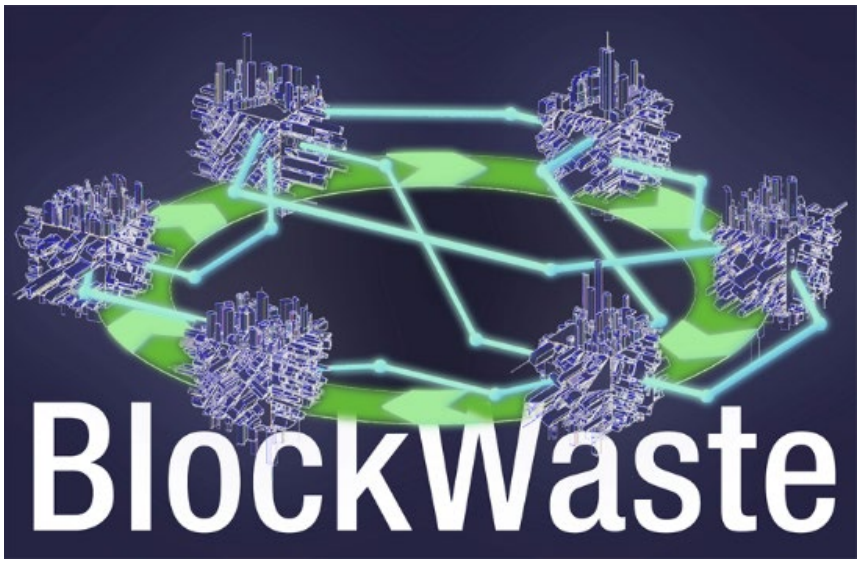
O1.A3 Manuales de Estrategias de Economía Circular aplicadas a la Gestión de Residuos Municipales utilizando tecnología Blockchain

Manual II: Blockchain



ΙΔΡΥΜΑ ΚΡΑΤΙΚΩΝ ΥΠΟΤΡΟΦΙΩΝ IKY

Co-funded by the Erasmus+ Programme of the European Union

Ficha de resultados:

Programa de financiación	Programa Erasmus+ de la Unión Europea
Financiación NA	EL01 Fundación de Becas Estatales Griegas (IKY)
Título completo del proyecto	Formación innovadora basada en la tecnología Blockchain aplicada a la gestión de residuos — BlockWaste
Campo	KA2 — Cooperación para la innovación y el intercambio de buenas prácticas KA203 — Asociaciones estratégicas para la educación superior
Número de proyecto	2020-1-EL01-KA203-079154
Duración del proyecto	24 meses
Fecha de inicio del proyecto	01-10-2020
Fecha de finalización del proyecto:	30-09-2022

Detalles de los resultados:

Título de salida: O1: Materiales de aprendizaje para Blockchain-RSU interdisciplinario

Título de la tarea: A3. Manuales de estrategias de economía circular aplicadas a la gestión de residuos municipales utilizando tecnología Blockchain

Líder de salida: NTUA

Líder de la tarea: Saxion UAS

Autor(es): Christa Barkel, c.barkel@saxion.nl, Saxion UAS, Países Bajos, Perry Smit, Saxion UAS, p.j.smit.01@saxion.nl, Países Bajos

Revisado por: Rainer Lenz, rlenz@fh-bielefeld.de, Bielefeld UAS, Alemania, Paraskevas Tsangaratos, Universidad Técnica Nacional de Atenas, ptsag@metal.ntua.gr, Grecia

CControl del documento

Versión del documento	Versión	Enmienda
V0.1	11/03/2022	Versión final — 29/04/2022

Contenido

Lista de figuras

Lista de abreviaturas

Abreviatura	**Definición**
CBDC	Moneda digital del Banco Central
CBDC	Moneda digital del Banco Central
DAO	Organización Autónoma Descentralizada
dApps	Aplicaciones descentralizadas
DLT	Tecnología de Ledger distribuida
DPOs	Prueba Delegada de Estaca
CEI-20 (protocolo)	Ethereum Solicitud de comentarios 20 (protocolo)
ICO	Oferta inicial de monedas
IEO	Oferta de intercambio inicial
RSU	Residuos Sólidos Urbanos
NFT	Token no fungible
P2P	Peer-to-Peer
Puntos de venta	Prueba de participación
POA	Prueba de autoridad
SPOF	Un solo punto de fracaso
STO	Oferta de tokens de seguridad
TTP	Tercero de confianza

Resumen ejecutivo

En este manual Blockchain se aborda desde una amplia gama de perspectivas. La expectativa es que esto ayudará al lector a diseccionar mejor la relevancia de Blockchain y obtener una comprensión más profunda de su potencial. Los primeros conceptos básicos se explican con Bitcoin como ejemplo. Bitcoin es la primera aplicación en usar Blockchain. Bitcoin utiliza una red descentralizada, en la que todas las personas que desean participar en el proceso de toma de decisiones de Bitcoin participan en la toma de decisiones juntas. El código Bitcoin es de código abierto, lo que permite a cualquier persona ver, copiar y editar fácilmente el código fuente a su gusto, permitiendo que surjan nuevos experimentos con otras, tal vez mejores formas de criptomonedas u otras aplicaciones y otras formas de consenso. Aunque Bitcoin es un ejemplo de explicación, es importante tener en cuenta que no solo el sistema financiero se ve afectado por Blockchain. La tecnología subyacente de blockchain ofrece nuevas oportunidades para transformar otras industrias, incluida la gestión de residuos sólidos municipales.

Este manual comienza con una explicación de Blockchain y sus características. Se da una distinción más clara entre la criptomoneda bitcoin y la red Bitcoin y se explica el mecanismo de consenso de Bitcoin, Proof-of-Work. Además de los principios básicos de Blockchain explicados en este manual utilizando Bitcoin, el enfoque cambia a una nueva generación de Blockchain diseñados específicamente para crear una plétora de otros tipos de aplicaciones descentralizadas o dApps. Una cadena de bloques específica en la que se centra la atención es Ethereum, que fue la primera en habilitar la programación de Smart Contracts. Un contrato inteligente es una automatización descentralizada y puede definirse como un contrato con ciertos términos y condiciones que se establecen en el código. El contrato es autoejecutable, ya que realiza las acciones correspondientes apropiadas cuando se cumplen los términos y condiciones.

Además, este manual explica brevemente dos fenómenos de Blockchain: aplicaciones descentralizadas (dApps) y organizaciones autónomas descentralizadas (DAO).

Blockchain se puede dividir en sus tipos desde tres perspectivas, el protocolo de consenso, la gobernanza y los tipos de cooperación entre los sistemas Blockchain. Los protocolos de consenso son esenciales para garantizar la confianza entre los diferentes participantes dentro de una red distribuida. Debe haber confianza en que los participantes no están corruptos y que los datos que se comparten entre ellos no están corruptos. A continuación, una Blockchain, como cualquier asociación, necesita ser administrada y controlada a través de una estructura de gobierno de Blockchain. Las opciones entre los diferentes tipos de Blockchain afectan el control de la organización. Cuanta más confianza haya en la naturaleza descentralizada de Blockchain, más fácil será participar. Cuanta más confianza haya en que los validadores puedan participar en la construcción de consensos como incógnitas, más transparente será el sistema.

Para concluir las tres perspectivas, hay diferentes tipos de cooperación entre los sistemas Blockchain. Blockchain donde diferentes compañías y terceros cooperan sin que un usuario central controle esta Blockchain, se llama Blockchain Enterprise. Para construir una Blockchain de este tipo, las empresas utilizan plataformas Blockchain. Estas plataformas permiten a los usuarios escribir aplicaciones utilizando ciertas tecnologías. Se han organizado varias asociaciones en torno a estas plataformas. Las plataformas son la tercera y última forma en que vemos los diferentes tipos de Blockchain aquí.

Uno de los grandes inventos de Satoshi Nakamoto es la combinación de tecnologías preexistentes con un sistema de recompensa que mantiene una red descentralizada en funcionamiento: economía criptográfica. La idea central detrás de la criptoeconomía dentro de Blockchain es que se desarrollan protocolos que alientan a las personas a participar en la red de tal manera que el valor de la red se maximice para los participantes.

Un token criptográfico se puede crear en una cadena de bloques y también representa un activo negociable. A veces se crean tokens para financiar un proyecto. El proceso de creación de tokens se llama tokenización. El comercio de estos tokens permite transferir la propiedad a los activos subyacentes. Este manual explica diferentes tipos de tokens y su uso.

Para concluir, hay tres ejemplos del uso y aplicación de Blockchain dados, incluida la interpretación de algunas condiciones cruciales requeridas para la implementación exitosa de Blockchain.

1 Introducción

1.1 Breve descripción del proyecto

El proyecto BlockWaste tiene como objetivo abordar la interoperabilidad entre la gestión de residuos y la tecnología Blockchain y promover su tratamiento adecuado a través de la formación educativa, para que los datos recopilados se compartan dentro de un entorno seguro, donde no hay lugar para la incertidumbre y la desconfianza entre todas las partes involucradas. Para ello, los objetivos del proyecto BlockWaste son los siguientes:

- Realizar investigaciones sobre los residuos sólidos generados en las ciudades y cómo se gestionan, de modo que puedan utilizarse para crear una base de información de buenas prácticas, con el fin de reintroducir los residuos en la cadena de valor, promoviendo la idea de Ciudades Circulares Inteligentes.
- Identificar los beneficios de la tecnología Blockchain dentro del proceso de gestión de residuos urbanos (RSU).
- Crear un plan de estudio que permita la formación de docentes y profesionales de organizaciones y empresas del sector, en la superposición de los campos de Gestión de Residuos, Economía Circular y Tecnología Blockchain.
- Desarrollar una herramienta interactiva basada en la tecnología Blockchain, que permitirá poner en práctica la gestión de los datos obtenidos a partir de residuos urbanos, visualizando así la forma en que se implementan los datos en la Blockchain y permitiendo a los usuarios evaluar diferentes formas de gestión.

BlockWaste tiene como objetivo implementar nuevos contenidos educativos transnacionales con el objetivo de formar a sus estudiantes en los países socios y proporcionarles las habilidades básicas necesarias que les permitan actuar profesionalmente como futuros trabajadores del sector, agregando las competencias digitales requeridas por las empresas que están abrazando el proceso de transformación digital. En este sentido, el proyecto está dirigido a:

- Empresas y pymes, profesionales de TI, urbanismos y profesionales de la gestión de residuos.
- Universidades (profesores, estudiantes e investigadores).
- Organismos públicos

El proyecto incluye cuatro salidas intelectuales de la siguiente manera:

- O1. Materiales de aprendizaje para Blockchain-RSU interdisciplinario
- O2. Plan de estudios común europeo sobre la aplicación de las tecnologías Blockchain a las estrategias de economía circular
- O3. Herramienta de aprendizaje electrónico basada en Blockchain-RSU centrada en la economía circular
- O4. BlockWaste Open Educational Resource (OER)

Este documento describe y explica los principios básicos de Blockchain. Describe qué es Blockchain, cuándo puede usarlo, qué componentes está compuesto por Blockchain, qué tecnologías de Blockchain se utilizan y da una descripción de varias aplicaciones de Blockchain exitosas.

1.2 Objetivos y enfoque metodológico

El objetivo de este Manual «Blockchain» es guiar a los profesionales del sector de la gestión de residuos sobre cómo deben implementar la tecnología IoT y Blockchain como estrategias de Economía Circular. Por lo tanto, se dirige a los profesionales que conocen las ventajas del uso de la tecnología Blockchain. Los tres manuales conjuntos de este proyecto Blockwaste tienen como objetivo proporcionar a los lectores un conocimiento suficiente del potencial de la tecnología Blockchain para contribuir a una mayor circularidad en la gestión de residuos sólidos municipales. El Manual 1 (Blockchain) y el Manual 2 (Economía circular) deben entenderse como un breve compendio y proporcionan una visión general del contenido esencial del Manual 3 (Gestión de residuos basada en la cadena de bloqueo) — cf fig 1.

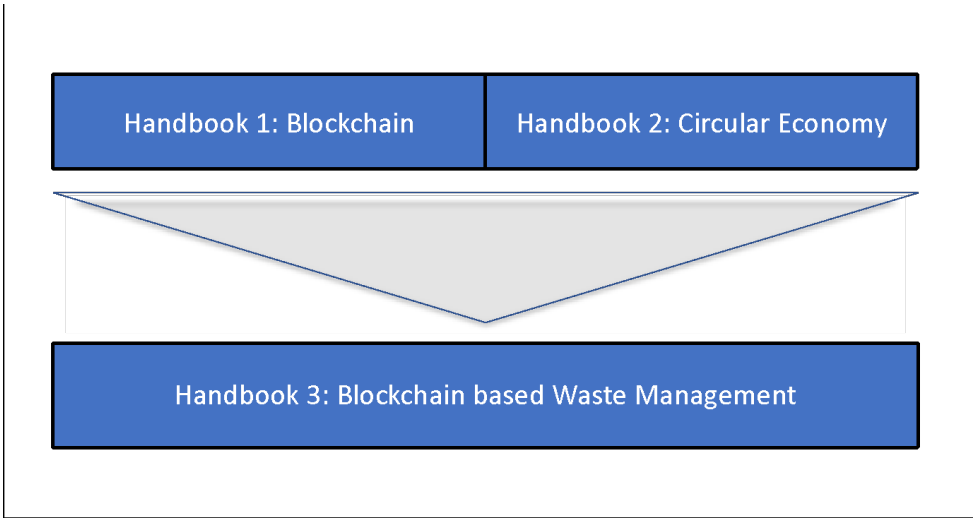


Figura 1: Manual del proyecto BlockWaste (los autores)

La estructura del manual sigue una lógica deductiva presentando, en la primera parte (capítulos 1 a 4), una breve historia de Blockchain por medio de Bitcoin y los fundamentos de la tecnología Blockchain La segunda parte del manual (capítulo 5) contiene una guía clara para los usos y aplicaciones de la tecnología Blockchain.

