votos, a la vez que asegura que la información enviada no se modifica. Además, todos los votos se verifican antes de ser enviados a la cadena de bloques [7].

  De esta manera, se proporciona a los votantes un alto nivel de seguridad, confianza y transparencia, dado que cualquiera podría realizar el recuento por su cuenta.

- En cuanto a la **identidad digital**, las cadenas de bloques podrían aplicarse en este entorno y eliminar la necesidad de utilizar documentos físicos de identificación. Con la tecnología *blockchain* se garantiza la identidad única del usuario y se le protege del robo de identidad, uno de los problemas más importantes en este momento [7].

- Las cadenas de bloques pueden ayudar a frenar los problemas de ***Internet of Things (IoT)***, al proporcionar un enfoque descentralizado. El uso de la tecnología de contabilidad distribuida puede solucionar los problemas de seguridad asociados con el procedimiento centralizado. Por otro lado, los *Smart Contracts* pueden automatizar muchas de las interacciones de *IoT* [7].

  El usuario final también puede beneficiarse de las cadenas de bloques, puesto que sus datos permanecen seguros en la red y él mismo puede decidir compartir los datos en sus propios términos [7].

3. Redes según acceso: públicas, privadas y de consorcio

La tecnología *blockchain*, desde su origen, se planteó como una red abierta y pública. Introdujo en el mundo el concepto de tecnología de contabilidad descentralizada (*Decentralized Ledger Technology*, *DLT*). Este concepto planteó una nueva manera de solucionar los problemas y proporcionó a las organizaciones la habilidad de trabajar sin depender de un entidad centralizada [8].

La tecnología distribuida solventa las desventajas de la centralización. No obstante, genera nuevos problemas a solventar a la hora de aplicar la tecnología *blockchain* a diferentes escenarios. En *Bitcoin*, se utilizaba un algoritmo de consenso ineficiente (*proof-of-work*) que requería a los nodos solucionar cálculos matemáticos consumiendo energía. Al principio, esto no suponía un problema mayor. Sin embargo, a medida que ha ido evolucionando, los cálculos han ido incrementando su dificultad y, por tanto, el tiempo invertido y el consumo de energía. Por este motivo, no es aplicable a cualquier escenario. Los sistemas que requieran ser eficientes a cualquier coste, como por ejemplo entidades bancarias que hacen numerosas transacciones a diario, necesitan un tipo de cadena de bloques más adecuado [8].

La escalabilidad es otro problema de esta primera generación de *blockchains*. No todas las empresas u organizaciones que quieran hacer uso de esta tecnología pueden utilizar una red *blockchain* pública. Existen ciertos datos críticos en las empresas que no deben ser revelados, puesto que podrían ser utilizados por la competencia y les perjudicaría seriamente. Es por esto que surgió la necesidad de crear cadenas de bloques con acceso controlado, es decir, redes *blockchain* en las que la organización decida quién participa en ella.

Debido a estas situaciones, existen tres tipos de redes *blockchain* según su acceso: redes públicas, redes privadas y redes de consorcio. En este capítulo realizaremos un análisis acerca de cada uno de estos tipos.

3.1 Redes *blockchain* públicas

Las redes públicas son uno de los distintos tipos de cadenas de bloques. Se trata de un *ledger* donde cualquier usuario con conexión a internet puede acceder, unirse y hacer transacciones. Es una versión no restrictiva de las cadenas de bloques donde cada par de la red de pares posee una copia de la *blockchain*. Permite que los pares de la red estén interconectados de una manera descentralizada.

3.1.1 Características de las redes públicas

Las redes *blockchain* públicas son redes abiertas, donde cualquier usuario puede unirse y participar en el consenso. Son sistemas totalmente descentralizados, dado que no dependen de ninguna entidad central de confianza, seguras, por su uso de criptografía avanzada y claves privadas para proteger las transacciones, e inmutables, ya que una vez que el bloque de transacciones se añade a la cadena de bloques no puede ser eliminado o modificado.

Las transacciones son anónimas, porque en ningún momento se revela la identidad de los usuarios, pero transparentes, puesto que, una vez que se verifican, se comparten con todos los nodos que forman parte de la red. En estas redes, la verificación de las transacciones se realiza por medio de métodos de consenso, como bien pueden ser las *proof-of-work* o las *proof-of-stake*. Son los propios nodos de la red los que realizan las operaciones de validación de las transacción. Por lo tanto, para que la red funcione es necesario que tenga los pares requeridos participando en la resolución de transacciones.

3.1.2 Ejemplos de las redes públicas

Las redes públicas pertenecen a la primera generación de cadenas de bloques. La primera aplicación de la tecnología *blockchain* fue ***Bitcoin***.

Figura 4: Logotipo de *Bitcoin.*

Bitcoin es una colección de conceptos y tecnologías que forman las bases de un ecosistema de dinero digital. Las unidades de la criptodivisa llamada "*bitcoin*" se utilizan para transferir valor entre los participantes de la red. Los usuario se comunican principalmente por el protocolo *bitcoin* vía internet, aunque se pueden utilizar otras redes de transporte. La pila del protocolo *bitcoin*, disponible como software de código abierto, puede ser ejecutada en un amplio rango de dispositivos, incluyendo ordenadores portátiles y smartphones, haciéndola una tecnología fácilmente accesible.

Los usuarios de esta red pueden transferir esta criptomoneda por la red y hacer prácticamente lo mismo que se puede hacer con el dinero físico, incluyendo comprar y vender bienes, enviar dinero a otras personas u organizaciones o incluso dar créditos. Los *bitcoins* se pueden comprar, vender e intercambiar por otras criptodivisas en sitios especializados. Por estos motivos se considera como la forma perfecta de dinero para internet porque es rápido, seguro y sin fronteras [3].

Otro ejemplo relevante de las redes *blockchain* públicas es ***Ethereum***. Se trata de una infraestructura informática descentralizada globalmente, de código abierto, que ejecuta programas llamados *Smart Contracts*. Hace uso de una cadena de bloques para sincronizar y almacenar los cambios de estado del sistema, junto con una criptomoneda, llamada "*ether*", para medir y limitar los costos de los recursos de ejecución [2].

Figura 5: Logotipo de *Ethereum*.

En términos más técnicos, *Ethereum* es una máquina de estados determinista pero prácticamente ilimitada, que consiste en un estado único accesible globalmente y una máquina virtual que aplica cambios a ese estado. Esta infraestructura es programable, lo cual permite a los desarrolladores construir potentes aplicaciones descentralizadas (*dapps*) con funciones económicas integradas. *Ethereum* proporciona una alta disponibilidad, auditabilidad, transparencia y neutralidad, del mismo modo que reduce o elimina la censura y reduce ciertos riesgos de contraparte [2].

XRP Ledger es otro claro ejemplo de las cadenas de bloques públicas. Este proyecto surgió con la intención de dar una solución a los problemas de eficiencia de *Bitcoin*. *XRP Ledger* es un sistema de pagos en línea, impulsado por una comunidad descentralizada. Es una red P2P abierta que gestiona la cadena de bloques a la que cualquiera puede unirse. La criptodivisa utilizada en esta red se llama "*XRP*" [9].

Figura 6: Logotipo de *XRP Ledger*.

Este sistema posee un procesamiento de transacciones resistente a la censura y un algoritmo de consenso rápido y eficiente. No requiere el tiempo y la energía de "minería" que requieren *Bitcoin* o *Ethereum*. En lugar de *proof-of-work* o *proof-of-stake*, el algoritmo de consenso de XRP Ledger utiliza un sistema en el que cada participante posee un conjunto superpuesto de

“validadores de confianza”, los cuales acuerdan de manera eficiente qué transacciones ocurren en qué orden.

3.1.3 Funcionamiento de las redes públicas

Como se ha mencionado anteriormente, la tecnología *blockchain* es de carácter descentralizado, distribuida, de consenso, segura y, en este caso, abierta. Todo ello se debe a su funcionamiento y diseño tan característicos.

Las redes *blockchain* son *Peer-To-Peer*, descentralizadas y altamente escalables, de tal forma que la integridad de la red se basa en un mecanismo de consenso y no en terceros. En otras palabras, no dispone de una infraestructura en la que participe un organismo de confianza, como bien pudiera tratarse de una entidad bancaria, como intermediario sino que los propios clientes de la red son quienes realizan todas las funciones, siguiendo unas reglas de consenso establecidas en la red. Al tratarse de una red P2P, se disminuye la posibilidad de que un único individuo o grupo de individuos controlen el sistema por completo. Todos los participantes de la red se adhieren a los mismos protocolos por igual. Por otro lado, la red carece de puntos críticos o centrales de vulnerabilidad que podrían ser explotados por atacantes, como en el caso de las redes centralizadas.