2 Fundamentos de blockchain

Comprender los principios de Blockchain a través de Bitcoin

«Perdón por ser una manta húmeda. Escribir una descripción para esta cosa para el público en general es sangrientamente difícil. No hay nada con lo que relacionarlo.»
— Satoshi Nakamoto (2010)

2.1 Introducción

Objetivos de aprendizaje

- Blockchain en el nivel más básico mirando Bitcoin.
- Blockchain es esencialmente un libro mayor distribuido en el que puede almacenar datos.
- Las diferencias entre una red Blockchain y una red centralizada.

Introducción

El 31 de octubre de 2008, se envió un correo electrónico bajo el nombre de Satoshi Nakamoto a la lista de correo de Cryptography.1 El correo electrónico incluía una referencia a un **libro blanco** titulado *Bitcoin: Un sistema de efectivo electrónico entre pares*. El libro blanco que adjuntó al anuncio es un documento de solo 9 páginas, que describe el funcionamiento técnico de Bitcoin. Este sistema permite enviar pagos en línea a otras partes, sin necesidad de una institución financiera.

Las principales características de este sistema de pago, según Satoshi:

1. El doble gasto se evita con una red peer-to-peer.
2. No hay menta u otras fiestas de confianza.
3. Los participantes pueden ser anónimos.
4. Las nuevas monedas están hechas de la prueba de trabajo estilo Hashcash.
5. La prueba de trabajo para la nueva generación de monedas también alimenta a la red para evitar el doble gasto.

Términos técnicos como doble gasto, red peer-to-peer, prueba de trabajo, Hashcash, marcas de tiempo, hashing y firmas digitales en el correo electrónico hacen que sea difícil para el público en general entender Bitcoin o más generalmente Blockchain. Especialmente, en ese momento, cuando no había nada que relacionar con la mayoría de la gente. En este capítulo, discutimos Bitcoin como el medio para entender los principios básicos de Blockchain.

[1] El correo electrónico original se puede encontrar en: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

Co-funded by the Erasmus+ Programme of the European Union

2.1.1 Bitcoin vs bitcoin

Generalmente hacemos una distinción entre bitcoin (caso inferior), el dinero digital también llamado criptomoneda, y Bitcoin, la red financiera subyacente que permite que los bitcoins sean enviados y recibidos.

2.1.2 Red peer-to-peer

Las computadoras, también llamadas ***nodos***, que ejecutan esta red financiera tienen y tienen acceso a un libro mayor en el que se registran todas las transacciones de bitcoin. Este libro mayor de Bitcoin es un registro de todas las transacciones válidas que alguna vez se han transmitido a la red, que es la infraestructura subyacente que consiste en los nodos que realizan un seguimiento, validan y marcan todas las transacciones de bitcoin. Llamamos a esta red una red ***peer-2-peer (P2P).***

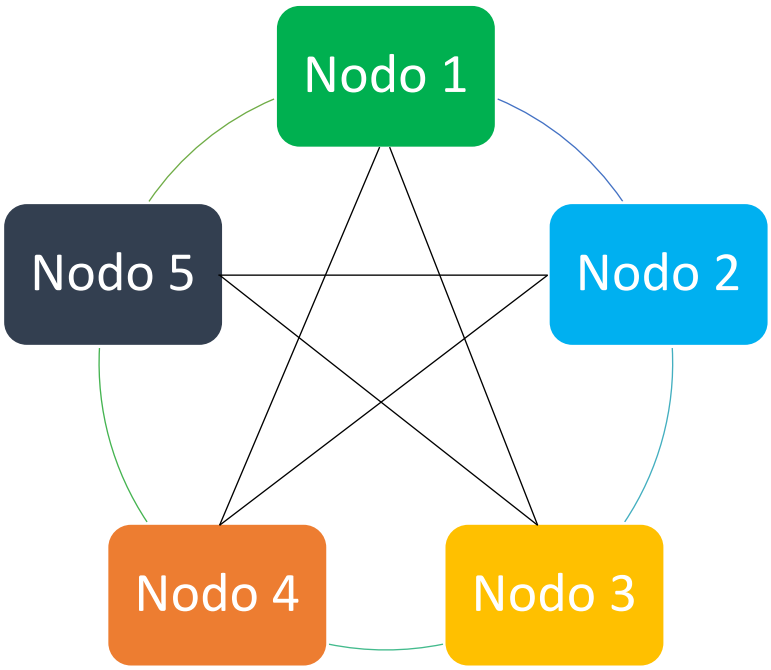


Figura 2: Una representación de una red distribuida, donde el Blockchain se distribuye a través de una red de nodos completos (Fuente: Lin Lim, C., Janse, A., Blockchain Basics, 2021, capítulo 1, página 14).

Una red P2P es una red de nodos, a menudo una computadora, que son igualmente privilegiados. Cada nodo puede ser un proveedor de servicios, así como un consumidor de servicios. Todo el mundo tiene acceso a la red Bitcoin y es libre de administrar un nodo en la red. Los nodos especializados en la red, también llamados ***nodos completos***, mantienen todo el historial de transacciones. Para eliminar toda la red y su historial de transacciones correspondiente, uno tendría que cerrar todos los nodos, lo que es casi imposible cuando la red consta de muchos nodos.

Cada participante dentro de la red sigue el protocolo Bitcoin. El protocolo Bitcoin es las reglas de procedimiento que rigen la red Bitcoin. Además, no hay intermediario entre dos nodos diferentes. Esto también significa que no hay ninguna parte central que pueda regular, detener y congelar sus transacciones. La eliminación de estos intermediarios permite transacciones más eficientes y más baratas.

2.1.3 Red cliente-servidor

Esta red P2P contrasta con la ***red cliente-servidor*** (workstation-server network).

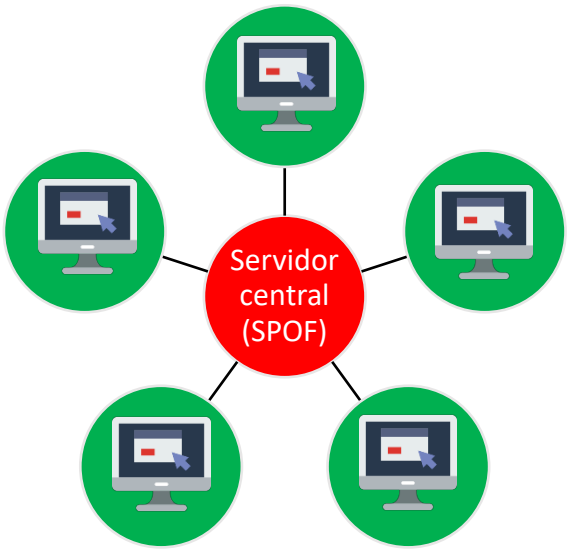


Figura 3: Árbol de decisiones simplificado si usar o no Blockchain (Fuente: Lin Lim, C., Janse, A., Blockchain Basics, 2021, capítulo 1).

Una red cliente-servidor utiliza servidores centralizados que proporcionan servicios, como un servicio de correo electrónico, a sus clientes. El servidor a menudo contiene datos y aplicaciones. Cuando los clientes necesitan acceso a estos recursos, pueden enviar una solicitud al servidor. Una debilidad de las redes cliente-servidor es que contiene un ***único punto de falla (SPOF)***. En este caso, el SPOF es el servidor central. Una vez deshabilitados, los clientes ya no podrán acceder a los servicios del servidor.

La necesidad de confiar en una parte central con sus datos y de confiar en que el SPOF no fallará hace que el modelo sea vulnerable. Las grandes empresas de buena reputación también pueden sufrir un diseño de red SPOF. Por ejemplo, en 2015 hubo un corte de energía en un solo centro de datos de PayPal. Como resultado, muchos usuarios ya no podían acceder al sitio web de PayPal, las transacciones con tarjetas de crédito ya no se podían procesar, las personas ya no podían acceder a la información de su cuenta personal o se mostraban balances incorrectos.[2]

[2] https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

2.1.4 Redes híbridas: el caso de Napster

También hay redes híbridas. Un ejemplo famoso es Napster, un servicio de descarga de música que ganó notoriedad a finales de la década de 1990 y principios de la década de 2000.

En 1999, un servicio de intercambio de archivos peer-to-peer llamado Napster fue lanzado por los adolescentes Shawn Fanning y Sean Parker. Napster hizo posible que las personas compartieran y descargaran fácilmente archivos de música digital de otros. Causó mucha conmoción, porque por primera vez la música se compartió ampliamente entre sí de forma gratuita. Napster permitió a la gente descargar y escuchar canciones individuales. Antes, si querías obtener una sola canción, tenías que comprar un álbum completo. En 2001, Napster finalmente se cerró después de una demanda con la Recording Industry Association of America, porque la distribución y descarga de archivos de música digital se consideró que violaba la ley de derechos de autor. Sin embargo, Napster todavía es conocido como un servicio revolucionario que ha interrumpido la industria de la música. En los Estados Unidos, las ventas de CD alcanzaron su punto máximo en el año 2000, después de lo cual hubo una fuerte disminución, en parte debido a Napster y servicios posteriores como BitTorrent y Spotify.

Napster Is Told to Remain Shut

By MATT RICHTEL JULY 12, 2001

SAN FRANCISCO, July 11 _ A federal judge today ordered that the Napster music-sharing service must remain off line until it can prove that it can more effectively filter copyrighted material, signifying the first time a judge has mandated the shut down of the Internet service.

The order comes at a time when Napster had already been taken out of service, a move it made of its own accord 10 days ago to add technology that would enable it to meet an earlier court order to filter copyrighted music.

Figura 4:Noticias de la hora de Nueva York; A Napster se le dice que permanezca cerrado el 12 de julio de 2001.

Napster es conocido por usar una red P2P. ¿Cómo es que las autoridades han podido cerrar Napster, lo que es prácticamente imposible con Bitcoin?

Napster utiliza un índice central que realiza un seguimiento de qué computadora tiene qué archivos compartir con otros usuarios. Si un usuario (ordenador A) quiere buscar una canción como Michael Jackson — Billie Jean, se hace una conexión con el índice y el índice busca qué computadoras tienen esta canción. Si el índice muestra que el ordenador B tiene esta canción, se realiza una conexión directa peer-to-peer entre los ordenadores A y B, lo que permite a A descargar directamente el número de la computadora de B.

Napster es un modelo mixto de cliente-servidor y peer-to-peer. El elemento de índice central es cliente-servidor, pero los archivos reales se descargan peer-to-peer. El servidor de índice central ha demostrado ser un talón de Aquiles serio para Napster porque se puede cerrar fácilmente, lo que hace que Napster deje de funcionar. Debido a que Napster solo tiene un servidor de índice central, que enumera qué computadoras tienen qué archivos de música compartibles, Napster no tiene archivos de música en su servidor. Solo ha facilitado a los usuarios hacer conexiones peer-to-peer y compartir música entre sí.

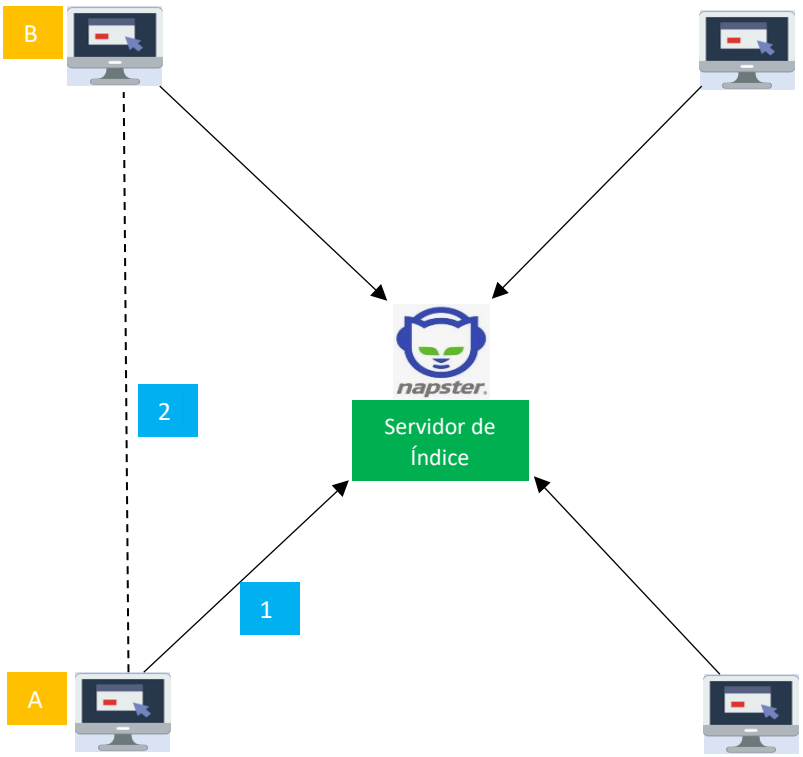


Figura 5: Red de Napster. (1) Computer A realiza una búsqueda en el servidor de índice central de Napster para Michael Jackson — Billy Jean. El servidor de índice central de Napster busca computadoras conectadas a la red que tengan el número disponible en su disco duro. (2) El ordenador B tiene el número. Colocando los ordenadores A y B una conexión directa peer-to-peer, después de lo cual el ordenador A descarga el archivo de música del ordenador B.

Si bien el intercambio de archivos de música es peer-to-peer con Napster, también incluye un elemento de servidor central, lo que lo hace propenso a ataques. En este caso, fue cerrado por la policía. Con la red Bitcoin, todos los nodos tienen una copia exacta del libro mayor público de Bitcoin. La red Bitcoin consta de muchos nodos, que se extienden por todo el mundo, lo que dificulta localizarlos y cerrarlos todos.

2.1.5 Blockchain

El libro mayor público de Bitcoin se considera descentralizado, ya que se distribuye entre nodos de todo el mundo. El libro mayor público de Bitcoin también se llama una cadena de bloques o una cadena de bloques que contiene los datos de la transacción. Si vemos la

Blockchain como una base de datos que registra información, estas son las propiedades inherentes esenciales de una Blockchain:

1. Los datos se organizan en bloques de datos.
2. Los bloques están ascendiendo gradualmente en números de bloques.
3. Los datos son confiables porque son criptográficamente verificables.

La cadena es la base de datos de transacciones que es construida por nodos que participan en el proceso de minería en la red Bitcoin. La cadena es mantenida por un servidor de marca de tiempo, que genera la prueba del orden cronológico de las transacciones. Cada bloque contiene una referencia hash al bloque sobre el que construye, lo que crea una secuencia lineal a lo largo del tiempo. Los bloques pueden ser considerados como las páginas individuales de un libro de registro.

Los mineros procesan constantemente las transacciones en bloques, que agregan al final de la cadena. El proceso del cual los mineros agregan nuevos bloques a la cadena también se llama ***Prueba de Trabajo***. Este proceso evita el ***doble gasto***.

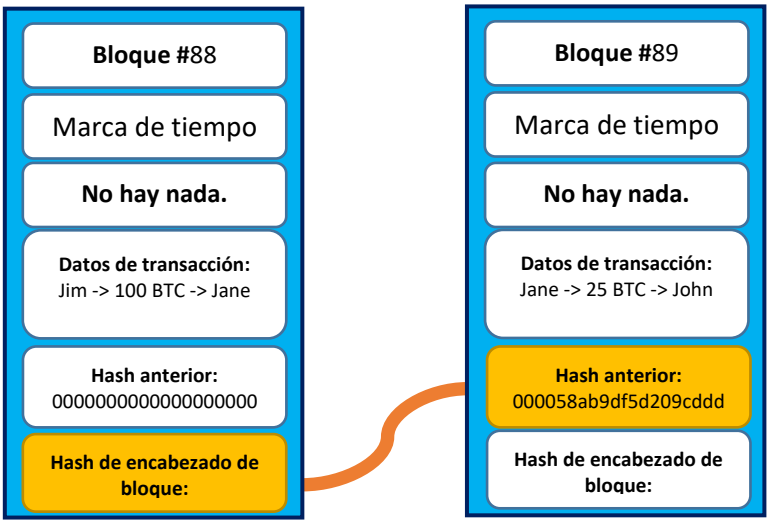


Figura 6: Representación simplificada de un bloque de génesis válido y bloque #2 con ambos bloques encadenados utilizando el hash del encabezado del bloque y el hash anterior. (Fuente: Lin Lim, C., Janse, A., Blockchain Basics, 2021, capítulo 3).

2.1.6 Doble gasto

Una cuestión importante que un sistema financiero electrónico peer-to-peer necesita resolver es la cuestión del doble gasto. El doble gasto es el acto de gastar un bitcoin más de una vez. Por ejemplo, si tienes 1 bitcoin y lo gastas en la persona A y la persona B al mismo tiempo. Dentro de una red financiera centralizada, el problema de doble gasto puede ser resuelto por un ***tercero de confianza (TTP)*** que mantiene el libro mayor y verifica todas las transacciones dentro del libro mayor.

Dentro de la red Bitcoin, este problema se resuelve a través de sus incentivos económicos y el uso de un servidor de marca de tiempo. Los mineros tienen un fuerte incentivo para no incluir estas transacciones en un bloque porque corren el riesgo de que su bloque sea rechazado por otros mineros, y además, serían cómplices en la realización de un delito.

2.1.7 Prueba de trabajo

Además de evitar el doble gasto, el propósito de la prueba de trabajo también es proteger a la red de los atacantes y llegar a un consenso sobre el estado del libro mayor público. En resumen, la prueba de trabajo es un mecanismo que requiere que los mineros usen la potencia de la computadora para encontrar los valores correctos para un bloque en el que están trabajando. Al encontrar el valor hash correcto, se les permite agregar el bloque a la Blockchain y recibir una recompensa en bitcoins. El proceso de encontrar el valor correcto se llama minería.

Las transacciones transmitidas a la red no son agregadas directamente a un bloque por el minero, ni se almacenan directamente en el libro mayor. Primero terminan en un ***pool de memoria*** (mempool) con otras transacciones que aún no se han agregado a un bloque por los mineros y que aún no han sido confirmadas por la red. Puede pensar en el mempool como un área de espera para todas las transacciones entrantes que aún no han sido confirmadas por la red. Cada minero tiene su propio mempool y es posible que los mempools individuales difieran por minero. Esto se debe a que siempre hay latencia de red dentro de una red informática: siempre toma un poco de tiempo para que una transacción enviada a la red llegue a todos los mineros de la red.

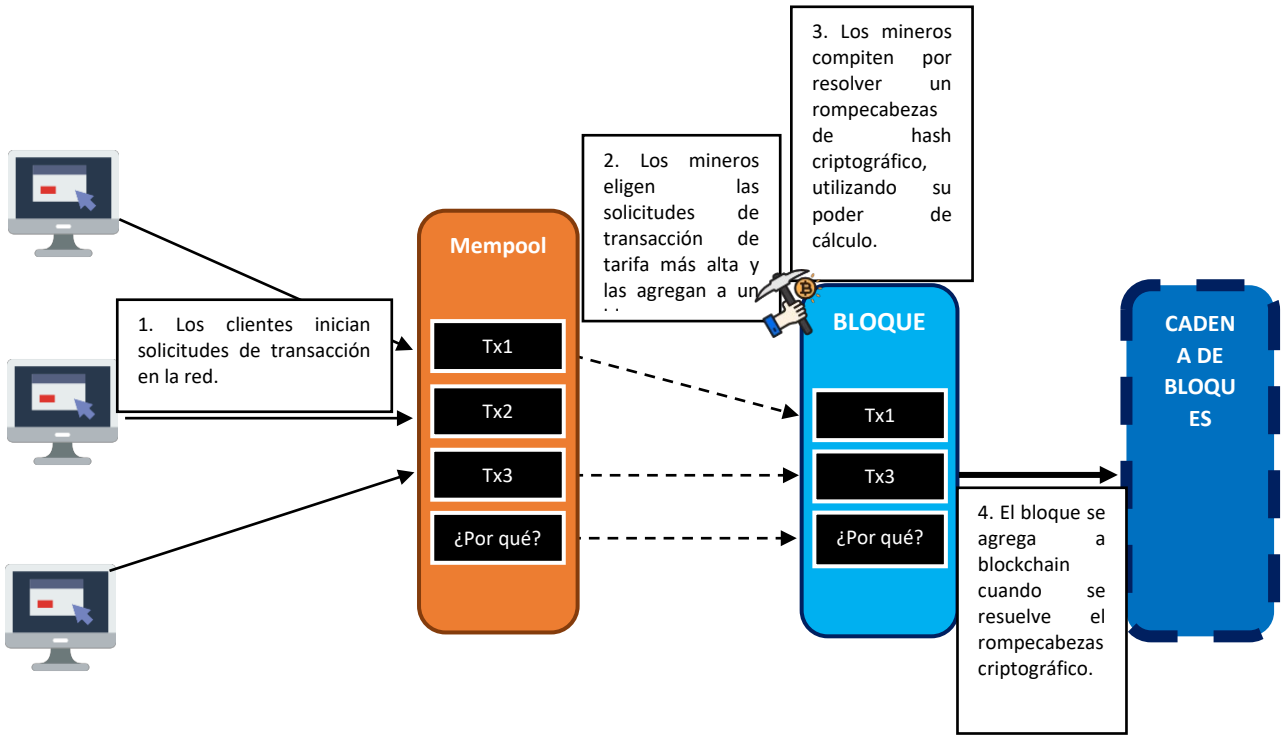


Figura 7:Representación esquemática de cómo se agrega una transacción a la Blockchain. El mempool es donde entran y se mantienen las transacciones no confirmadas. Los mineros eligen cuál de las transacciones del mempool quieren agregar al bloque. Posteriormente, intentan resolver un

rompecabezas criptográfico. Una vez resueltos, reciben una recompensa en bloque en bitcoins.(Fuente: Libro del libro: Lin Lim, C., Janse, A., Blockchain Basics, 2021, capítulo 4).

Cada transacción requiere tarifas de transacción. Se alienta económicamente a los mineros a agregar las transacciones de tarifas más altas a su bloque porque cobran estas tarifas cuando son los primeros en encontrar un hash válido para el bloque. Además de las tarifas de transacción, los mineros también reciben una recompensa por bloque, que se reduce a la mitad cada 210.000 bloques.

El sistema es seguro siempre y cuando los nodos honestos controlen colectivamente más poder de cálculo que cualquier grupo cooperante de nodos atacantes.

2.1.8 Descentralización

Los términos «red descentralizada y red distribuida» a menudo se utilizan indistintamente.3 La descentralización proporciona otra característica de seguridad importante con respecto a la destrucción de cualquier nodo único que aloja los datos como un SPOF. Las soluciones habituales que tienen las empresas es mantener múltiples copias para todo su sistema/aplicación alojada en centros de datos en múltiples ubicaciones. Esta es una enorme duplicación de costos que se necesita para la seguridad de los datos que Bitcoin logra solo por su diseño arquitectónico nativo.

- **Una Blockchain descentralizada requiere confirmaciones de nuevos datos de otros nodos**

Con un servidor centralizado, es relativamente fácil incluir nuevas inyecciones de datos en la base de datos. Los nuevos datos solo deben ser añadidos por una sola parte. Esto es diferente para una red descentralizada. Si los nuevos datos se agregan a una Blockchain por un minero, estos datos aún deben ser verificados por otros nodos completos y luego también incluidos en las Blockchain alojadas por otros nodos.

- **Una Blockchain descentralizada requiere consenso**

¿Qué pasa con las nuevas actualizaciones del protocolo de red? Una Blockchain descentralizada requiere consenso para actualizaciones y acuerdos sobre el estado correcto de la Blockchain.

- **Una Blockchain descentralizada es difícil de hackear**

A medida que el Blockchain se mantiene en diferentes nodos que pueden residir en diferentes lugares del mundo, es difícil hacerse cargo del control de la red. Para controlar la red, debe ser capaz de crear la cadena más larga que solo se puede lograr teniendo una potencia de cálculo mayoritaria. Le permite encontrar hashes de bloques válidos más rápido que el resto

[3] Debido a que Blockchain es una base de datos distribuida a través de diferentes servidores, esta tecnología también se conoce como ***Tecnología de Ledger Distribuido*** (DLT). Blockchain puede ser considerado un DLT, pero un DLT no siempre tiene que ser un Blockchain.

de la red combinada. Un ataque basado en la potencia de cálculo mayoritaria también se llama un ***ataque del 51 %***.4 Un ataque del 51 % te permite gastar dos veces.

- **Una Blockchain descentralizada complica la censura y el fraude**

El Blockchain, si se distribuye lo suficientemente lejos y ancho, es más a prueba de manipulaciones. Sin embargo, es posible cambiar o eliminar datos si hay consenso dentro de la red para hacerlo. Si asumimos que la red está bien descentralizada, podemos decir que la censura de Blockchain es difícil de lograr.

2.1.9 Privacidad

Satoshi Nakamoto declaró en su primer anuncio de la red Bitcoin que Bitcoin es anónimo, pero en realidad no es cierto. Bitcoin es pseudónimo. Esto significa que es privado pero no anónimo. Publica todas las transacciones en una Blockchain pública en texto claro para que cualquiera pueda auditar y ejecutar cosas como algoritmos de aprendizaje automático para realizar análisis de rastreo en él. Sin embargo, es privado, lo que significa que a menos que haya una necesidad de saber (como una orden judicial) y si el usuario la está utilizando con la intención de mantener su transacción financiera privada (no reutilizando sus direcciones públicas varias veces) ya que la privacidad está incorporada.

La privacidad todavía se mantiene manteniendo las claves públicas y su correspondiente dirección de billetera seudónimo. El libro mayor público permite a todos ver qué dirección ha hecho qué transacción, pero siempre y cuando sus direcciones sean desconocidas y no estén vinculadas a su información personal, puede realizar transacciones más bien «anónimamente».