Se dice que la red es abierta dado que cualquier dispositivo que descargue el programa para la *blockchain* correspondiente, puede participar en la red como un nuevo nodo. Entre los nodos de las redes con un algoritmo de consenso de prueba de trabajo, existen los nodos mineros o validadores que son los encargados de verificar las transacciones. [3] Se trata de ordenadores (de elevada potencia en el caso de redes potentes como *Bitcoin*) que trabajan sin descanso para validar las transacciones (resolviendo problemas matemáticos altamente complejos) por referencia a las reglas de consenso de la *blockchain*. Las transacciones se agrupan en bloques, lo cual conlleva un enorme trabajo de computación para probarse, pero escaso trabajo de verificarse como probado. Por lo tanto, la minería o validación es un sistema de trabajo que garantiza la seguridad de la cadena de bloques al rechazar las transacciones no consideradas válidas o mal hechas. Del mismo modo, para rentabilizar el trabajo de la minería se otorgan recompensas en forma de criptomoneda a los mineros. En algunas *blockchains* hay un límite de emisión respecto de su criptodivisa y en otras no. La cantidad otorgada como recompensa puede variar dependiendo de la red; en unas se disminuye de manera automática y en otras a partir de decisiones de los desarrolladores. De esta forma, la minería de la *blockchain* crea un delicado equilibrio entre el costo y la recompensa. En *Bitcoin*, por ejemplo, cada minero exitoso recibe una recompensa proporcional a su participación en la creación del bloque, siempre y cuando haya validado correctamente todas las transacciones, satisfaciendo las normas de consenso. El costo de la minería será la electricidad utilizada por el minero durante la resolución de los problemas matemáticos. Este equilibrio

entre costo y recompensa, proporciona seguridad a las cadenas de bloques, donde no existe una autoridad central. En cuanto a las transacciones, son irreversibles. Es decir, una vez realizadas es imposible modificarlas, anularlas o revertirlas.

Las transacciones se generan constantemente en la red desde los nodos y aguardan a la creación de nuevos bloques en grupos temporales de transacciones no verificadas. A medida que los mineros van creando nuevos bloques, estas transacciones se agregan al bloque, priorizadas las que tienen la tarifa más alta, y después intentan probar la validez del bloque con el algoritmo de minería de prueba de trabajo (*proof-of-work*). Cada bloque, a parte de las transacciones, guarda la referencia del bloque que le precede (en forma de función hash) y su propia referencia (también una función hash). En redes como *Bitcoin*, los mineros añaden además una transacción especial en su bloque, concretamente una que les paga la recompensa del bloque más la suma de las tarifas de transacción de todas las transacciones incluidas en el bloque. En caso de que el bloque sea validado satisfactoriamente, cobrarán la recompensa mentada y este bloque se añadirá a la cadena de bloques global. En la figura 7 [10], se puede observar un esquema del proceso completo.

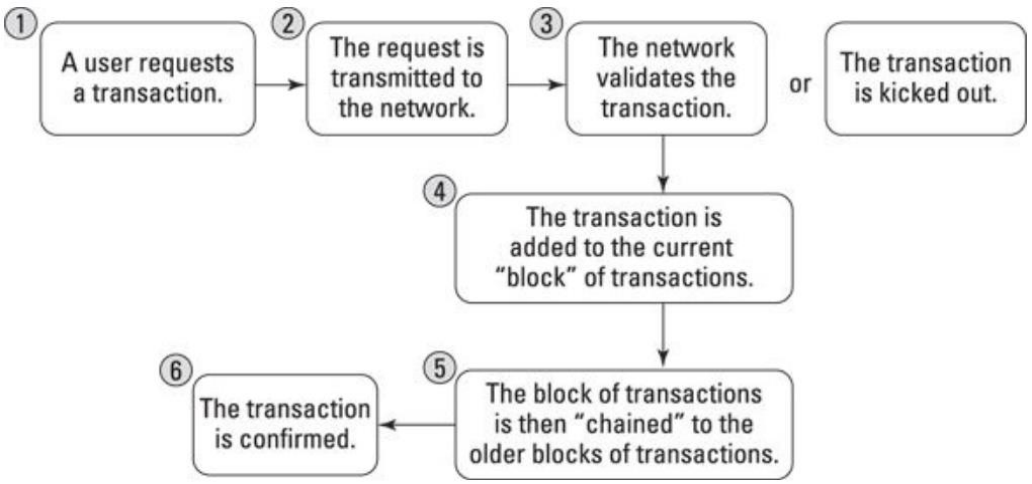

Figura 7: Proceso de validación de un bloque de transacciones.

En ocasiones, se validan y se añade más de una rama de bloques al último bloque de la cadena, generando un *fork* temporal en la *blockchain*. Como se ha mencionado anteriormente, las cadenas de bloques son un estructura de datos en forma de lista lineal, por lo que debe existir una única línea de bloques. El algoritmo de la *blockchain* está preparado para seleccionar cuál de los "hijos" debe ser el elegido para seguir la rama y ser el predecesor del "padre". A los bloques no seleccionados se les llama bloques huérfanos (en color lila en la figura 8 [1]). Este funcionamiento respalda y garantiza la integridad de la que presume la tecnología de las cadenas de bloques, ya que desde su creación con el bloque origen (en verde en la figura 8) no se elimina ni modifica ningún bloque de la cadena y todos guardan un orden cronológico. Por estos motivos se considera a las cadenas de bloques como un *ledger* transparente, un libro contable con todas las transacciones documentadas y

compartidas con todos los miembros de la red. Por lo tanto, las cadenas de bloques permiten llevar a cabo una contabilidad pública de las transacciones realizadas en la red de un modo transparente, minimizando la posibilidad de fraude y previniendo la pérdida de datos.

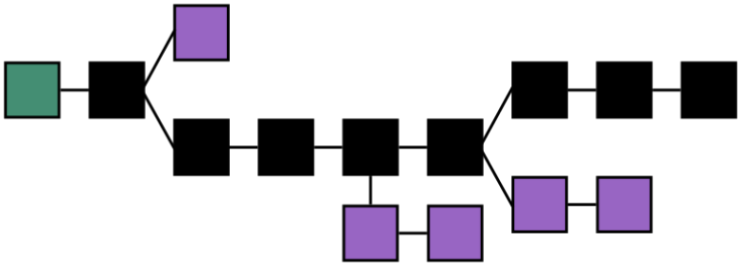

Figura 8: Representación de una cadena de bloques.

Cada nodo de la red guarda una copia actualizada en tiempo real de la cadena de bloques; no existe una copia centralizada. Siempre que un nodo valida un bloque nuevo, actualiza su copia de la *blockchain* y distribuye dicha actualización al resto de nodos de la red, de tal forma que todos los pares obtienen la misma versión. Los nodos poseen una cartera (*wallet*) en la que almacenan las criptomonedas que obtienen mediante las transacciones o mediante la minería.

Los sistemas de seguridad de las cadenas de bloques incluyen el uso de métodos criptográficos como las claves públicas y privadas. La clave pública correspondería a una dirección en la cadena de bloques. La clave privada funcionaría como una contraseña, la cual permitiría al propietario el acceso a sus activos digitales y firmar transacciones. La posesión de la clave privada permite al usuario demostrar que es el propietario de los activos.

Como se ha comentado previamente, cada bloque de la cadena contiene un conjunto de transacciones verificadas junto con información relativa a estas transacciones y al propio bloque. Esta información incluye el hash del bloque que precede al bloque actual y el hash del bloque actual. A parte de esto, se almacena también el hash raíz (*root hash*) del árbol de *Merkle*.

El árbol de *Merkle* es una estructura ramificada utilizada en *blockchains* como *Bitcoin* para resumir y verificar de manera eficiente la integridad de los conjuntos de transacciones [3]. Se trata de un árbol binario que contiene hashes criptográficos. Su funcionamiento consiste en generar un hash para cada transacción del bloque (hojas), combinar estos hashes en pares y generar nuevos hashes de las parejas resultantes. Este procedimiento se repite hasta lograr un único hash (raíz) de esta estructura con forma de árbol. En la figura 9 [1], los valores L1, L2, L3 y L4 representarían las transacciones verificadas del bloque de la *blockchain*. Se puede apreciar cómo se generan y combinan los hashes sucesivamente hasta lograr el "*Top Hash*", también llamado hash raíz. El algoritmo hash criptográfico utilizado en los árboles *Merkle* de *Bitcoin* es *SHA256* aplicado dos veces, también conocido como doble-*SHA256* [3].

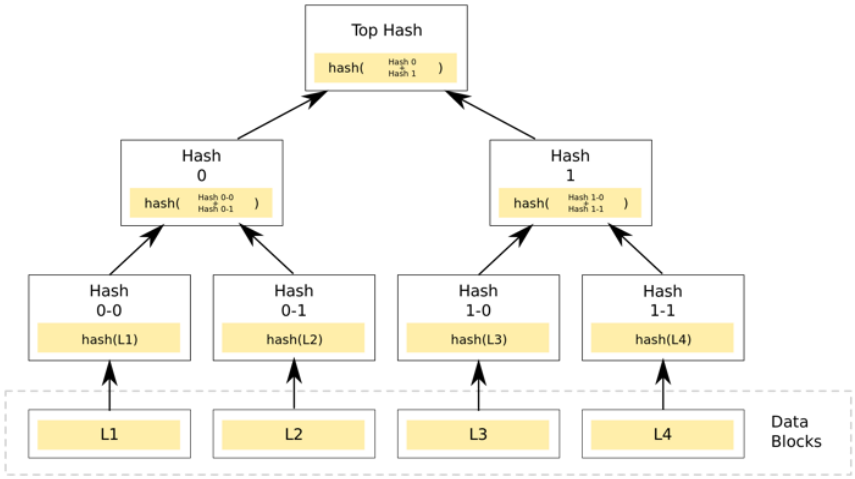

Figura 9: Estructura de un árbol *Merkle*.