En el documento técnico de Bitcoin, Satoshi también mencionó que como un firewall adicional para preservar la privacidad, se debe usar un nuevo par de claves para cada transacción para evitar que estén vinculados a un propietario común. Algunos enlaces todavía son inevitables con transacciones de múltiples entradas, que necesariamente revelan que sus insumos eran propiedad del mismo propietario. El riesgo es que si se revela el propietario de una clave, la vinculación podría revelar otras transacciones que pertenecían al mismo propietario.

La visión general de que Bitcoin es una moneda anónima es, por lo tanto, objetivamente incorrecta. Por el contrario, funciona como un libro abierto transparente y esto creó un espacio para todo un nuevo conjunto de criptomonedas centrándose en ser anónimos como monero, zcash y algunos otros. Muchos países ya están trabajando activamente en la legislación.

El modelo bancario tradicional alcanza un nivel de privacidad al limitar el acceso a la información a las partes involucradas y al tercero de confianza. La necesidad de anunciar todas las transacciones públicamente excluye este método, pero la privacidad todavía se puede mantener rompiendo el flujo de información en otro lugar: manteniendo las claves públicas anónimas. El público puede ver que alguien está enviando una cantidad a otra persona, pero sin información que vincule la transacción a nadie. Esto es similar al nivel de información

[4] Si bien el ataque del 51 % es el más conocido, muchos otros ataques también son posibles. Los ataques regulares que ocurren en redes centralizadas, como la corrupción de los desarrolladores principales, los errores en el código escrito incorrectamente o el robo de claves que dan acceso a los servidores también ocurren con Blockchains.

divulgada por las bolsas de valores, donde el tiempo y el tamaño de las operaciones individuales, la «cinta», se hace pública, pero sin decir quiénes eran las partes.

2.1.10 Resumen

Aunque existen muchos tipos diferentes de Blockchains y con diferentes niveles de descentralización, podemos concluir que en general una red Blockchain descentralizada tiene los siguientes atributos:

1. No hay un único punto de fracaso (SPOF).
2. Los nuevos datos deben ser confirmados por otros nodos.
3. Se requiere algún tipo de consenso para hacer actualizaciones y acordar el estado correcto de la Blockchain.
4. Es difícil hackear.
5. Hace que sea más difícil censurar o cambiar los datos en la Blockchain.
6. Es una red peer-to-peer, que no requiere confianza en un partido central.

Observaciones finales

- Las cadenas de bloques difieren de las bases de datos tradicionales.
- La razón por la que Napster falló es porque tenía un SPOF. Un Blockchain, por otro lado, no tiene SPOF y por lo tanto es más difícil de apagar.
- Una Blockchain es una red peer-to-peer.

Iconos utilizados

Ordenador fabricado por Prettycons de www.flaticon.com

Mina hecha por Strip de www.flaticon.com

2.2 Blockchain 2.0 y contratos inteligentes

«Queremos toda una secuencia de empresas: título digital, activos de medios digitales, acciones y bonos digitales, crowdfunding digital, seguros digitales. Si tiene confianza en línea como proporciona Blockchain, puede reinventar campo tras campo». **— Marc Andreessen (2014)**

2.2.1 Introducción

Objetivos de aprendizaje

- Qué es Blockchain 1.0 y por qué hay una necesidad de Blockchain 2.0.
- Ethereum es un ejemplo de Blockchain 2.0.
- Qué contratos inteligentes son.
- Qué son las aplicaciones descentralizadas (dApps).
- Qué son las organizaciones autónomas descentralizadas (DAO).

Introducción

El capítulo anterior discutió principalmente los principios básicos de Blockchain a través de Bitcoin. En este capítulo, cambiamos nuestra atención a una nueva generación de Blockchains que están específicamente destinadas a crear una plétora de otros tipos de aplicaciones descentralizadas o dApps. Una cadena de bloques específica en la que nos enfocamos es Ethereum, que también se promociona a sí misma como la computadora descentralizada del mundo.

2.2.2 Blockchain 1.0 y 2.0

La primera generación de Blockchains también se conoce como ***Blockchain 1.0***, que se centran principalmente en el dinero digital. Vitalik Buterin tuvo la idea de desarrollar una nueva Blockchain, Ethereum, en la que se podrían crear nuevas monedas, contratos con condiciones y requisitos e incluso ***aplicaciones descentralizadas*** en toda regla (dApps). Blockchains con tales capacidades también se conocen como Blockchains de segunda generación: ***Blockchain 2.0***.[5]

2.2.3 Ethereum

Ethereum fue introducido por primera vez por Vitalik Buterin en "Ethereum White Paper: una nueva generación Smart Contract & descentralization Application Platform" (2013). En el libro blanco, Buterin explica que Bitcoin se puede describir como un «sistema de primer archivo» en el que el orden de las transacciones es crucial. Técnicamente, Bitcoin puede considerarse

[5] Estas son Blockchains que han resuelto un grupo de problemas con los que Blockchain 2.0 todavía se enfrenta. Ejemplos de tales cuestiones son la escalabilidad, la interoperabilidad, la privacidad y la sostenibilidad y la gobernanza (Ackermann & Meier, p. 1). EOS, Cosmos, Cardano, Avalanche, Terra son ejemplos de Blockchains que podrían considerarse Blockchain 3.0.

un sistema de transición de estado simple donde (a) el «estado» consiste en el estado de propiedad de todos los bitcoins existentes y (b) la «función de transición de estado» que toma un estado y una transacción y produce un nuevo estado que es el resultado. Sin embargo, es difícil ejecutar contratos relativos a la transacción, que pueden capturarse en varios estados. Por ejemplo, es difícil transmitir una pieza de lógica que dice que Bob puede enviar su dinero a Alice, pero que Alice solo puede reclamarlo después de que ella haya proporcionado algo a cambio. (Buterin, 2013, p. 12)

El objetivo de Ethereum es proporcionar a los desarrolladores la capacidad de desarrollar aplicaciones basadas en términos y condiciones arbitrarios. El lenguaje de programación desarrollado específicamente para Ethereum se llama ***Solidity***.

2.2.4 Transacciones de Ethereum y gas

La criptomoneda subyacente de Ethereum Blockchain es el éter (ETH). Hacer una transacción en la red Ethereum requiere ***gas***. El gas se expresa en la criptomoneda Ether. El gas en la red Ethereum es básicamente lo mismo que los costos de transacción. Esto se calcula utilizando los costos estándar por unidad de potencia de cálculo x el número de unidades. Puede especificar una cantidad específica de gas, o costos de transacción, para cada transacción que realice. El usuario debe pagar una cantidad adecuada de gas para la transacción. Si se paga muy poco gas, los mineros pueden no incluir la transacción en el bloque y, por lo tanto, esta transacción no se ejecutará. Además de la recompensa de bloque, el minero también recibe todas las tarifas de gas que se incluyeron con las transacciones en el bloque.

La razón económica criptográfica por la que el gas se ha introducido en la red Ethereum es que prioriza transacciones importantes. Un bloque solo tiene espacio para un número limitado de transacciones. El sistema de gas asegura que no se desperdicia energía en spam o transacciones de bajo valor.

2.2.5 Contratos inteligentes

Un contrato inteligente es la automatización descentralizada y puede definirse como un contrato con ciertos términos y condiciones que se establecen en el código. El contrato es autoejecutable, ya que realiza las acciones correspondientes apropiadas cuando se cumplen los términos y condiciones.

Por ejemplo, un contrato inteligente podría ser un contrato de trabajo, donde Alice quiere pagar a Bob 500 EUR para desarrollar un sitio web. El contrato podría funcionar de la siguiente manera:

1. Alice pone 500 EUR en el contrato y los fondos están bloqueados.
2. Cuando Bob ha desarrollado el sitio web, Bob envía un mensaje al contrato para liberarle los fondos.
3. El fondo se libera cuando Alice está de acuerdo.
4. Si Bob decide no finalizar el sitio web, Bob puede cancelar su trabajo enviando un mensaje al contrato, después del cual el fondo se devuelve automáticamente a Alice.

5. Si Bob afirma que ha completado el sitio web, pero Alice no está de acuerdo, un juez podría ser llamado después de un período de espera de 7 días para expresar un veredicto a favor de Alice o Bob. (Buterin, 2014)

Ventajas de los contratos inteligentes

Los contratos inteligentes ofrecen muchas ventajas. ChainTrade (2017) ha enumerado los once siguientes:

1. *Precisión:* Todos los términos y condiciones deben registrarse en detalle en un contrato inteligente. Si se omiten ciertas condiciones, esto puede conducir a un comportamiento no deseado del contrato inteligente.
2. *Transparencia:* todos los términos y condiciones son totalmente visibles y accesibles para todas las partes involucradas. Una vez finalizado el contrato, ya no podrá disputarlo.
3. *Comunicación clara:* la necesidad de contratos inteligentes meticulosamente definidos garantiza que la comunicación en el contrato esté claramente establecida de modo que no haya margen para la mala comunicación y la mala interpretación.
4. *Velocidad: los contratos*inteligentes pueden automatizar y acelerar significativamente los procesos comerciales tradicionales. No es necesario presentar ninguna solicitud para su aprobación y no hay que procesar o aprobar documentos por parte de particulares.
5. *Seguridad: los contratos*inteligentes se ejecutan en plataformas Blockchain y utilizan el cifrado de datos.
6. *Eficiencia:* Debido a la precisión y velocidad, los contratos inteligentes ejecutan los procesos de negocio de manera más eficiente o incluso los eliminan por completo.
7. *Libre de papel:* no se requiere papeleo para la ejecución de contratos inteligentes.
8. *Almacenamiento y copia de seguridad: los contratos*inteligentes y sus detalles se almacenan permanentemente en Blockchain. Como resultado, no se pueden perder y son fáciles de encontrar.
9. *Ahorro de costos: los contratos*inteligentes pueden ahorrar muchos costos, porque hay menos necesidad de intermediarios como abogados, testigos y bancos para interpretar y

2.2.6 Aplicaciones descentralizadas

Definimos una ***aplicación descentralizada*** (dApp) como una aplicación que utiliza el almacenamiento de datos descentralizado de una Blockchain. La aplicación no se ejecuta a través de un servidor central, sino a través de una red descentralizada de nodos. Al igual que una aplicación normal, a menudo tiene un front-end y una interfaz de usuario. La interfaz ofrece al usuario una interacción más fácil con los contratos inteligentes y la Blockchain. Al almacenar y ejecutar los contratos inteligentes que componen el código central de una dApp de manera descentralizada, no hay un único punto de falla. El funcionamiento de la aplicación y los datos de la aplicación no pueden ser simplemente censurados o eliminados.

2.2.7 Organización autónoma descentralizada (DAO)

Las***organizaciones autónomas descentralizadas*** (DAO) se pueden definir como una organización no jerárquica que realiza y registra tareas rutinarias en una Blockchain. Las reglas

a las que se adhiere el DAO también se registran en la Blockchain. Además, la DAO depende de las contribuciones voluntarias de las partes interesadas internas para guiar a la organización a través de un proceso de consulta democrática. (Hsieh et al., 2018, p. 2)

Lo que hace que un DAO sea fundamentalmente diferente de una organización centralizada es que no tiene un equipo de alta dirección o un CEO. Tampoco tiene sucursales, empleados o subsidiarias. En cambio, existe un DAO en una red descentralizada de usuarios y nodos que recopilan, verifican y actualizan transacciones en una Blockchain. Las decisiones sobre los cambios en el código se toman por procesos democráticos de votación. Es una forma radicalmente diferente de establecer una organización empresarial. Debido a su naturaleza autónoma, después de todo, es un sistema autosuficiente y autoorganizado, Bitcoin puede caracterizarse como un DAO, porque (a) ejecuta un sistema de pago, (b) emplea subcontratistas que trabajan como mineros y (c) paga a estos subcontratistas con bitcoins recién distribuidos (Vigna & Casey, 2015, p. 229). Además, los mineros pueden votar a favor de propuestas de mejora del protocolo por medio de su potencia de cálculo. Las DAO están controladas por un proceso colectivo de toma de decisiones de las partes interesadas a través de un protocolo descentralizado y no están influenciadas por un órgano de gobierno central.

Observaciones finales

- Con Blockchain 2.0, se puede construir una plétora de nuevos tipos de aplicaciones.
- Puede desarrollar contratos inteligentes en Ethereum donde los términos y condiciones están tan claramente establecidos que en caso de incumplimiento del contrato, ya no se requiere interpretación de terceros.
- Bitcoin es un sistema de primera en presentar.
- Bitcoin es la primera organización autónoma descentralizada (DAO).

3 Tipos de Blockchain

En este capítulo dividiremos Blockchain en sus tipos desde tres perspectivas, el protocolo de consenso, la gobernanza y los tipos de cooperación entre los sistemas Blockchain.

3.1 Tipos de Blockchain según protocolo de consenso

Los protocolos de consenso son esenciales para garantizar la confianza entre los diferentes participantes dentro de una red distribuida. Debe haber confianza en que los participantes no están corruptos y que los datos que se comparten entre ellos no están corruptos. Para garantizar esta confianza, los nodos participantes deben verificar los mensajes o transacciones para verificar la corrección y neutralizar a otros participantes que son corruptos y engañosos: la solución al problema de los generales bizantinos como se discutió en el capítulo anterior.