Los árboles *Merkle* permiten resumir todas las transacciones de un bloque, produciendo una huella digital general de todo el conjunto de transacciones, proporcionando un proceso muy eficiente para verificar si una transacción está incluida en un bloque o no.

3.2 Redes *blockchain* privadas

Las organizaciones que quieren utilizar la tecnología de las cadenas de bloques, en muchas ocasiones, no pueden permitirse ser totalmente transparentes, dado que poseen ciertos datos que son críticos para el funcionamiento de la empresa y que no pueden ser revelados. Debido a este tipo de situaciones, surgieron las redes *blockchain* privadas.

Podrían ser definidas como las redes *blockchain* que funcionan en un ambiente restringido, como una red cerrada. Son cadenas de bloques controladas por una sola entidad. Este tipo de redes son la mejor opción para organizaciones que quieren utilizarlas para casos de uso internos [8].

3.2.1 Características de las redes privadas

Las redes *blockchain* privadas están gobernadas por una entidad u organización, que se encarga de controlar y decidir quién puede participar en la red y quién no. Por tanto, no es una red totalmente descentralizada, ya que una sola autoridad supervisa toda la red.

En las redes privadas, únicamente los individuos o entidades seleccionados tendrán derecho a ver los nodos de la red y a realizar transacciones. Estas redes, al igual que las redes *blockchain* públicas, ofrecen transparencia, confianza y seguridad a los participantes seleccionados. Esto las convierte en redes altamente eficientes, rápidas en las transacciones y con bajos costes de transacción. Poseen una arquitectura robusta y un diseño escalable. Muchas de las redes privadas no utilizan criptomonedas.

3.2.2 Ejemplos de las redes privadas

Muchas *blockchains* han sido adaptadas y reestructuradas para un uso empresarial privado. A diferencia de ellas, plataformas como ***Hyperledger Fabric*****,** iniciada por la Fundación Linux, han sido diseñadas desde el principio para uso empresarial. Esta plataforma de libro mayor distribuido (*DLT*) de código abierto y de grado empresarial, está diseñada para su uso en contextos empresariales y ofrece algunas capacidades de diferenciación clave sobre otras plataformas populares de contabilidad distribuida o *blockchain* [12].

Figura 10: Logotipo de *Hyperledger Fabric*.

Hyperledger Fabric es una cadena de bloques de carácter privado que tiene una arquitectura modular con una definición de roles entre los nodos que forman parte de la infraestructura. Permite la creación de contratos inteligentes (llamados *chaincode* en *Fabric*) en lenguajes de programación de uso general (como *Java*, *NodeJS* o *Go*). Asimismo, ofrece compatibilidad con protocolos de consenso conectables, que permiten que la plataforma se pueda personalizar de una manera más eficaz para poder adaptarse a casos de uso particulares y modelos de confianza [12].

Otro ejemplo de gran relevancia en el ámbito de las redes de cadenas de bloques privadas es ***Quorum***. Se trata de una *blockchain*, creada por *JP Morgan*, basada en *Ethereum*, centrada en la empresa y dirigida al sector financiero.

Figura 11: Logotipo de *Quorum*.

En el sector financiero se requieren cadenas de bloques rápidas, con un alto rendimiento y que funcionen mientras se mantiene bajo control la privacidad de los participantes. *Quorum* ofrece un procesamiento y rendimiento de alta velocidad al mismo tiempo que mantiene en el anonimato los detalles de la transacción. Al estar basado en *Ethereum*, utiliza contratos inteligentes para facilitar las transacciones dentro de la cadena de bloques. El objetivo de esta plataforma es la implementación de una iniciativa de red global de pagos y ayudar a las entidades bancarias a hacer uso de redes distribuidas. Este proyecto pretende aumentar la eficiencia, agilizar los pagos globales y habilitar el seguimiento de estado sin interrupciones, entre otros [13].

La *blockchain* ***Corda***, al igual que *Quorum*, está orientada hacia el sector financiero. Es un software de registro distribuido que procesa y registra datos para promover un entorno de red descentralizado. También gestiona contratos inteligentes. En cuanto a las transacciones, *Corda* no las comparte con todos los nodos de la red, sino que las comparte entre los nodos que tienen transacciones en común. De este modo, mantiene la privacidad entre las partes. Para el consenso de transacciones, únicamente se realiza entre las partes involucradas y por un tercer nodo llamado “notario”. Este nodo es el encargado de justificar que la transacción se ha realizado una sola vez y que se ha ejecutado correctamente, antes de quedar grabada en la cadena de bloques. Sin embargo, en *Corda* se mantiene la ventaja principal de las *DLT*s: la inmutabilidad. Una vez que el contrato ha sido gestionado, éste puede servir como base legal encaso de disputas [14].

Figura 12: Logotipo de *Corda*.

3.2.3 Funcionamiento de las redes privadas

El funcionamiento de todas las *blockchain* es muy similar. Es una tecnología que se basa en una red P2P para garantizar la descentralización y la interconectividad entre todos los nodos de la red. Dentro de esa plataforma existen las normas y los algoritmos de consenso, los cuales se encargan de establecer y garantizar el correcto funcionamiento de la cadena de bloques.

En las *blockchains* de carácter privado, la gobernanza de la red no depende de todos los participantes de la red, depende de una única entidad u organización. Esta organización es la encargada de supervisar la red, de establecer las normas de consenso y de gestionar el acceso a la red. En una red *blockchain* privada el acceso es limitado y solamente los participantes

seleccionados tienen derecho a participar y a realizar transacciones. Al ser una red cerrada, los participantes no gozan del anonimato de las redes públicas, ya que tendrán algún tipo de esquema de autorización a la identidad para ingresar a la plataforma [15].

Estas cadenas de bloques están pensadas para el sistema de redes internas de una empresa. Por tanto, debe existir confianza entre todos los nodos para garantizar un correcto funcionamiento. Estos nodos deben cumplir las reglas de consenso.

Al tener un acceso limitado, en las redes privadas hay un número controlado de participantes. Esto permite controlar las tareas que se realizan y, por tanto, se evita el consumo de recursos adicionales y la ralentización de la plataforma. Para ello, las cadenas de bloques privadas hacen uso de protocolos de consenso ecológicos para llegar a un acuerdo. Es por esto que se consideran redes altamente eficientes.

Por otro lado, la privacidad y la confidencialidad juegan un papel importante en estas redes. Son dos de las características más relevantes para las empresas que tratan de utilizar estas cadenas de bloques, dado que gestionan información crítica que de ser revelada provocaría grandes pérdidas para la empresa. Para ello, algunas redes privadas, como *Hyperledger Fabric*, permiten la confidencialidad a través de su arquitectura de canales y la función de datos privados. En los canales, los usuarios de una red de *Fabric* establecen una subred donde cada miembro tiene visibilidad de un conjunto específico de transacciones. De este modo, únicamente los nodos que participan en ese canal tienen acceso al contrato inteligente (*chaincode*) y a los datos transferidos, preservando así la privacidad y confidencialidad de ambas partes. Los datos privados permiten recopilaciones entre miembros en un canal. Esto permite, en gran parte, la misma protección que los canales, pero sin la sobrecarga de mantenimiento de crear y mantener un canal separado [12]. En plataformas como *Quorum*, todas las transacciones, incluidos los contratos inteligentes, son validadas dentro de la *blockchain*. Los contratos inteligentes se ejecutan utilizando la capa de seguridad de conocimiento cero, que garantiza que la liquidación privada se realice sin ningún compromiso [13].

Las cadenas de bloques privadas, generalmente, utilizan *Smart Contracts*. Estos contratos inteligentes funcionan como una aplicación distribuida y confiable que obtiene su seguridad y confianza de la propia *blockchain* y del consenso subyacente entre los nodos de la red. En la mayoría de plataformas con capacidad para contratos inteligentes, se ejecutan en gran cantidad simultáneamente en la red. Estas plataformas siguen una arquitectura de orden-ejecución en la que el protocolo de consenso valida y ordena las transacciones y luego las comparte con todos los nodos pares. Después cada par ejecuta las transacciones secuencialmente [12].

Los *Smart Contracts* que se ejecuten en una cadena de bloques que siga una arquitectura de ejecución de órdenes, deben ser deterministas. De lo contrario, resultará muy difícil alcanzar un consenso. Para abordar este problema, muchas plataformas requieren que los contratos inteligentes estén

escritos en un lenguaje específico del dominio, de tal forma que las operaciones no deterministas se puedan eliminar. Esto requiere que los desarrolladores aprendan un nuevo lenguaje y puede acarrear errores de programación. Por este motivo, *Hyperledger Fabric*, para ser una opción más competitiva, permite la creación de *Smart Contracts* en lenguajes de programación de uso general [12].

En las redes privadas el rendimiento es muy alto. Se realiza un mayor número de transacciones por segundo que en las redes públicas, es decir, son más rápidas debido al reducido número de participantes. Esto implica que la red tarda menos tiempo en llegar a consenso. Por otra parte, estas cadenas de bloques son más escalables porque solamente unos pocos nodos están autorizados a validar transacciones. Por lo tanto, no importa que la red crezca, puesto que funcionará a su velocidad y eficiencia anteriores. La clave de este funcionamiento reside en el aspecto de centralización de la toma de decisiones [8].

3.3 Redes *blockchain* de consorcio

En ocasiones es necesario llegar a un punto intermedio entre *blockchains* públicas y privadas para satisfacer las necesidades de una organización. Es aquí donde aparece el tercer tipo de red *blockchain* en función de su acceso: Las redes de consorcio. Son una solución creativa para aquellas empresas u organizaciones que necesitan funciones tanto de cadenas de bloques públicas como privadas. También pueden llamarse “cadenas de bloques federadas”.

En este tipo de redes, algunos de los aspectos de las organizaciones se hacen públicos, mientras que otros se mantienen privados. Por lo general, un consorcio *blockchain* está administrado por más de una organización.

3.3.1 Características de las redes de consorcio

En las cadenas de bloques de consorcio los procedimientos de consenso están controlados por los nodos preestablecidos en la red. Al igual que las redes privadas, éstas tampoco están abiertas al público; todos los participantes son seleccionados por las autoridades que controlan la red. Sin embargo, se mantiene la naturaleza descentralizada de las redes públicas, puesto que no hay una única fuerza que controle la *blockchain*. Las cadenas de bloques de consorcio están administradas por más de una organización [8].

Este tipo de redes *blockchain* ofrecen todas las características de las redes privadas, incluidas la transparencia, la privacidad y la alta eficiencia, sin

que una de las partes tenga poder de consolidación. En otras palabras, es una combinación de las mejores características de ambos tipos de redes de cadenas de bloques.

3.3.2 Ejemplos de las redes de consorcio

Las cadenas de bloques de consorcio son proyectos que involucran a más de una empresa que, en la mayoría de los casos, pertenecen al sector financiero. Uno de los ejemplos más relevantes es *Voltron*.

Figura 13: Logotipo de *Voltron*.

Este proyecto, impulsado por las empresas *R3* y *CryptoBLK* y que recibe soporte técnico de *Microsoft Azure*, consiste en una red *blockchain* de consorcio en la que participan doce bancos internacionales: *HSBC*, *BBVA*, *BNP Paribas*, *Scotiabank*, *ING*, *U.S. Bank*, *SEB*, *Bangkok Bank*, *CTBC Bank*, *Natwest*, *Mizuho*, e *Intesa Sanpaolo*. En esta red se utiliza *Corda*, ya que esta *blockchain* está desarrollada por *R3* [16].

Otro buen ejemplo de este tipo de redes es *Marco Polo*. Se trata de otro proyecto de *R3*, esta vez en colaboración con *TradeIX*, en la que participan diez entidades financieras: *SMBC*, *Bangkok Bank*, *OP Financial*, *DNB*, *ING*, *Commerzbank*, *Standard Chatered*, *Natixis*, *BNP Paribas* y *NatWest* [16].

Figura 14: Logotipo de *Marco Polo*.

En la figura 15 [17], podemos observar más proyectos de cadenas de bloques de consorcio (*Batavia*, *We.Trade* y *HKTFP*), a parte de los ya comentados, en los cuales participan otras empresas relevantes como: *CaixaBank*, *Banco Santander*, *KBC*, *Deutsche Bank*, *Nordea* o *Bank of China*.

Figura 15: Proyectos de *blockchains* de consorcio.

3.3.3 Funcionamiento de las redes de consorcio

Las cadenas de bloques de consorcio funcionan de una manera muy similar a las redes *blockchain* privadas. Los algoritmos de consenso estándar basados en *proof-of-work* o en *proof-of-stake*, están pensados para redes públicas, en las cuales no hay confianza entre los nodos. En las redes privadas y de consorcio, todos los nodos se conocen entre sí, puesto que antes de unirse a la red tienen que identificarse [16].

En las redes de consorcio, al haber menos participantes de los que podría haber en una red pública, el algoritmo de consenso se basa en un sistema de votación. Este sistema asegura una baja latencia y una gran velocidad en la red.

Los procedimientos de consenso están controlados por los nodos preseleccionados. Para garantizar una funcionalidad propicia, el consorcio tiene "nodos validadores", que pueden realizar dos funciones principalmente: validar transacciones y también iniciar o recibir transacciones.

Todos los nodos de la red pueden leer o escribir transacciones, pero solamente los nodos validadores pueden validar transacciones. Por otra parte, ningún nodo puede añadir un bloque a la cadena de bloques por sí mismo. Para ello, debe someterse a una votación en la que todos los nodos confirmen y den su consentimiento de que el bloque sea añadido a la *blockchain*. En caso

de que un solo nodo no esté de acuerdo, el bloque no se añadirá a la cadena. Debe haber consenso.

Este método de votación se conoce como *proof-of-vote*. Su propósito principal es hacer un seguimiento de los nodos seleccionados, ya que cada nodo tendrá que votar para validar los bloques. El número de votos requerido será predeterminado por los desarrolladores de la red. Si no se alcanza un consenso absoluto en ese número de votos, no se añade el bloque a la cadena [16]. Mediante el uso de este mecanismo, las organizaciones participantes se aseguran de que cada bloque sea correcto y no contenga actividades ilegales.

Al igual que las redes privadas, estas redes son rápidas, dado que tienen un número determinado de participantes y que los nodos encargados de validar las transacciones (nodos validadores) son siempre los mismos. Esto permite una rápida y eficiente distribución del trabajo de validación. Tampoco habrá, por tanto, problemas de escalabilidad, ya que la red siempre controlará la cantidad de nodos validadores. Por otro lado, el consumo de energía en las cadenas de bloques de consorcio durante los protocolos de consenso para verificar las transacciones es muy bajo. Esto permite que estas *blockchain* sean una opción muy eficiente, rentable y segura para las organizaciones [18].

4. Redes según privilegios: *permissioned* y *permissionless*

Las cadenas de bloques, en su origen, fueron desarrolladas como una tecnología pública. Una red distribuida y descentralizada que elimina la necesidad de una autoridad central de control, que se basa en unas normas de consenso para garantizar el correcto funcionamiento del sistema, y que funciona como un libro mayor (*ledger*) seguro y transparente para sus usuarios.

Sin embargo, a medida que esta tecnología ha ido creciendo y demostrando su potencial, ha evolucionado para adaptarse a nuevos casos de uso, dando lugar a la aparición de las redes privadas y de consorcio.

Esta clasificación se realiza desde el punto de vista del acceso de las redes. No obstante, las redes también pueden ser clasificadas desde el punto de vista de los privilegios. En este capítulo se procederá a analizar las redes de cadenas bloques con permisos o "*permissioned blockchains*" y las cadenas de bloques sin permisos o "*permissionless blockchains*".

4.1 Redes *blockchain* con permisos: *Permissioned*

Las redes *blockchain* con permisos (también llamadas *permissioned blockchains* o cadenas de bloques autorizadas) son uno de los dos tipos de cadenas de bloques en función de los privilegios. A menudo se suele pensar que las redes con permisos solamente pueden ser redes privadas. No obstante, pueden adaptarse tanto a redes privadas como públicas como de consorcio.

El objetivo de las redes con permisos es limitar los privilegios de los usuarios. Estos privilegios pueden afectar al acceso a la red, aunque no es su único propósito, puesto que también pueden determinar qué nodos pueden validar transacciones o ver ciertos datos de la red. En otras palabras, se pretende que las redes no pertenezcan al público y que sea una autoridad central la que gestione estos privilegios y tome las decisiones. Esto las convierte en redes parcialmente descentralizadas.

Este tipo de redes pueden ser utilizadas por entidades bancarias, empresas u otras instituciones que no tengan problemas para cumplir con las regulaciones pero que necesiten proteger cierta información crítica para ellas.

4.1.1 Características de las redes con permisos

En este tipo de cadenas de bloques la descentralización puede variar. Es decir, dependiendo del tipo de acceso que se permita en estas redes pueden ser totalmente descentralizadas, parcialmente descentralizadas o centralizadas (aunque esto va en contra de los principios de la tecnología de las cadenas de bloques). La autoridad que gestiona los privilegios de la red es la encargada de tomar la decisión de quién puede unirse a la red y quién no. Esta decisión deberá ser la que mejor se adapte a los intereses del propietario. La descentralización de este tipo de redes es más flexible, ya que en la mayoría de casos, los algoritmos de consenso son elegidos por la autoridad central [19].

En cuanto a la gobernanza, estas redes están controladas por una organización. Ésta selecciona a los miembros de la red y se asegura de que la mayor parte de la red tenga una naturaleza descentralizada, aunque siempre con algún control central. En estas redes la autoridad puede decidir incluir nodos validadores para verificar las transacciones [19].