Como un protocolo de consenso, por lo tanto, toca la esencia de un sistema Blockchain que se utiliza aquí como una forma de discernir los tipos de Blockchain.
En el capítulo anterior se introdujo el primer protocolo de consenso, **Proof-of-Work**, utilizando el Bitcoin como ejemplo. De acuerdo con este protocolo, un bloque de datos solo se puede agregar a la Blockchain cuando se ha encontrado un hash válido del bloque. A medida que los mineros de Bitcoin entraron en una feroz competencia en la potencia informática para recibir las recompensas de encontrar un hash válido primero, el consumo de electricidad de la red Bitcoin ha llevado a preocupaciones sobre los efectos negativos de Blockchain para el medio ambiente. La búsqueda resultante de soluciones más sostenibles al problema de los generales bizantinos ha llevado a protocolos de consenso alternativos.
Una de las principales alternativas a la prueba de trabajo es la prueba de participación que ahora se ha implementado en varios proyectos de Blockchain con el notable ejemplo de Ethereum que se está transfiriendo a la prueba de participación en 2022.

Mientras que a los mineros de Proof-of-Work se les permite producir nuevos bloques cuando pueden encontrar un hash válido, un productor de bloques en Proof-of-Stake se elige en base a (a) un proceso de selección al azar y (b) **una «stake»** como el número de monedas que tiene. Como consecuencia, no necesita poder de cómputo para participar. Todo lo que se necesita es una computadora estándar, una conexión a Internet y tener una moneda. Por lo tanto, al productor de bloques de Proof-of-Stake no se le llama minero, sino ***falsificador***. Debido a que el falsificador también recibe una recompensa al producir un nuevo bloque, también puede **falsificar** la prueba de participación como un método en el que obtiene un ingreso pasivo en sus monedas. Cuanto más apuesta tengas, mayor será la probabilidad de que produzcas el siguiente bloque. Además de producir bloques, los falsificadores también validan las transacciones, ayudando a proteger la red.

Además de la eficiencia energética, las ventajas de la prueba de participación de la prueba de trabajo son que la facilidad de staking permite que la Blockchain se distribuya mejor y que realizar un ataque del 51 % sea menos atractivo.

Hay diferentes variantes dentro de la Prueba de Estaca que tienen sus propias propiedades únicas. En primer lugar, en la **Prueba de Estaca Delegada** cualquier persona que tenga una moneda puede votar por testigos y delegados. Los testigos validan las transacciones y producen nuevos bloques por los que reciben una recompensa. Los delegados supervisan la estructura de gobierno del protocolo Blockchain. Como resultado, la prueba de participación

delegada puede manejar más transacciones por segundo que las Blockchain que están más descentralizadas.
En segundo lugar, en una **prueba de participación arrendada, todos** pueden arrendar sus monedas en los nodos en juego, aumentando así la posibilidad de que los nodos de estaca produzcan un bloque. Los nodos de estaca distribuyen su recompensa proporcionalmente entre ellos y los arrendatarios. Como resultado, este protocolo alienta a las personas a participar en el proceso de staking.

En tercer lugar, con **Proof-of-Stake Velocity** los usuarios son recompensados por (a) el número de monedas que tienen y (b) qué tan activamente utilizan sus monedas. Por lo tanto, se anima a la comunidad a no solo conservar las monedas, sino a utilizarlas realmente para las transacciones.

En cuarto lugar, con **Proof-of-Authority**, los productores de bloques (nodos de autoridad) están autenticados y aprobados en función de su identidad y reputación. Al vincular la reputación a la identidad, los nodos de autoridad se estimulan extra para mostrar un buen comportamiento y no para incluir transacciones maliciosas en Blockchain. Si lo hacen, causará daño a la reputación. La prueba de autoridad es un ejemplo de creación de una variante de prueba de participación donde la posibilidad de crear un nuevo bloque no depende completamente del número de monedas que apostes.
Tenga en cuenta que es dudoso si la prueba de autoridad cae bajo prueba de participación. A veces se piensa que es una forma de prueba de participación delegada y se usa más comúnmente en Blockchains cerradas y autorizadas.

Una ventaja de tipificar la Blockchain utilizando protocolos de consenso es que ayuda a explicar las diferencias en la **escalabilidad de Blockchains**. Esto como escalabilidad en general depende de la influencia de los protocolos de consenso sobre el tiempo de bloque, el tamaño del bloque, el nivel de distribución o descentralización de la Blockchain y la forma en que se producen los bloques, las transacciones se envían a la Blockchain y se verifican las transacciones. Para mejorar esta escala, se prueban diferentes soluciones, como tomar transacciones fuera de la cadena. Ejemplos bien conocidos de esto son la red de rayos, plasma (ambos llamados soluciones de 'capa 2') y sharding.

3.2 Gobierno de blockchain y quién puede participar con qué rol

Una Blockchain, como cualquier asociación, necesita ser administrada y controlada. La estructura de gobierno de Blockchain resultante ofrece una segunda manera de discernir los tipos de Blockchain que se discutirán aquí.

Los elementos de gobernanza notables son:

1. **Derechos** a presentar, ejecutar y supervisar las propuestas de **decisión** de un grupo o de todos.
2. **Rendición de cuentas** y derecho a supervisar las decisiones y comportamientos y a rendir cuentas de sus responsabilidades.
3. **Incentivos** y alentar a los participantes a mantener la Blockchain.

La forma en que se interpretan estos elementos depende de los objetivos que persigue la asociación y, por lo tanto, del tipo de gobernanza que necesita.

Una de las necesidades de gobierno puede ser que un grupo central de personas ejerza el control y dicte términos (mentalidad de control**central)**, frente a las necesidades de un grupo más grande de trabajar juntos en igualdad de condiciones sin una jerarquía o control central (mentalidad de control**descentralizado**).

El tipo de control que se ejerce se utiliza para decidir a quién se le concede permiso para participar en una Blockchain o no. Si las autoridades centrales conceden el acceso, el Blockchain es el tipo Blockchain **privado**. Si el acceso se organiza para todos, el Blockchain se llama Blockchain **público**. Los tipos de Blockchain público y privado se encuentran combinados en el **consorcio** tipo Blockchain, una forma intermedia que está más centralizada que una Blockchain pública y más descentralizada que una Blockchain privada.

En un consorcio, múltiples organizaciones trabajan juntas para establecer una Blockchain y el consenso es administrado por una selección de nodos. El consorcio decide para toda la red quién puede participar en qué función, qué transacciones se pueden ver abiertamente o pueden protegerse de otros participantes y cómo debe estructurarse la gobernanza.

Usted utiliza principalmente una **Blockchain pública**, donde todos son tratados por igual, si desea que un grupo de personas de ideas afines trabajen juntos. La cooperación está garantizada aquí por el mecanismo de consenso que actúa como una «máquina de confianza». «Acceso a todos» conduce a un mayor número de nodos que crean confianza en el sistema Blockchain. Un Blockchain público muestra un menor grado de confianza en las autoridades que gobiernan la Blockchain en nombre de otros. Esta actitud hacia la confianza y la confianza favorece la decisión de protocolos de consenso con un carácter más descentralizado, la confianza en la naturaleza de código abierto de su Blockchain, así como la necesidad de una total transparencia en la toma de decisiones. Por lo tanto, esta actitud conduce a una mayor confianza en que los extraños se unan y participen en la asociación. Después de todo, la confianza radica en el sistema y no en el usuario.

En general, una empresa que se inclina hacia una **Blockchain privada**, querrá saber quién está en el sistema Blockchain. Piense en una intranet en la que compruebe los nodos, los datos y el código fuente. Usted sabe que todos y todas las transacciones se pueden ver si esto es necesario, pero también protege a las personas de verificar o ver ciertas transacciones. Esto es útil cuando los datos son sensibles a la empresa. En un sistema público también es posible construir esto técnicamente, pero por el momento en la práctica esto resulta ser un desafío.

Por lo tanto, en una Blockchain privada es relevante estar al tanto de todos los roles que asigna a los participantes a los que concedió acceso. Una función importante es la posibilidad de **mantener el mecanismo de consenso**. ¿Debería darse esta posibilidad a todos los participantes en la Blockchain o solo a un grupo selecto?

La respuesta a esta pregunta conduce a los tipos de **Blockchain sin permiso y con permiso**.

Si a cada participante a la Blockchain se le permite mantener el mecanismo de consenso, se trata de un **tipo Blockchain sin permiso**. Si el rol para mantener el mecanismo de consenso está reservado para un grupo selecto, estamos hablando de un tipo de Blockchain autorizado.

Además de mantener el consenso, hay roles que le permiten ejecutar, ver y ajustar transacciones en Blockchain, técnicamente mantener la Blockchain o participar en la votación de ideas. Estos roles no son relevantes para la elección entre un sistema sin permiso o con permiso. Sin embargo, estas funciones son pertinentes para la naturaleza de las asociaciones. Esto es relevante porque si a las autoridades no les importa quién accede al sistema y confía

en el propio sistema, lo más probable es que esté inclinado a otorgar el anonimato a los participantes. Actualmente las empresas que utilizan sistemas de control de gestión Classis, sin embargo, optarían por conocer a las personas a las que conceden acceso, así como elegirían saber qué roles hay y a qué participante pueden otorgar qué papel.

Al segregar los roles, estas empresas pueden seguir utilizando su estructura organizativa subyacente. Por lo tanto, pueden hacer cumplir la identidad de su empresa dentro de su Blockchain, ya que controlan el perfil de las personas, así como sus roles. Además de transferir parcialmente la confianza al sistema, pueden continuar administrando su organización, su propio sistema de control de gestión, como la gestión específica del personal.

Esto ayuda a explicar por qué dentro de un sistema sin permiso, los tokens criptográficos están disponibles para fomentar la colaboración.

Los diferentes tipos de Blockchain se utilizan en combinación en Blockchains de hoy:

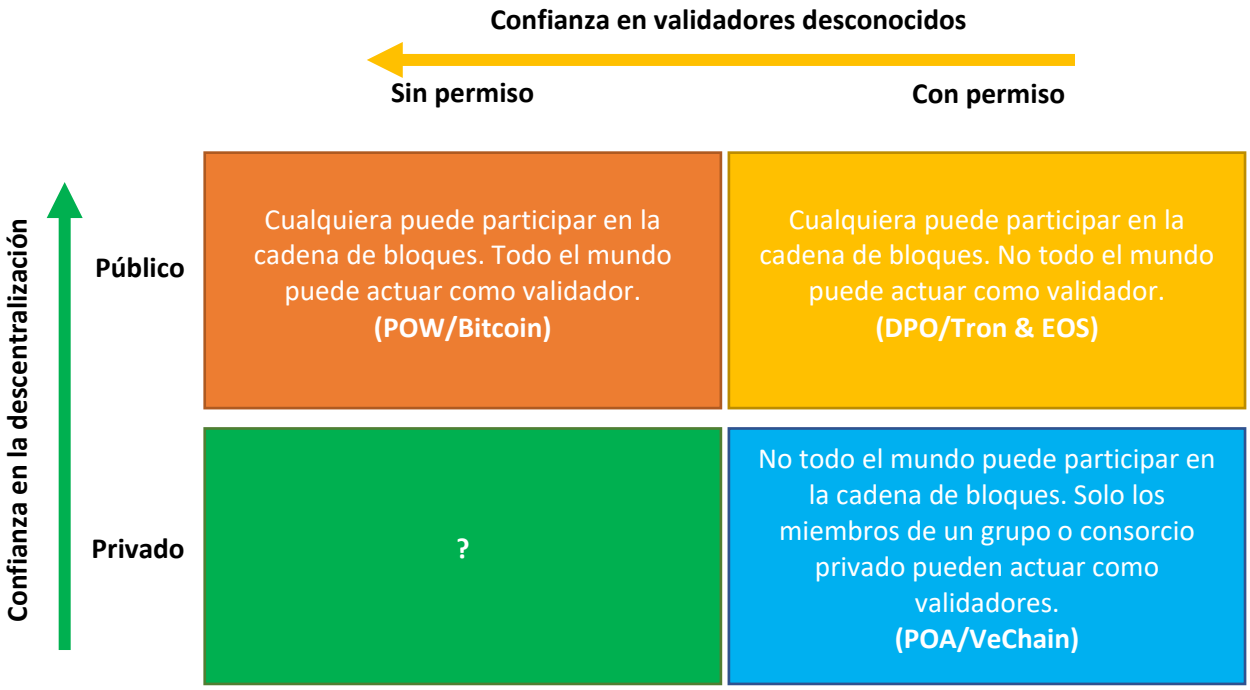


Figura 8: Una visión general de los diferentes tipos de Blockchain, expresado en sin permiso, con permiso, privado y público (Fuente: Lin Lim, C., Janse, A., Blockchain Basics, 2021, capítulo 9).

Con la confianza en el sistema con Blockchains públicas, se considera de menor importancia al «quien escribe datos a la cadena de bloques», «quién lee datos de la cadena de bloques» y «a quién se le permite mantener la cadena de bloques». Esto, a su vez, lleva a que la mayoría de las cadenas de bloques públicas no tengan permiso. Debido a la baja barrera para unirse a la red, tales Blockchains son los más descentralizados.

Los participantes determinan el funcionamiento de la Blockchain en línea con motivos grupales como la apertura, la neutralidad y la libertad. Dentro de la Blockchain pública, todos pueden participar en la toma de decisiones sobre todos los asuntos de gobernanza.

Un Blockchain **público** no siempre es deseable para las empresas, especialmente en un entorno más regulado en el que se espera, entre otras cosas, que conozcan la identidad de todas las partes que escriben datos a la Blockchain.