Las cadenas de bloques con permisos son eficientes en lo que a velocidad de transacciones y escalabilidad se refiere, ya que tienen un mayor control sobre los nodos que participan en los procesos de validación.

El anonimato de los usuarios en este tipo de redes no es del todo posible, ya que los nodos que se unen a la red deben ser conocidos por la autoridad central. En cuanto a la privacidad de los nodos, la identidad individual de cada uno está protegida con criptografía avanzada y, en muchos casos, únicamente la autoridad central conoce a los usuarios. Por otro lado, la transparencia del sistema dependerá de las necesidades de la organización central [19].

4.1.2 Ejemplos de las redes con permisos

Un buen ejemplo de las cadenas de bloques con permisos o *permissioned blockchains* es la plataforma *EOS*. Este proyecto de la empres *Block.one* plantea la creación de un software que presenta una arquitectura de *blockchain* diseñada para permitir el escalamiento vertical y horizontal de aplicaciones descentralizadas (*dapps*) [20].

Esta cadena de bloques utiliza un algoritmo de consenso basado en pruebas de participación delegada o *delegated-proof-of-stake* (DPOS), una variación de las *proof-of-stake*. La producción de bloques no está permitida para cualquier nodo, dado que se añaden a la cadena de bloques siguiendo un sistema de votación.

Los usuarios de *EOS* no deben pagar por utilizar la red, lo que implica que no hay pago de comisiones por transacciones dentro de ella. No obstante, sí que consta de ciertos activos por los que hay que pagar con *tokens* de la propia red [20].

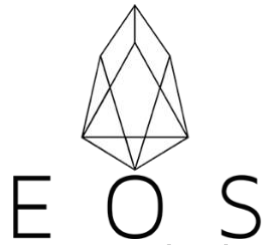

Figura 16: Logotipo de *EOS*.

Otro ejemplo de *permissioned blockchains* es *Sovrin*. Esta red es una cadena de bloques pública con permisos. Esto significa que cualquiera puede hacer uso del libro mayor de *Sovrin* para realizar transacciones, pero no todos los nodos pueden operar la red y ejecutar los nodos validadores. En esta red solamente las nodos de confianza (llamados *Stewards*) pueden ejecutar la red de nodos validadores que logran el consenso de las transacciones en el *ledger* [21].

Figura 17: Logotipo de *Sovrin*.

Las redes *Hyperledger Fabric* o *Quorum*, comentadas en apartados anteriores también son ejemplos de redes de cadenas de bloques con permisos.

4.1.3 Funcionamiento de las redes con permisos

En este tipo de redes existe una autoridad central encargada de gestionar todos los permisos de la cadena de bloques. También es la encargada de seleccionar qué nodos pueden unirse a la red, de tal manera que se controla el grado de descentralización. Son redes que se pueden adaptar a todos los requerimientos y preferencias de las organizaciones que las gobiernan.

La autoridad central posee el control sobre qué nodos pueden validar las transacciones y, generalmente, los bloques se añaden a la cadena de bloques

por métodos de consenso como la votación. Esto proporciona a los usuarios una mayor velocidad de validación de transacciones, porque no depende de todos los nodos de la red. Las *blockchain* con permisos poseen también una mayor escalabilidad que las redes sin permisos.

4.2 Redes *blockchain* sin permisos: *Permissionless*

Las redes *blockchain* sin permisos (también llamadas *permissioless blockchains*) son el segundo de los dos tipos de cadenas de bloques en función de los privilegios. Son aquellas en las que no hay restricciones para que las entidades de la red puedan procesar las transacciones y crear bloques. En la mayoría de redes de este tipo se hace uso de monedas digitales o *tokens* como incentivos para que los usuarios mantengan la red.

En una cadena de bloques sin permisos, un usuario puede crear una dirección personal y después interactuar con la red, ya sea ayudando a validar transacciones como simplemente enviando transacciones a otro usuario de la red. Los datos dentro de estas cadenas de bloques están disponibles para todos los participantes de la red y todos ellos guardan una copia en tiempo real de la versión más actual de cadena de bloques [22].

4.2.1 Características de las redes sin permisos

Una característica asociada a este tipo de redes es que suelen hacer uso de *tokens* de utilidad o criptomonedas como método de incentivación para que los usuarios mantengan la red. El valor de estas monedas digitales o *tokens* puede crecer o decrecer en función de la relevancia y estado de la cadena de bloques a la que pertenecen.

Las cadenas de bloques sin permisos son transparentes. Dado que no existe una autoridad central que controle el acceso a la información dentro de la red, todos los usuarios pueden acceder a toda la información, incluyendo direcciones de otros nodos, las transacciones y los bloques. De esta manera, se incentiva la confianza entre los nodos de la red.

La gobernanza de estas cadenas de bloques no depende de una entidad central. El funcionamiento de las redes se controla mediante el consenso entre los nodos que las forman. Esto implica que cualquier cambio en la red requerirá que al menos el 51% de los participantes estén de acuerdo y den su consentimiento [22].

4.2.2 Ejemplos de las redes sin permisos

Los ejemplos más conocidos de las redes *blockchain* sin permisos son *Bitcoin* y *Ethereum*. Estos proyectos han servido de referentes para otros proyectos como el de la criptomoneda *Monero*. Esta *blockchain* tiene como objetivo principal la protección transacciones.

Figura 18: Logotipo de *Monero*.

Los principios de *Monero* son la descentralización de la red (su red y su *ledger* están distribuidas globalmente), la seguridad financiera (posee mecanismos de criptografía incorruptible), la privacidad financiera (las transacciones y las identidades de los usuarios no se pueden rastrear) y la fungibilidad (activos indistinguibles e intercambiables) [23].

Dash es otro buen ejemplo de las redes *blockchain* sin permisos. Se trata de un proyecto de pagos con criptomonedas (de mismo nombre) que busca ofrecer un sistema sencillo, ágil, seguro y con bajas comisiones.

Figura 19: Logotipo de *Dash*.

Esta *blockchain* ofrece dos servicios de pago únicos: *InstantSend*, que permite realizar transacciones prácticamente instantáneas, y *PrivateSend*, que ofrece un nivel de privacidad mejorado. Por otro lado, *Dash* implementa una red de dos niveles: uno en el que la creación de los bloques y la seguridad de la red dependen de los mineros y otro en el que el consenso está constituido por nodos completos llamados "*masternodes*". Estos nodos maestros ofrecen los servicios *InstantSend* y *PrivateSend* y participan en la gobernanza [24].

4.2.3 Funcionamiento de las redes sin permisos

Las redes de cadenas de bloques sin permisos no están controladas por ninguna autoridad central; son redes descentralizadas en las que los nodos se encargan del mantenimiento de la red. Es decir, son cadenas de bloques de funcionamiento público. En la mayoría de estas redes se hace uso de criptodivisas o *tokens* como método de incentivación para que los nodos participen en los procesos de validación de transacciones y la creación de bloques. Generalmente, el funcionamiento de estas cadenas de bloques consiste en el uso de algoritmos de consenso basados en *proof-of-work* o *proof-of-stake*.

Todos los nodos pueden realizar y validar transacciones; no hay una autoridad que conceda permisos para realizar estos procesos. Por lo tanto, cualquier transacción válida enviada a la red será correctamente ejecutada, sin depender de la decisión de una entidad central.

En este tipo de cadenas de bloques participan un gran número de nodos. Todos ellos pueden ser anónimos, ya que no es necesario identificarse para obtener una dirección y realizar transacciones. Asimismo, cada nodo guarda una copia en tiempo real de la cadena de bloques actualizada.

La red es totalmente transparente, puesto que cualquier nodo que forme parte de la red pueden acceder al *ledger*. Sin embargo, no se revelan datos relativos a la identidad de los emisores o receptores de las transacciones, ya que son redes que pretenden preservar la privacidad de los usuarios en todo momento.

Para realizar cambios en estas redes, normalmente se requiere el consenso de, al menos, el 51% de los nodos.

5. Clasificación de distintas *blockchains*

Las cadenas de bloques surgieron como una tecnología innovadora y revolucionaria, que permite mantener registros distribuidos y descentralizados de transacciones digitales en forma de libro mayor (*ledger*). Introdujeron el concepto de tecnología de la contabilidad descentralizada (*DLT*), planteando así una nueva forma de registrar información sin la necesidad de una entidad central que controle la red.

Como se ha podido apreciar en los capítulos previos, las cadenas de bloques desde su primera aplicación, debido a su gran potencial, han ido evolucionando y variando para poder adaptarse a más proyectos y ofrecer servicios personalizados a las organizaciones que quieran adaptar esta tecnología a su negocio. Estas variaciones han afectado, principalmente, al acceso y a los privilegios de las redes *blockchain*.

Para clasificar las cadenas de bloques, si se tiene en cuenta el acceso, se puede decir que son públicas, privadas o de consorcio. Por otro lado, si se tienen en cuenta los privilegios, las cadenas de bloques pueden ser "*permissioned*" (con permisos) o "*permissionless*" (sin permisos). Estas clasificaciones se pueden combinar, puesto que el acceso y los privilegios forman parte de las características de cada cadena de bloques. En este capítulo, se procederá a explicar y comparar estas posibles combinaciones para analizar los distintos tipos de cadenas de bloques que existen.

5.1 Redes *blockchain* públicas sin permisos

Las cadenas de bloques, en su origen, fueron creadas como una tecnología pública y abierta. Debido a esto, las primeras aplicaciones de las *blockchains*, como *Bitcoin* o *Ethereum*, son redes públicas y sin permisos. Esto implica que la gobernanza de dichas redes no depende de ninguna entidad central. Son redes totalmente descentralizadas y distribuidas en las que cualquier nodo puede realizar transacciones con cualquier otro nodo de la red, así como participar en los procesos de validación de transacciones.

Al ser redes públicas, cualquiera que implemente el software de código abierto que hace funcionar la red puede obtener una dirección y unirse a la red como un nuevo nodo. El usuario será anónimo, puesto que, a diferencia de las redes privadas, no es necesario que se identifique para poder unirse a la red.

En las redes públicas sin permisos, los algoritmos de consenso están basados en pruebas de trabajo (*proof-of-work*) o pruebas de participación (*proof-of-stake*). Las pruebas de trabajo han demostrado ser menos eficientes, dado que, en casos como el de *Bitcoin*, requieren una gran potencia de cálculo

y suponen un alto consumo de energía durante el proceso de cálculos sobre los bloques (minería). Las pruebas de participación, por otro lado, surgieron con el objetivo de solucionar estos problemas y aportar una mejor seguridad y escalabilidad a las redes que las implementan.

Los puntos fuertes de estas redes son, entre otros, la confianza que proporcionan entre los nodos participantes, su acceso abierto, su alta seguridad, su naturaleza anónima y la ausencia de una autoridad central. Ofrecen completa transparencia, dado que todos los nodos tienen acceso a la cadena de bloques y pueden verificar todas las transacciones que se hicieron desde su origen, sin comprometer la privacidad de los participantes de cada transacción. Además, las cadenas de bloques son inmutables, puesto que una vez un bloque es añadido a la cadena ya no es posible eliminarlo o modificarlo.

En cuanto a los inconvenientes de estas redes, su velocidad para validar transacciones es más lenta que la de las cadenas de bloques privadas o de consorcio. Esto a su vez afecta a la escalabilidad. En redes tan grandes como *Bitcoin*, el tamaño de los bloques es fijo, pero el número de nodos es cada vez mayor. Por tanto, como la cantidad de transacciones aumenta, se ralentiza cada vez más el proceso de validaciones y la red se vuelve menos escalable. Por otro lado, algunas redes públicas sin permisos utilizan métodos de consenso que consumen mucha energía, como *proof-of-work*.

Respecto a las vulnerabilidades, estas redes son vulnerables a los ataques del 51%, mediante los cuales un solo individuo o grupo de individuos podrían hacerse con el control del 51% de los nodos. Así, los atacantes dispondrían de más capacidad de cálculo que el resto de los nodos y más participantes en las “votaciones” para alterar el funcionamiento de la red. En redes tan grandes como *Bitcoin* o *Ethereum*, es muy poco probable que puedan suceder este tipo de ataques.

Otro ataque que cabe destacar es el que sufrió *DAO* (Organización Autónoma Descentralizada) de *Ethereum*. Este proyecto de capital de riesgo sufrió un ataque que implicó el robo de 50 millones de dólares. *Ethereum*, como reacción ante este ataque, realizó una bifurcación dura (*hard fork*) para restaurar los fondos robados, aunque no todas las partes aprobaron la decisión. Así, la red se dividió en dos cadenas de bloques distintas: *Ethereum* y *Ethereum Classic*.

En relación con los casos de uso, las redes de cadenas de bloques públicas sin permisos son ideales para sistemas de votación, sistemas de pago (criptomonedas) y desarrollo de aplicaciones descentralizadas.

5.2 Redes *blockchain* públicas con permisos

Las redes de cadenas de bloques públicas con permisos son redes abiertas a las que cualquiera puede acceder. Al igual que en el caso anterior,

no existe ninguna autoridad central que gobierne la red. Son de código abierto y cualquier usuario que implemente el software que hace funcionar a la red puede obtener una dirección y unirse como un nuevo nodo. No obstante, en este tipo de redes no todos los nodos pueden validar transacciones o crear nuevos bloques. Son los encargados del mantenimiento de la red los que tienen la capacidad de designar partes privilegiadas. De tal forma, que esos nodos tienen habilidades no disponibles para el resto de los nodos.

Una red pública con permisos, como *XRP Ledger* o *EOS*, combina los permisos de una red privada con el modelo de gobernanza descentralizado de las redes públicas sin permisos. El objetivo de esto es obtener las mejores propiedades de ambos modelos [25]. De este modo, se obtiene un algoritmo de consenso basado en un sistema de validación en el que cada participante posee un conjunto superpuesto de "validadores de confianza", los cuales acuerdan de manera eficiente qué transacciones ocurren en qué orden. Esto reduce el tiempo y el gasto de energía que se requerirían en las validaciones de las redes públicas sin permisos, y demuestra que son un tipo de *blockchain* más eficiente y rápida. Estas redes pueden procesar un mayor número de transacciones en menos tiempo y son altamente escalables. Por otro lado, se mantiene la transparencia de la cadena de bloques para todos los usuarios de la red.

Este tipo de redes poseen las ventajas de las redes públicas, como la descentralización de la red, el libre acceso para nuevos participantes, los métodos de incentivación para el mantenimiento de la red y la transparencia, además de las ventajas de ser una red con permisos, como la escalabilidad, la alta eficiencia y los métodos de consenso más rápidos.

Respecto a los inconvenientes, en estas redes no todos los nodos pueden crear bloques o validar transacciones. Son menos anónimas, debido a la existencia de los grupos de confianza y la seguridad depende de la integridad de los participantes.

En cuanto a los casos de uso, las redes de cadenas de bloques públicas con permisos son una buena opción para sistemas de pago más rápidos y eficientes, así como para aplicaciones descentralizadas (*dapps*).

5.3 Redes *blockchain* privadas sin permisos

En las redes privadas sin permisos cualquiera puede activar un nodo para unirse como en las redes públicas. Sin embargo, a diferencia de las cadenas de bloques públicas, los demás nodos solamente reconocerán su existencia, pero no compartirán ningún dato. Los contratos inteligentes en estas redes privadas no sólo definen a quién se le permite realizar acciones contractuales, sino que también a quién se le permite leer el contrato y toda la información relacionada [26].

Para lograr esto, las soluciones privadas sin permisos, en lugar de crear una sola cadena de bloques compartida por todos, crean para cada instanciación de un *Smart Contract* su propia cadena ad-hoc. Es otras palabras, la implementación de un contrato inteligente en una cadena de bloques privada sin permisos crea automáticamente una cadena "lateral" privada asociada con ese contacto [26]. Un solo nodo puede contener varias cadenas ad-hoc, pero nunca todas.

Los privilegios de lectura no se otorgan a nodos específicos, sino a personas u organizaciones específicas (identificadas por una firma criptográfica). Cada contrato posee un identificador (o dirección) único y cada nodo una dirección en forma de URL. Es necesario conocer tanto la dirección del nodo como el identificador del contrato para poder obtener una copia del contrato y la cadena asociada [26]. Un usuario puede utilizar tanto su nodo como uno en el confíe para solicitar una copia de una cadena ad-hoc privada y comenzar a participar en el contrato. Los nodos solamente contienen la información mínima necesaria para dar servicio a sus usuarios, en lugar de toda la información de la red.

Este tipo de redes, como en el caso de *LTO Network*, permiten que todos los nodos puedan comunicarse entre sí en una única red que nadie controla. Todos los nodos pueden ejecutar contratos inteligentes y tienen acceso completo a su cadena ad-hoc. Estas redes son descentralizadas, ya que no son controladas una autoridad.

Figura 20: Logotipo de *LTO Network*.

En lo relativo a las desventajas, no son una opción adecuada si se desea interactuar con toda la red. La transparencia de la red se limita a las cadenas ad-hoc a las que el participante tiene acceso. Por otro lado, los nodos no son anónimos, puesto que para poder unirse a la red deben identificarse previamente.

Las redes *blockchain* privadas sin permisos son una buena opción para multinacionales y gobiernos. Estas redes tienen un fuerte enfoque en la privacidad y en el cumplimiento del RGPD (Reglamento General de Protección de Datos).

5.4 Redes *blockchain* privadas con permisos

Las redes de cadenas de bloques privadas con permisos son aquellas en las que existe una autoridad central que controla la red. Esta autoridad decide qué nodos pueden o no unirse a la red, así como qué nodos de los seleccionados pueden validar transacciones. Estas redes están parcialmente

descentralizadas, ya que la gobernanza de la red depende de una entidad, no de todos los nodos de la red, como en el caso de las redes públicas.

Este tipo de redes implementan contratos inteligentes, ya que generalmente están basados en *Ethereum*. Las redes privadas con permisos, como *Hyperledger Fabric* o *Quorum*, están enfocadas en la rapidez y eficiencia de los procesos de validación de transacciones, así como en el control de la privacidad de los nodos. Siguen una arquitectura de ejecución de órdenes en la que el protocolo de consenso valida y ordena las transacciones y luego las propaga a todos los nodos pares. Después, cada par ejecuta las transacciones secuencialmente [12].