Este partido central a menudo ha establecido una serie de nodos que se administran a sí mismos y que mantienen la cadena de bloques funcionando juntos. En el caso más extremo, la fiesta tiene un solo nodo en el que se ejecuta Blockchain. Sin embargo, esto no ofrece ninguna ventaja sobre una red centralizada que también es un SPOF.

Las opciones entre los diferentes tipos de Blockchain afectan el control de la organización. Cuanta más confianza haya en la naturaleza descentralizada de Blockchain, más fácil será participar. Cuanta más confianza haya en que los validadores puedan participar en la construcción de consensos como incógnitas, más transparente será el sistema. Después de todo, todos pueden ejecutar un nodo completo y ayudar a validar todos los datos. Debido a la naturaleza descentralizada, estos sistemas a menudo tienen muchos validadores y, en parte debido a esto, todavía tienen problemas de escalabilidad. Además, tales Blockchains son relativamente más caros que las variantes menos descentralizadas y autorizadas.

A la larga, sin embargo, se espera que una Blockchain pública sin permiso se vuelva cada vez más eficiente, por lo que las partes más profesionales optarán por tales Blockchains. Estas Blockchains deben organizarse de tal manera que los roles que los participantes pueden asumir para aplicaciones empresariales estén bien definidos y cumplan con los requisitos del negocio. Por ejemplo, las empresas en Blockchains públicas sin permiso pueden anonimizar los datos a través de pruebas de conocimiento cero y se puede pedir a los participantes a nivel de aplicación que muestren su identidad.

3.3 Plataformas y consorcios

Una Blockchain donde diferentes compañías y terceros cooperan sin que un usuario central controle esta Blockchain, se llama Blockchain empresarial. Para construir una Blockchain de este tipo, las empresas utilizan plataformas Blockchain. Estas **plataformas** le permiten escribir aplicaciones utilizando ciertas tecnologías. Se han organizado varias asociaciones en torno a estas plataformas. Las plataformas son la tercera y última forma en que vemos los diferentes tipos de Blockchain aquí.

Las **plataformas** blockchain permiten que su aplicación colabore con otras aplicaciones, por ejemplo, en su lenguaje de programación propio o compartido, se almacenan o comparten documentos y se obtiene acceso a una red específica. Las dos plataformas más destacadas son actualmente Ethereum y Hyperledger, con Corda como la tercera más prominente.

Cada plataforma tiene sus propias características únicas. Ethereum es, en general, una cadena de bloques pública, Hyperledger ofrece módulos plug-and-play utilizando varias tecnologías, y Corda es una tecnología Ledger descentralizada que está más especializada en servicios financieros. Los miembros que se han unido a una asociación en torno a una plataforma a menudo también son miembros de asociaciones alrededor de las otras plataformas. Las plataformas en sí son de código abierto. Ethereum y Hyperledger han estado luchando por una mayor integración entre los dos en los últimos años en su objetivo mutuo de implementar sistemas Blockchain en compañías de todo el mundo.

Cuando las asociaciones se refieren a una forma de cooperación de Blockchains en la que los nuevos participantes son conocidos y asignados roles específicos, trabajan en estructuras que,

confusamente, también se llaman consorcios (véase el párrafo 3.2 anterior), pero desde otra perspectiva entonces mezclan las características de Blockchain públicos y privados solo. Las partes que cooperan pueden variar desde organismos gubernamentales, grupos de interés e incógnitas, hasta proveedores, clientes y competidores directos.

Además, los consorcios aquí ayudan a las partes a superar cuatro desafíos principales que las organizaciones enfrentan en la implementación de Blockchain. En primer lugar, los consorcios comparten conocimientos y mantienen un contacto activo con los organismos nacionales de supervisión (supra). Los consorcios ayudan a aclarar las leyes y reglamentos, entre otras cosas.

En segundo lugar, los consorcios ayudan a las organizaciones a difundir los riesgos sobre diferentes partes compartiendo recursos para desarrollar sistemas Blockchain.

En tercer lugar, a través de la colaboración, los consorcios proporcionan masa crítica para adoptar un sistema de rendimiento estable.

Y cuarto, los consorcios dan la oportunidad de establecer nuevas asociaciones descentralizadas con partes confiables y no confiables, sin que las organizaciones participantes pierdan demasiado de su autonomía. Esto ofrece a los competidores, por ejemplo, procedimientos estándar para crear e intercambiar datos entre sí, o colaborar con los clientes y proveedores de cada uno. Sin embargo, como las partes participantes tendrán que confiar mutuamente para trabajar juntas, por lo general hacen cumplir su confianza con contratos sobre recursos compartidos, toma de decisiones, sanciones, información sensible e intercambio de datos mutuos. Estos contratos tienden a elevar la barrera para unirse a un consorcio, ya que aumenta la barrera para salir de un consorcio. Es probable que coexistan diferentes consorcios. La interoperabilidad dentro de los consorcios y entre ellos desempeña un papel importante en esto.

4 Criptomonedas y tokens

Uno de los grandes inventos de Satoshi Nakamoto es la combinación de tecnologías preexistentes con un sistema de recompensa que mantiene una red descentralizada en funcionamiento. Como se mencionó anteriormente, la recompensa en Bitcoins se paga al minero que produce un bloque.

Los**tokens** en nuestra sociedad actual se conocen como vales y monedas, por ejemplo, puntos de lealtad, monedas de casino y tarjetas de regalo. También conocemos tokens en TI que proporcionan derechos de acceso a una red para realizar una tarea o como representaciones de derechos sobre activos subyacentes. Un Bitcoin, que también podría ver como un token criptográfico, difiere de los tokens mencionados anteriormente en el sentido de que representa valor. Los tokens criptográficos se pueden utilizar por muchas razones. En el panorama Blockchain, sirven principalmente a un **Internet de Valor** donde los valores se pueden intercambiar a través de un Internet descentralizado de una manera confiable.

Con tokens criptográficos como Bitcoin, puede pagar o ahorrar, pero también puede llevarlo un paso más allá. Bitcoin, por ejemplo, se puede ganar suministrando energía informática para producir nuevos bloques. Por lo tanto, crea una economía en la que se anima a varios participantes a ayudar a proteger la red a cambio de criptografía. El uso de tokens criptográficos para estimular cierto comportamiento de los participantes y para castigar el comportamiento incorrecto a través de un protocolo de consenso es parte de **la criptoeconomía**.

En este capítulo, 4.1 primero describe **la criptoeconomía** como el concepto base en el que los tokens están demostrando desempeñar un papel útil. Posteriormente, 4.2. describe **qué son los tokens** y los **clasifica**. Esta clasificación incluye tokens dApp y criptomonedas, pero también la diferencia entre token fungible y no fungible y cómo apoyan la economía criptográfica. El capítulo se continúa en la sección 4.3 con una visión general de cómo los tokens pueden ser utilizados para la recaudación de fondos por una Oferta Inicial de Monedas, Oferta de Tokens de Seguridad y Oferta de Intercambio Inicial.

4.1 Criptoeconomía

Los tokens criptográficos sirven para diferentes propósitos, como acceder a un sistema o representar información desde un objeto físico. Esto proporciona a los tokens un **valor** que se puede intercambiar entre diferentes partes dentro de una Blockchain. Esta nueva disciplina que estudia la transferencia de riqueza a través de redes informáticas, criptografía, teoría de juegos y desarrollo de software, junto con la creación y el consumo de riqueza, se **llama criptoeconomía.**

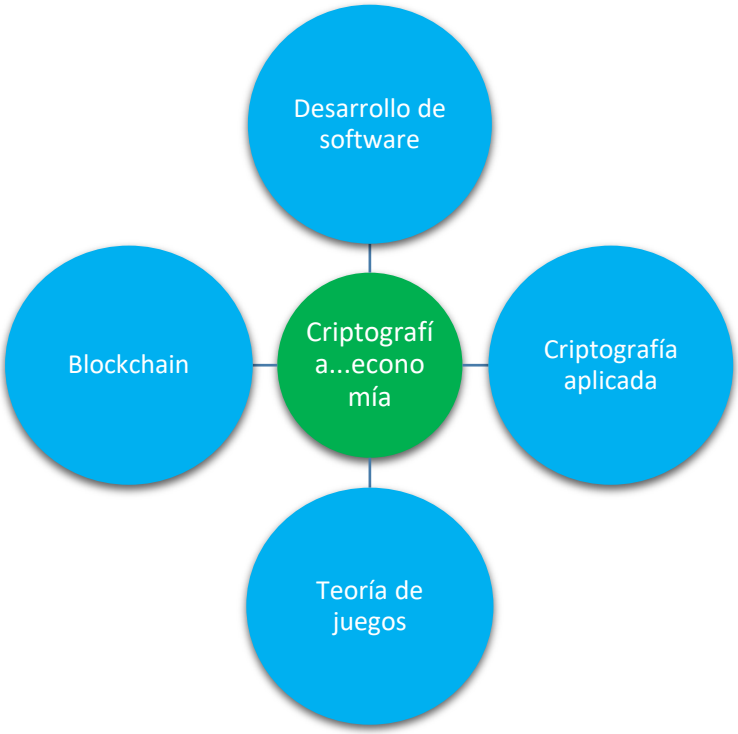


Figura 9: Aspectos multidisciplinarios de la criptoeconomía. (Fuente: Lin Lim, C., Janse, A., Blockchain Basics, 2021, capítulo 10).

Las redes informáticas están diseñadas con ciertas reglas que actúan como una especie de ley para todos los que participan. Sin embargo, estas leyes están diseñadas por partes/comunidades privadas y en parte aplicadas por software en lugar de por gobiernos. Dentro de estas leyes, entonces, se hacen suposiciones sobre cómo los participantes pueden comportarse y comportarse mal dentro de la red.

La idea central detrás de la criptoeconomía dentro de **Blockchain** es que se desarrollan protocolos que alientan a las personas a participar en la red de tal manera que el **valor** de la red **se maximice** para los participantes. El valor de la red solo se puede maximizar si la red y las transacciones que tienen lugar en ella también están **aseguradas**. Para lograr esto, la **criptografía** se utiliza para proteger las transacciones dentro de la red a través de **software** como, por ejemplo, funciones hash y firmas digitales. Además, se pagan recompensas a los participantes que ayudan a proteger la red a través de, por ejemplo, minería o staking. La combinación de este pensamiento se ejemplifica en el papel de Bitcoin como un token que estimula a las personas a colaborar y así ayudar a mantener un sistema cripto-económico autoorganizado. La criptoeconomía es una premisa importante para apoyar la idea de un sistema sostenible y preferiblemente autoorganizado, sin que las partes centrales insten a las personas a actuar de cierta manera. Importante para esta premisa es la **teoría de*juegos,*** un estudio sobre cómo se crean condiciones óptimas en un entorno competitivo con el fin de que los participantes siempre elijan mostrar un buen comportamiento en sus elecciones, ya que esto conduce a más ganancias que malas conductas. Una forma de alentar a los participantes en el buen comportamiento es a través de las recompensas de tokens criptográficos.

4.2 Clasificación de tokens Blockchain

Internetse creó inicialmente para intercambiar información entre sí. Esto también se conoce como **Internet de la Información**. Dentro de esto, es difícil almacenar y mover valor sin un intermediario de confianza (Tapscott, 2016) que comprueba principalmente si un valor, como el euro, no se gasta dos veces (Satoshi, 2008, p. 2). Con el advenimiento de Blockchain, puede evitar la necesidad de intermediarios y comercio de valor peer-to-peer directamente. Esto también se conoce como **Internet del Valor**. Los tokens criptográficos desempeñan un papel fundamental en la contribución a este sistema económico criptográfico. Un token criptográfico se puede crear en una cadena de bloques y también representa un activo negociable. A veces los tokens se crean en una ICO o una STO para financiar un proyecto. El proceso de creación de tokens se llama **tokenización**. El comercio de estos tokens le permite transferir la propiedad a los activos subyacentes.

Hay diferentes perspectivas de cómo ver los tokens criptográficos. El siguiente formato encapsula todos los tokens diferentes con la ventaja añadida de abordar el papel futuro de los tokens en un Internet de Valor:

Aplicación	Token en beneficio de la aplicación	Token como activos
Fichas fungibles	De la red: Éter dApp: Augur	Activo: el oro Seguridad: parte Shell Moneda criptográfica: Bitcoin
Fichas no fungibles		Activo: certificado de nacimiento Seguridad: préstamo personal

Figura 10: Formato dual de tokens. Por un lado, distinguir tokens que se utilizan a la red Blockchain para mantener frente a demostrar y transferir la propiedad. Por otro lado, distinguir tokens que intercambiables de no ser intercambiables. (Fuente: Lin Lim, C., Janse, A., Blockchain Basics, 2021, capítulo 10).

Tenga en cuenta que los tokens pueden tener una estructura de token dual en la que sirven múltiples propósitos al mismo tiempo. Por ejemplo, Bitcoin se utiliza como un token de red o aplicación y un activo.

Los**tokens en beneficio de la aplicación** se utilizan en el nivel más básico para alentar a las personas a participar en una aplicación Blockchain y mantener esta red en funcionamiento. Esta red puede servir como una plataforma en la que se ejecutan aplicaciones descentralizadas, dApps. Aquí los **tokens de red** se utilizan para **recompensar a los**

participantes por el trabajo que hacen para ayudar a mantener la red. Estos tokens ocupan un lugar central dentro de una Blockchain, porque como idea organizacional apoyan una red de confianza distribuida y, por lo tanto, dan forma al sistema cripto-económico de una Blockchain. Además de una aplicación, una red también puede ser una **plataforma** en la que las aplicaciones se ejecutan como en Ethereum o Cardano con sus tokens ETH y ADA para lograr consenso y recompensar el sistema de transacción. Tomando el pensamiento un paso más allá se puede ver que dentro de una Blockchain existe la opción de usar un token, o ignorar el uso de tokens todos juntos.

los tokens dApp, o **tokens de utilidad**, solo son útiles dentro de su propia aplicación y se utilizan para acceder a esta utilidad. No sirven de nada fuera de esa aplicación. Todavía puede intercambiarlos fuera de la aplicación. Sin embargo, no siempre están programados como moneda o participación en una red. Por ejemplo, Siacoin (SC) donde las personas pueden ganar SC cuando ponen su espacio libre en disco disponible para otros en la red.

los tokens dApp en Ethereum se realizan de acuerdo con el protocolo **de solicitud de comentarios 20** (ERC-20). El protocolo define ciertas reglas y estándares relacionados con la emisión de tokens en la red Ethereum. Todos los tokens dApp hechos según ERC-20 son únicos para su aplicación y se pueden comercializar dentro de la red Ethereum.

Los tokens en beneficio de las aplicaciones difieren de los tokens que giran en torno a la captura e intercambio de valor dentro de las aplicaciones Blockchain por las que demuestran la posesión de este valor y permiten la transferencia del derecho a este valor, **tokens como activos**. Esto se puede subdividir en tokens de activos, tokens de seguridad y monedas criptográficas.

Los tokens de activos representan registros de derechos y obligaciones con el activo subyacente, como el oro o el petróleo, pero también para una casa, un clip de papel o objetos de colección criptográficos como avatares de juegos o ilustraciones digitales. Estos tokens pueden representar insignificantes a valores subyacentes muy vastos. Una condición importante para los tokens de activos es que se pueda establecer la identidad del propietario. Los tokens criptográficos de activos potencialmente traen beneficios debido a la posibilidad de programarlos**(tokens inteligentes**) y comerciarlos con baja fricción y alta seguridad:

1. Puede dividir fácilmente las tenencias de activos y hacerlos disponibles en unidades pequeñas. Un ejemplo de este **fraccionamiento** es representar la propiedad de la Mona Lisa en 1.000 fichas para vender/arrendar.
2. Puede programar los derechos del token criptográfico y hacer cumplirlos a través de contratos inteligentes. Por ejemplo, establezca su token Mona Lisa para que se venda solo a organizaciones sin fines de lucro, o programa que una reventa automáticamente incluya una comisión del 2 % al vendedor original.
3. Reduce la fricción de comprar y vender, en parte debido a las microtransacciones rápidas y baratas. Por ejemplo, un refrigerador inteligente escanea la electricidad más barata para ciertos intervalos de tiempo.
4. Puede registrar toda la información relevante para los activos subyacentes en el token. Por ejemplo, verifique a los propietarios anteriores de su máquina de segunda mano, mejorando así la economía compartida.
5. Usted mismo puede crear fácilmente un activo, como un boleto de entrada a un concierto en casa.

En resumen, los tokens inteligentes transfieren fácilmente valor, información, ideas, derechos y obligaciones a través de contratos inteligentes.

Los tokens de seguridad representan bonos, acciones, préstamos, futuros, opciones y otros activos financieros negociables. Aunque pertenecen a los tokens de activos, se mencionan por separado. Todo tipo de derechos se pueden dar a los tokens de seguridad. Por ejemplo, el derecho de no revender la seguridad a todos, o de poder prestar temporalmente sus derechos de voto sobre la dirección de la empresa a alguien.

Los tokens de criptomonedas también pertenecen a los tokens de activos y se tratan por separado dado su mayor impacto financiero-económico esperado. Bitcoin es el ejemplo más conocido de una criptomoneda. En este caso, el token está destinado a actuar como dinero. Lenta pero seguramente, las **monedas estables** están atrayendo la atención, ya que demuestran posibles formas de estabilizar el valor de los tokens criptográficos y, por lo tanto, entre otros, potencialmente para servir como alternativas descentralizadas o representaciones de monedas fiduciarias. Las monedas estables pueden ser colateralizadas con varios activos como moneda fiduciaria o oro o criptografía, o no ser colateralizadas en absoluto.

Varios bancos centrales están probando monedas estables en lo que se llama una moneda digital del **Banco Central** (CBDC). Si bien el CBDC puede usar elementos de Blockchain, no es necesariamente una aplicación Blockchain. Los CBDC se oponen diametralmente a los orígenes descentralizados de Bitcoin, ya que un CDBC es una moneda regulada centralmente.

Existe la cuestión de cómo aplicar tokens criptográficos en un sistema económico donde se realiza el intercambio. Una forma de hacer esto es mirar la **fungibilidad del token**. Algunos tokens se pueden intercambiar más fácilmente por otro. Por ejemplo, un paquete de 1 kg de harina se puede cambiar por otro paquete de 1 kg de harina. Un billete de 10 EUR también se puede cambiar por dos billetes de 5 EUR. Lo mismo ocurre con las **fichas fungibles**: las unidades individuales son indistinguibles entre sí y se pueden intercambiar entre sí. Un ejemplo es Polkadot: 1 token Polkadot se puede cambiar por otro y dos tokens de Polkadot medio se pueden cambiar por 1 Polkadot entero.

Contrario a esto son tokens **no fungibles donde**los tokens son únicos en sí mismos y por lo tanto escasos. Pensemos, por ejemplo, en personas, países y certificados de nacimiento que no puedan intercambiarse con otras personas, países y certificados de nacimiento.

Blockchain en particular es adecuado para capturar y comercializar estos tokens de manera eficiente, incluso si los tokens solo representan un valor minúsculo o son únicos en su tipo. Esto es importante ya que en un mundo digital, es fácil crear una copia de un bien digital. Así que al tener un token como representación, no solo hay una oportunidad para intercambiar fácilmente bienes del mundo real. También le da la oportunidad de dar a cualquier bien físico una representación digital auténtica, por pequeña o tonta que pueda ser, y comerciarla. Además, crear un token escaso es económicamente interesante si quieres mantener el precio alto dado el adagio: «cuanto menor sea la oferta de un token, mayor será la escasez y, por lo tanto, la posibilidad de un precio más alto».
Varias de las ventajas que se mencionaron anteriormente para los tokens criptográficos de activos como el fraccionamiento y la creación de tokens inteligentes, apoyan el caso del usuario de tokens no fungibles en que pueden convertirse en representaciones altamente

individuales de cualquier objeto (para digitalizar) creado y comercializado a través de una barrera baja (todos pueden entrar, todos pueden participar) red segura, el Internet del Valor. Un Internet que se puede utilizar para medir de manera transparente su impacto en el medio ambiente y lo empuja a apoyar los objetivos de una comunidad más grande. Sea su papel el de propietario de un panel solar, usuario de electricidad o inversor de red de red.

En el futuro, teóricamente podría usar cualquier activo que posea, tokenizar y usar estos tokens fraccionadamente o de otro modo como medio de pago o financiación.

4.3 Fichas de adquisición de fondos

Todos estos tokens separados se pueden utilizar de varias maneras para adquirir fondos: desde Ofertas Iniciales de Monedas (ICO), a través de Ofertas de Tokens de Seguridad (STO) y Ofertas de Intercambio Inicial (IEO) hasta Ofertas Iniciales DEX (IDO).

La **Oferta Inicial de Monedas** (ICO) se utilizó principalmente en el pasado para recaudar fondos en Internet para proyectos de Blockchain. Ethereum en particular fue la cadena de bloques principal para crear y vender tokens. Un número sustancial de casos de abuso surgieron al comienzo de la tendencia de ICO, también porque las ICO tuvieron lugar fuera de la protección de las leyes y regulaciones nacionales. Como resultado, la **seguridad**

La oferta de tokens (STO) se concibió sirviendo al mismo propósito que una ICO, sin embargo ahora con considerar un token como una seguridad con protocolos estándar, derechos de voto y más en línea, aunque no completamente, con varias ecuridadesnacionales y leyes y regulaciones de intercambio. El STO no ha demostrado ser particularmente exitoso en el espacio público hasta la fecha. También como nuevas alternativas más reguladas, pero aún «abiertas», fueron concebidas como la **Oferta de Intercambio Inicial** (IEO) y la **Oferta Inicial DEX** (IDO). Aquí los intercambios centralizados o descentralizados, como Binance o Uniswap, tienen la oportunidad de obtener crowdfunding a través de su plataforma intermediaria, que generalmente toma controles KYC y AML.

La tendencia de dar forma a un Internet de Valor descentralizado por parte de la comunidad parece continuar en un torbellino de ideales, ideas, posibilidades técnicas, errores, accidentes maravillosos y perseverancia.

5 Usos y aplicaciones de Blockchain

En este capítulo se dan tres ejemplos del uso y aplicaciones de Blockchain. Antes de hacerlo, se da una introducción sobre cómo las organizaciones pueden pensar estratégicamente sobre los elementos relevantes de su modelo de negocio y las oportunidades que ofrece Blockchain. El capítulo termina con puntos específicos a los que una empresa presta atención una vez implementada Blockchain.

5.1 Modelos de negocio

Blockchain generalmente ofrece valor dentro de los modelos de negocio y los ecosistemas de negocios donde los datos digitales y la tecnología se pueden crear y compartir entre los socios. Esto como Blockchain es una tecnología digital que encaja con estos modelos de negocio basados en datos digitales y permite a los socios trabajar juntos donde no podían antes. Estos socios ahora pueden poner su confianza «en el sistema», donde antes de Blockchain no confiaban entre sí para cooperar desde el principio. En este sentido, Blockchain es especialmente una oportunidad para crecer y digitalizar ecosistemas que utilizan **modelos de negocio basados en datos digitales**.

En cuanto a los modelos de negocio, el modelo de **negocio descentralizado Canvas** [6][7] es relevante, así como la descentralización es fundamental para las adaptaciones de Blockchain sin permiso público. En este particular, los titulares de tokens de lienzo tienen una posición central, ya que tienen múltiples roles como usuario, validador, empleado o propietario. Este tipo de pensamiento «nuevo» da una idea de las posibles nuevas oportunidades que ofrece Blockchain sin permiso público, ya que las partes que no se conocen tienen alternativamente la configuración y el uso de un sistema de barrera relativamente baja para compartir y verificar datos juntos mientras no se conocen.

El gobierno entonces se establece de manera descentralizada por el público, los datos se almacenan de manera descentralizada y la comunicación entre las diversas partes se lleva a cabo peer-to-peer. Esta es la forma más abierta de una Blockchain. Una empresa es libre de ajustar los bloques de construcción de Blockchain en sí. Con un sistema centralizado, una organización central toma las decisiones.

En un modelo de negocio descentralizado, las ventas a menudo se comparten entre aquellos que más contribuyen a la red y los costos de uso de la plataforma son muy bajos, por ejemplo, con la plataforma Blockchain de blogs sociales Steemit.

5.2 Aplicaciones de Blockchain empresarial

Este párrafo describe tres aplicaciones implementadas dentro de cuatro industrias diferentes, y las compara utilizando las ventajas comparativas que Blockchain ofrece en estas aplicaciones. Las cuatro aplicaciones son:

1. Gobierno y Bienes Públicos por Lantmäteriet.
2. Fabricación por BMW.

[6] https://canvanizer.com/new/decentralized-business-model-canvas
[7] https://medium.com/mvp-workshop/decentralized-business-model-canvas-1-9daf6e4bc9fe

3. Billetera digital de Singapore Airlines.

Una descripción general útil aquí para ayudarlo a comprender dónde muchos sectores Blockchain están implementando Blockchain es de abajo la investigación entre 67 redes de Blockchain empresariales y los sectores en los que caen estas implementaciones (Rauchs, Blandin, Bear, McKeon, 2019).

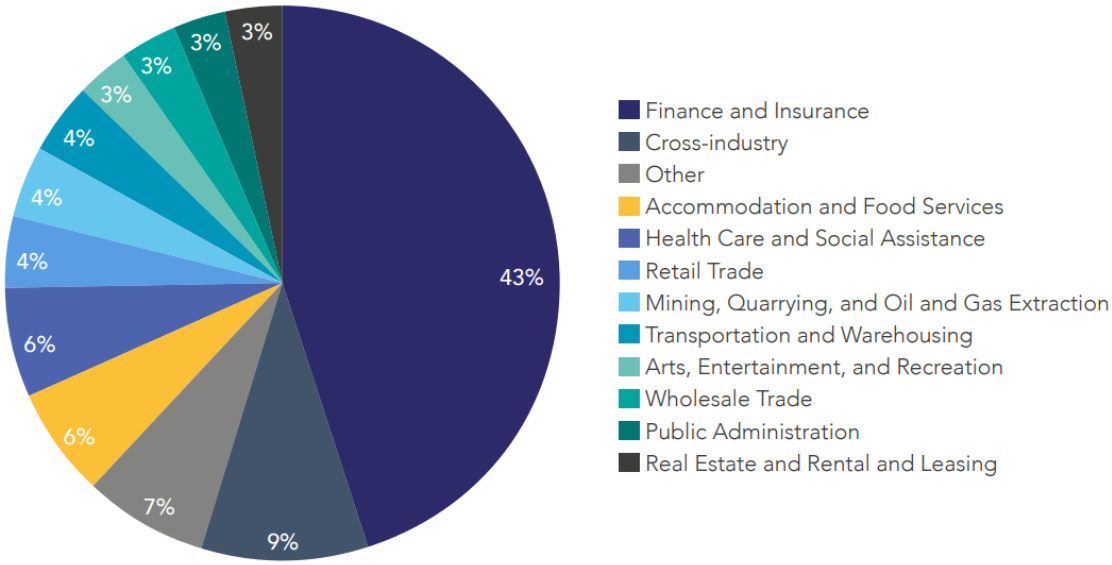


Figura 11: Visión general de 67 redes de Blockchain empresariales en vivo y en qué sectores caen (Fuente: Rauchs, Blandin, Bear, McKeon, 2019).