En cuanto a los puntos fuertes de estas redes, ofrecen una eficiencia y rapidez en el proceso de validaciones de transacciones superior al de las redes públicas sin permisos y garantizan la privacidad de los nodos. Son redes personalizables, es decir, se adaptan a las necesidades y requerimientos de la entidad que controle la red.

En relación a los inconvenientes, los nodos no son anónimos, puesto que son identificados antes de unirse a la red. No es un sistema transparente, debido a que la autoridad central decide qué nodos pueden ver y quienes no el libro contable de la red. Además, puede haber censura en las transacciones por parte de las autoridades.

Las redes privadas con permisos son la mejor opción para las entidades financieras que quieran hacer uso de redes distribuidas. También son redes pensadas para el comercio, servicios gubernamentales, gestión de cadenas de suministros o incluso entidades aseguradoras.

5.5. Redes *blockchain* de consorcio

Las redes de cadenas de bloques de consorcio surgen como una solución creativa para las entidades u organizaciones que quiere hacer públicos ciertos aspectos, mientras que otros se mantienen privados. Son una combinación entre las redes públicas y las privadas. Estas redes están descentralizadas, dado que están controladas, generalmente, por más de una organización. Estas organizaciones seleccionan a lo nodos que pueden unirse a la red. Estos nodos no serán anónimos puesto que se deben identificar para poder acceder a la red.

Los procedimientos de consenso están controlados por los nodos preestablecidos. Para garantizar la funcionalidad adecuada, el consorcio tiene un nodo validador por cada organización participante que puede tanto validar transacciones, como iniciarlas o recibirlas. Los nodos miembros, en comparación, solamente pueden iniciar o recibir transacciones.

Los algoritmos de consenso de este tipo de redes, como *Voltron* o *Marco Polo*, se basan en votaciones para poder agregar bloques a la cadena de bloques de la red. En estas votaciones los nodos validadores deben alcanzar un consenso, puesto que bastará con que un nodo no esté de acuerdo para que el bloque no sea añadido a la cadena.

Entres las ventajas de estas redes están su rapidez en los procesos de validación de transacciones, su alta escalabilidad, su bajo consumo de energía, el nulo riesgo de ataques del 51% y la baja probabilidad de actividades delictivas, ya que ninguno de los nodos de la red es anónimo y es muy poco probable que un atacante se una a la red sin ser descubierto.

En lo relativo a los inconvenientes, en estas cadenas de bloques los usuarios no son anónimos. Tampoco son redes tan transparentes como otros tipos de *blockchains*, puesto que no todos los nodos tienen acceso a todos los datos. A pesar de ser redes seguras, esta seguridad depende de la integridad de los miembros. Por otro lado, las regulaciones y la censura de las autoridades pueden tener un gran impacto en a funcionalidad de la red.

Este tipo de redes están pensadas para grupos de entidades bancarias que quieran trabajar conjuntamente en una red distribuida. Asimismo, pueden ser una buena opción para grupos de investigación, mejorando la forma de compartir datos y resultados de investigaciones.

6. Conclusiones y trabajo futuro

6.1 Conclusiones

Cada vez son más las empresas y organizaciones que demandan un sistema de gestión de la información avanzado, distribuido y eficiente, para no quedarse atrás en una era en la que la digitalización de las cosas no para de crecer. La tecnología de las cadenas de bloques ha demostrado ser la respuesta a dicha demanda.

A lo largo de este trabajo, se ha podido apreciar la evolución que ha tenido la tecnología *blockchain* desde su origen. El proyecto que introdujo la tecnología de libro mayor distribuido (*DLT*) en el mundo, demostró ser una tecnología con mucho potencial en su primera aplicación: el *Bitcoin*. Más adelante, otros proyectos como *Ethereum*, fueron modelando las cadenas de bloques para poder ofrecer más funcionalidades a los usuarios (*Smart Contracts*). A medida que *Bitcoin* y *Ethereum* crecían, aparecieron nuevos desarrolladores que se basaron en ambos proyectos para eliminar o disminuir sus defectos y potenciar sus virtudes, para adaptarlos a nuevos escenarios. Es así como fueron surgiendo los distintos tipos de cadenas de bloques que existen.

La tecnología *blockchain* permite mantener registros descentralizados y distribuidos de transacciones digitales documentadas en forma de libro mayor (*ledger*). Dichas transacciones se realizan de manera segura y transparente, sin revelar la identidad de los usuarios en ningún momento. Asimismo, ofrece un amplio abanico de posibilidades para poder adaptarse a los requerimientos de la organización que quiera implementar esta tecnología.

Los distintos tipos de cadenas de bloques se pueden clasificar en función de su acceso (públicas, privadas o de consorcio) o de sus privilegios (con permisos o sin permisos). Estas características se pueden combinar para dar origen a cinco tipos de cadenas de bloques: cadenas de bloques públicas sin permisos, públicas con permisos, privadas sin permisos, privadas con permisos o de consorcio. Tras el análisis realizado en este trabajo, queda claro que para las empresas u organizaciones, como las entidades financieras por ejemplo, que priman la velocidad de las transacciones y la eficiencia de las cadenas de bloques, las redes privadas son la mejor opción. Si estas redes pretenden englobar a más de una organización, entonces las cadenas de bloques de consorcio son la solución. Ambos tipos de *blockchain* son totalmente personalizables, limitan el acceso a los participantes que se desee y establecen unas reglas de consenso en torno a las necesidades o requerimientos de la organización que las controla. Ofrecen procesos de validación más rápidos y eficaces que el resto de las cadenas de bloques.

Por otro lado, las cadenas de bloques públicas son una buena opción para la gestión de criptomonedas. Permiten el intercambio de divisas entre nodos de la red de pares, que pueden estar incluso en continentes distintos, de manera rápida y directa, sin la necesidad de intermediarios. Permiten a su vez, que cualquier nodo participe en procesos de minería para la mejora y el mantenimiento de la red, a cambio de ciertas recompensas.

En resumidas cuentas, las cadenas de bloques son una tecnología de libro mayor distribuido muy versátil y con mucho potencial. Es más, las criptomonedas y los sistemas de pago no son más que la punta del iceberg de las posibles aplicaciones de esta tecnología, puesto que ya existen proyectos con el fin de integrar las cadenas de bloques en ámbitos como la sanidad, la gestión de identidades, la protección de patentes y derechos de autor, el voto electrónico, la venta y alquiler de bienes inmuebles, la educación, la logística o los seguros, entre otros.

Siguiendo los objetivos marcados para este trabajo, se ha logrado exponer los conceptos básicos necesarios para comprender el funcionamiento de la tecnología *blockchain*, analizar uno a uno los distintos tipos de cadenas de bloques que existen, realizar una comparación de los aspectos más relevantes entre los distintos tipos y, finalmente, exponer y analizar las conclusiones obtenidas a raíz de los análisis realizados. De tal manera, que se ha logrado cumplir con los objetivos principales del trabajo.

6.2 Trabajo futuro

En esta memoria se ha realizado un análisis de los distintos tipos de cadenas de bloques. No obstante, no se ha podido profundizar lo suficiente en el ámbito de la seguridad, las vulnerabilidades y los ataques sufridos en las cadenas de bloques. Una nueva línea de trabajo podría ir enfocada al análisis de estos aspectos, ofreciendo ejemplos de situaciones de ataques verídicos y cómo se consiguieron solucionar. Así, se obtendría un análisis más profundo y completo sobre las cadenas de bloques y sus distintos tipos.

Por otro lado, se podría ampliar el ámbito del proyecto a redes *DLT* (*Distributed Ledger Technology*), como *IOTA*. De esta forma, se cubrirían los dos tipos de redes de registro de transacciones digitales en forma de libro mayor. Asimismo, sería posible realizar una comparación entre la tecnología de cadenas de bloques y la tecnología de libro mayor distribuido (*DLT*), comparando los aspectos más relevantes de ambas tecnologías.

7. Glosario

Árbol de Merkle: es una estructura de datos en forma de árbol. Su funcionamiento consiste en generar un hash criptográfico de cada una de los nodos (hojas) y combinarlos por pares. De cada par se genera un nuevo hash y se repite el proceso hasta obtener un único hash raíz (*root hash*). Esta estructura permite asegurar la integridad y verificación de los datos.

Ataque del 51%: este tipo de ataque consiste en que un individuo o grupo se haga con el control del 51% de la red *blockchain*. De esta manera, pueden tomar decisiones que alteren el funcionamiento de la red y validar transacciones fraudulentas.

Criptodivisas, criptomonedas: es un medio digital de intercambio que utiliza criptografía avanzada para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido.

Descentralized Apps (Dapps): se trata de aplicaciones que funcionan en un sistema distribuido y descentralizado como las *blockchains*. Estas aplicaciones sirven para implementar contratos inteligentes.

Descentralized Autonomous Organization (DAO): en castellano, Organización Autónoma Descentralizada. Se trata de una organización controlada en su totalidad por algoritmos computacionales. Dichos algoritmos son *Smart Contracts* que rigen las normas de cómo deben cooperar las partes implicadas en la DAO.

Distributed Ledger Technology (DLT): en castellano Tecnología de Libro Mayor Distribuido. Es un sistema electrónico o base de datos para registrar información que no es ejecutada por una sola entidad. Esta nos permite almacenar y utilizar datos que pueden ser descentralizados y distribuidos tanto de forma privada como pública.

Escalabilidad: anglicismo que describe la capacidad de un negocio o sistema de crecer en magnitud. Es la propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para reaccionar y adaptarse sin perder calidad, o bien manejar el crecimiento continuo del trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

Fork: se trata de una bifurcación. Hace referencia a la creación de una copia de sí mismo por parte de un programa, que entonces actúa como un “proceso hijo” del proceso originario, ahora llamado “padre”. Los procesos resultantes son idénticos, salvo que tienen distinto número de proceso (PID).

Fungibilidad: este término hace referencia a todos aquellos activos que tienen la característica de consumirse debido a su uso. El dinero o los

alimentos son claros ejemplos de bienes fungibles, dado que al hacer uso de ellos desaparecen, se consumen o se transforman.

Hard fork: en castellano, bifurcación dura. En lo que respecta a la tecnología *blockchain*, hace referencia a un cambio radical en el protocolo de una red que hace que los bloques y transacciones previamente válidos sean invalidados o viceversa. Esta bifurcación requiere que todos los nodos se actualicen a la última versión del software de protocolo.

Internet of Things (IoT): es un concepto que se refiere a una interconexión digital entre objetos cotidianos e internet. Constituye un cambio radical en la vida de las personas en la sociedad, ofrece una gran cantidad de nuevas oportunidades de acceso a datos, servicios específicos en la educación, seguridad, asistencia sanitaria y en el transporte, entre otros campos.

Proof-of-stake: consiste en una *proof-of-work* que no requiere un gran consumo de energía. Se podría traducir como "prueba de participación", donde los nodos "apostarían" monedas, siguiendo los requisitos que establece la red, para ser elegible para participar en el algoritmo de consenso. Es decir, que los usuarios que posean más criptomonedas y que hayan participado por más tiempo en la red, tendrán más posibilidades de ser elegidos para validar los bloques de la cadena de bloques.

Proof-of-vote: consiste en un sistema de votación, mediante el cual los nodos de la red de consorcio deben valorar si consideran adecuado que un bloque sea añadido a la cadena de bloques de la red. Si hay consenso, el bloque se añadirá a la cadena. En caso de que un solo nodo no esté de acuerdo, el bloque no se añadirá.

Proof-of-work: también llamada "prueba de trabajo", consiste en una forma de prueba criptográfica de conocimiento cero en la que una parte (el probador) demuestra a los demás (verificadores) que se ha gastado una cierta cantidad de un esfuerzo computacional específico. Tiene el fin de desincentivar y dificultar comportamientos indeseados como ataques DDoS o spam.

Protocolo *Gossip*: es un protocolo de comunicación que utilizan los dispositivos digitales para propagar información en una red P2P de forma rápida y segura. Permite diseñar sistemas de comunicación altamente eficientes, seguros y de baja latencia.

Red P2P (*Peer-To-Peer*): una red P2P o red de pares, 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 más, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Este tipo de redes permite el intercambio directo de información, en cualquier formato, entre los ordenadores conectados.

Reglamento General de protección de Datos (RGPD): es el reglamento europeo relativo a la protección de las personas físicas en lo que

respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 24 de mayo de 2016 y fue aplicada desde el 25 de mayo de 2018.

Token: es una unidad de valor destinada a ser una pieza del ecosistema de la *blockchain*. Se utilizan para incentivar a los nodos que participan en el mantenimiento de una red *blockchain*. Pueden ser *tokens* de utilidad o monetarios (criptomonedas).

Transacción: es un envío o transferencia de valor entre dos partes dentro de una red *blockchain*. Estas transacciones pueden ser económicas o simplemente transferencias de datos.

Wallet: es una cartera digital que sirve para coleccionar y administrar claves privadas dentro de una cadena de bloques. También sirve para realizar transacciones entre los nodos de la red.

8. Bibliografía

[1] NAVARRO, Benjamín Yahari. *Blockchain y sus aplicaciones*. Artículo de investigación: UC Asunción (Paraguay), 2017. Disponible en: http://jeuazarru.com/wp-content/uploads/2017/11/Blockchain.pdf

[2] ANTONOPOULOS, Andreas M. y WOOD, Gavin. *Mastering Ethereum*. O'Reilly Media, Inc., 2018. ISBN 9781491971949.

[3] ANTONOPOULOS, Andreas M. *Mastering Bitcoin*. O'Reilly Media, Inc., 2014. ISBN 9781449374044.

[4] Vadapalli, Ravindhar. (2020). BLOCKCHAIN FUNDAMENTALS TEXT BOOK Fundamentals of Blockchain.

[5] KOONE, Lance. *Let's Desintermediate All the Lawyers: Smart Contracts on the Blockchain (Why Blockchain Matters to the Arts, Part 4)* [en línea]. Artículo de investigación en *Medium*, 2016. Disponible en: https://medium.com/creativeblockchain/lets-disintermediate-all-the-lawyers-smart-contracts-on-the-blockchain-why-blockchain-matters-to-the-cd031e40a75e

[6] *Built in* [en línea] [fecha de la consulta: 3 de mayo de 2021]. Disponible en: https://builtin.com/blockchain/blockchain-real-estate-companies

[7] *101 Blockchains* [en línea] [fecha de la consulta: 3 de mayo de 2021]. Disponible en: https://101blockchains.com/blockchain-usage/

[8] *101 Blockchains* [en línea] [fecha de la consulta: 6 de mayo de 2021]. Disponible en: https://101blockchains.com/types-of-blockchain/

[9] *XRP Ledger* [en línea] [fecha de la consulta: 6 de mayo de 2021]. Disponible en: https://xrpl.org/xrp-ledger-overview.html

[10] LAURENCE, Tiana. *Blockchain For Dummies*. For Dummies, 2017. ISBN 9781119365594.

[11] PASTORINO, Cecilia. *Blockchain: qué es, cómo funciona y cómo se está usando en el mercado* [en línea]. Artículo de investigación en *WeLiveSecurity*, 2018. Disponible en: https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

[12] *HYPERLEDGER FABRIC* [en línea] [fecha de la consulta: 12 de mayo de 2021]. Disponible en: https://hyperledger-fabric.readthedocs.io/es/latest/whatis.html

[13] *101 Blockchains* [en línea] [fecha de la consulta: 12 de mayo de 2021]. Disponible en: https://101blockchains.com/es/quorum-blockchain-guia/

[14] BLANCO, David. *Corda: una DLT para entidades financieras* [en línea]. Artículo en Paradigma, 2020. Disponible en: https://www.paradigmadigital.com/dev/corda-dlt-entidades-financieras/

[15] *101 Blockchains* [en línea] [fecha de la consulta: 12 de mayo de 2021]. Disponible en: https://101blockchains.com/public-vs-private-blockchain/

[16] *101 Blockchains* [en línea] [fecha de la consulta: 13 de mayo de 2021]. Disponible en: https://101blockchains.com/es/blockchain-federadas/#5

[17] *CBInsights* [en línea] [fecha de la consulta: 15 de mayo de 2021]. Disponible en: https://www.cbinsights.com/research/banks-regulators-trade-finance-blockchain/

[18] *101 Blockchains* [en línea] [fecha de la consulta: 15 de mayo de 2021]. Disponible en: https://101blockchains.com/private-blockchain-vs-consortium-blockchain/

[19] *101 Blockchains* [en línea] [fecha de la consulta: 17 de mayo de 2021]. Disponible en: https://101blockchains.com/permissioned-vs-permissionless-blockchains/

[20] *CoinTelegraph* [en línea] [fecha de la consulta: 17 de mayo de 2021]. Disponible en: https://es.cointelegraph.com/eos-101/what-is-eos

[21] *SOVRIN* [en línea] [fecha de la consulta: 17 de mayo de 2021]. Disponible en: https://sovrin.org/faq/is-sovrin-permissioned/

[22] *Blockchain Council* [en línea] [fecha de la consulta: 19 de mayo de 2021]. Disponible en: https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/

[23] SERHACK. *Mastering Monero: The future of private transactions*. 2018. Disponible en: https://masteringmonero.com

[24] *CoinTelegraph* [en línea] [fecha de la consulta: 19 de mayo de 2021]. Disponible en: https://es.cointelegraph.com/dash-101/what-is-dash

[25] RUIZ Jesus. Public-Permissioned blockchains as Common-Pool Resources. [Technical Report] Alastria Blockchain Ecosystem. 2020. Hal-02477405.

[26] *LTO Network* [en línea] [fecha de la consulta: 19 de mayo de 2021]. Disponible en: https://blog.ltonetwork.com/permissionless-private-blockchains-lto-network/

[27] Singhal, Bikramaditya & Dhameja, Gautam & Panda, Priyansu. (2018). Beginning Blockchain. 10.1007/978-1-4842-3444-0.