El primer ejemplo se da en el **sector del Gobierno y los Bienes Públicos**. El **Lantmäteriet** sueco tiene la tarea de mantener el sistema catastral, proporcionar geodatos y realizar el registro de tierras. Es necesario una mayor transparencia y una mayor eficiencia del proyecto, ya que los diferentes socios trabajan juntos utilizando procesos manuales que parecen ineficientes y propensos a errores.

Lantmäteriet probó una solución para ver cómo actores como compradores de propiedades, vendedores, corredores, servicios financieros, abogados, fondos de pensiones y Lantmäteriet pueden trabajar juntos en una plataforma en línea eficiente que proporciona transparencia inmediata de una solicitud a través de dispositivos digitales. El proyecto fue configurado como un proyecto incremental (2015-2019) en una situación de caja controlada con socios de confianza, pero sin demasiado ambicioso perseguir la descentralización a corto plazo. Hubo un claro enfoque en la recolección de frutos bajos con el registro de títulos de propiedad, al tiempo que se creaba una base para los servicios futuros.

Durante el proyecto surgieron problemas legales que debían superarse. Para un Lantmäteriet tuvo que considerar cómo tratar con el derecho de las personas a controlar sus propios datos (Reglamento General de Protección de Datos de la UE — GDPR), incluido el poder protegerlos y eliminarlos cuando lo desee y sea posible. Así como sobre cómo se pueden utilizar las firmas digitales como firmas legalmente vinculantes dentro de la UE (directrices eIDAS) o el estado de los contratos firmados digitalmente (e-) basados en Blockchain.

La venta de títulos de propiedad fue ambiciosa en que diferentes partes crearon un nuevo proceso y juego con una nueva solución tecnológica. Las soluciones Blockchain incluían sistemas Blockchain privados, cerrados y autorizados, así como una red pública distribuida. La Blockchain privada es propiedad del gobierno, dirigida por un número limitado de nodos de intermediarios de confianza y bajo la supervisión del gobierno público sueco. Este sistema colabora con ChromaWay y la red privada de las partes interesadas. Utiliza contratos inteligentes, los mecanismos de consenso de tolerancia a fallos bizantinos prácticos y prueba de trabajo, identidades digitales fuera y en cadena a través de una aplicación de teléfono móvil y sin tokens.

La escritura permanece registrada en Lantmäteriet y no se transfiere a una cadena de bloques pública dados los problemas anteriores con GDPR. Los contratos se firman manualmente y se colocan en la cadena de bloques a través de hashes. Los contratos originales están en el servidor con otras partes, esta información tiene copias de seguridad. Telia ofrece una solución de ID de aplicación móvil que permite a las personas registrarse sin publicar su número de servicio público sueco. Estos registros se almacenan en la cadena de bloques de Bitcoin a través de un hash y se verifican. La información personal digital se puede eliminar si una persona así lo desea y no está obligada por ley a ser información pública.

Las principales ventajas fueron la seguridad del uso de la tecnología Blockchain, así como operativa. En cuanto a este último, ya que el plazo de registro de un título de propiedad pasó de 4 a 6 meses a unos pocos días. Además, se previeron ahorros de 100 millones EUR/año a través de menos errores y mantenimiento (Kairos Future, 2017). Esto reduce los riesgos de contrato con características ambiguas, datos fraudulentos o posibilidades de robar propiedades. La pista de auditoría para ambos clientes, auditor como legislador también se hizo transparente. Además, el ecosistema fortaleció sus procesos mutuos e intercambio de datos sin demasiada agitación de su servicio central y modelo de negocio. Y, por último, pero no menos importante, la accesibilidad pública aumentó la confianza en el proceso y en las partes. Después de la prueba, el sistema podría ampliarse para incluir a partes como aseguradoras, notarios y otras autoridades públicas locales.

El proyecto se finalizó en 2019 mostrando que tanto la arquitectura de la plataforma trabajada demostró lo posible, sin embargo, según Mats Snäll, director de innovación de Lantmäteriet, «Nunca se integró en el sistema de producción del registro de la tierra», ya que se necesitaría un cambio en la legislación antes de que el sistema pudiera ampliarse en el futuro. (Baraniuk, 2020). Probablemente esto apunta al desafío de publicar datos de identidad de usuario en el Blockchain público.

Otras investigaciones también apuntan a un «cambio fundamental en la estructura de gobernanza, como el papel de Lantmäteriet», que podría haber proporcionado un motivo subyacente específicamente para que los ecosistemas inmobiliarios congelaran los avances en el proyecto (Schnuer, 2020).

Mientras tanto, Lantmäteriet utiliza sus lecciones para continuar la experimentación con Bockchain. Por ejemplo, la asignación gubernamental conjunta con DIGG es encontrar «un modelo o solución conceptual sobre cómo generar confianza en la automatización con IA y con otras nuevas tecnologías como la tecnología Blockchain». (AI Sweden, Lantmäteriet, 2020).

El segundo ejemplo de aplicación Blockchain se refiere a BMW dentro **del sector manufacturero. Los modelos de negocio automotriz tienen que lidiar con las**tecnologías de[la] **cuarta revolución industrial, como la electrificación y los sistemas autónomos bajo condiciones cada vez mayores conscientes del medio ambiente.**

BMW en este ejemplo trata de entender cómo se puede usar una identidad digital para automóviles para que pueda permitir el uso de otras tecnologías y conceptos de la 4ª Revolución Industrial. En particular, los problemas de privacidad/seguridad de tener una conexión constante a Internet del automóvil y del usuario, así como la necesidad de almacenar estos datos de forma segura. Este intercambio seguro de datos entre dispositivos que garantizan identidades digitales seguras es lo que Blockchain potencialmente trae a la mesa, lo que ofrece una entrada al mercado de la economía de automóviles compartidos para BMW.

BMW ha probado una serie de aplicaciones para compartir coches como Share Now, donde la identidad digital de ambos coches como usuario puede estar involucrada. Estas identidades digitales combinadas automotrices pueden, por ejemplo, registrarse cuando se deposita gasolina o donde el automóvil está estacionado. Este tipo de información entonces se puede utilizar en modelos de negocio donde los fabricantes de automóviles, junto con o sin intermediarios, ofrecen servicios personalizados como seguros no de vida, paseos en automóvil autónomos o mejora su experiencia en el coche en general.

En este ejemplo particular, sin embargo, BMW experimentó con un proyecto más simple con enfoque exclusivo en la identificación del automóvil y sus datos almacenados, por lo que no se centró en el usuario. La idea es que los posibles compradores de BMW usados estarían interesados en datos de confianza sobre el kilometraje, el historial de accidentes, el historial de servicio y otra información del automóvil. Un vendedor potencial podría compartir estos datos con un vendedor prospecto o su aseguradora, BMW podría usar la información para mejorar su modelo de negocio, como usarlo para dar un mejor servicio a sus clientes.

Para crear esta solución, el garaje de inicio de BMW trabajó con startups Blockchain, en este caso VeChain. Además, BMW utiliza los resultados para desarrollar la identificación de un automóvil, un primer paso para una identidad de vehículo (VID) que los miembros de Mobility Open Blockchain Initiative (MOBI) pueden utilizar juntos. Mobi es un consorcio Blockchain que desarrolla estándares de Blockchain juntos.

La cooperación con VeChain dio lugar a la **aplicación** VerifyCar. VeChain es una organización autónoma descentralizada con un órgano de gobierno central que utiliza el método de consenso de prueba de autoridad y diferentes tokens en su blockchain pública VeChain.

El VID tiene un ID único en esta Blockchain. Periódicamente, la aplicación captura datos (a través de tarjetas SIM en el automóvil y comunicación máquina a máquina), que se verifican en VeChain Blockchain: VeChain solo almacena la referencia a los datos, los datos permanecen en el propio vehículo. Los datos del automóvil capturados contienen información estática, como el tipo y la fecha de producción del automóvil, así como información dinámica, como el número de kilómetros de conducción. Cada vez que un propietario de un automóvil desea compartir datos con otra parte, utiliza la aplicación VerifyCar para mostrar los datos, incluidas las referencias en la cadena de bloques, para mostrar que estos son los datos reales almacenados en el vehículo.

La intención de BMW de no tener control sobre el gobierno de VeChain o el código. A partir de 2022 la aplicación no ha visto producción.

Al pilotar esta solución, BMW está dando un primer paso controlado hacia la integración incremental de la tecnología Blockchain descentralizada. Además, si VerifyCar se puede utilizar para automóviles, entonces ¿por qué no tener una tarjeta de identidad digital VID para garantizar que las piezas del automóvil no sean falsificadas, en qué ubicación se pueden encontrar las materias primas compradas en la línea de producción o comprender las condiciones de fabricación o transporte de ciertas máquinas de producción que ha pedido? En línea con ese pensamiento BMW experimenta con Blockchain en beneficio de una **cadena de suministro transparente** también.

Por ejemplo, en 2019, **el** piloto de PartChain para la compra de luces frontales con Amazon Web Services, Microsoft Azure y Hyperledger Fabric Blockchain (Ledger Insights (2020, 31 de marzo) se amplió a otros proveedores. Esto permitió a BWM poder rastrear sus componentes y, a largo plazo, las materias primas críticas «desde la mina hasta la fundición». (BMW Pressclub Global, 2020). Y, además, garantizar una «certificación más fácil y unos procedimientos aduaneros más cortos» (BMW, 2019).

Un **último ejemplo es la billetera digital de Singapore Airlines, KrisPay**. Singapore Airlines buscaba aumentar aún más la lealtad de sus clientes mediante el uso de Blockchain. Esto resultó en fortalecer su programa de viajero frecuente KrisFlyer con la billetera digital KrisPay Blockchain en 2018.

Con KrisPay, los clientes pueden intercambiar sus airmiles KrisFlyer por millas KrisPay, tokens de criptomonedas. Estos tokens KrisPay se pueden guardar en/gastar con diferentes comerciantes como bancos, gasolineras y tiendas. También el cliente puede ahorrar e intercambiar otras recompensas, como mediante el uso de la tarjeta de crédito de DBS (Development Bank of Singapore Limited), o ganar, comprar o gastar millas de Singapore Airlines como para mejoras de vuelo. El valor monetario del token KrisPay es dictado por Singapore Airlines. Así que la solución que KrisPay ofrece aquí es dar a los clientes una manera fácil de canjear sus recompensas para evitar que millas se desperdicien junto a guardar estos tokens en la red de comerciantes. En cierto modo, los clientes están recibiendo una adición digital/alternativa a las monedas respaldadas por fiat.

La funcionalidad de KrisPay es fácil de usar a través de una aplicación en su dispositivo móvil y transacciones instantáneas de punto de venta. Para mejorar la usabilidad, las millas KrisFlyer se pueden transferir dentro de la familia o nominados autorizados.

Al combinar billeteras Blockchain y criptomonedas, KrisPay utiliza fortalezas de Blockchain como la seguridad para todos los usuarios, ya que el registro de las transacciones es una prueba de manipulación. Los comerciantes inmediatamente tienen sus transacciones aprobadas y perspicaces, sin el uso de un intermediario más lento y más costoso. Esto apoya la conciliación de los pagos de tokens entre los comerciantes (y sus administraciones financieras) y les da información actualizada del cliente.

KrisPay fue desarrollado con KPMG Digital Village y Microsoft. KrisPay es una empresa privada propiedad de Singapore Airlines que trabaja en una combinación de Microsoft Azure (originalmente basado en el protocolo Ethereum) con la aplicación Azure y las funciones de

base de datos. Diferentes socios mantienen y verifican la base de datos Blockchain para que cada uno tenga la información del cliente/transacción disponible al mismo tiempo.

Microsoft anunció retirar su Azure Blockchain en 2021 y apoyar la migración de clientes al Servicio Quorum Blockchain, otra variante del protocolo Ethereum (Microsoft, 2021).

Los tokens y la billetera KrisPay se combinaron en una nueva aplicación en 2020, Kris+. Esta aplicación utiliza además los datos de los clientes para que Singapore Airlines pueda atender mejor a sus clientes, así como ofrecer ofertas personalizadas, incluso en función de la ubicación geográfica desde el teléfono móvil.

Potencialmente, la billetera KrisPay se puede utilizar para la emisión de boletos, la prueba de su identidad digital o como un token genérico adicional que se puede utilizar para intercambiar contra monedas fiduciarias u otros puntos de lealtad.

En conclusión, **todas estas aplicaciones** son casos de Blockchain bien definidos que se implementan cuidadosamente como parte de una visión más amplia dentro de un entorno en el que los iniciadores confían y controlan. Los casos muestran claridad sobre los elementos que ven como una oportunidad o ninguna oportunidad, y utilizan un proceso de cambio incremental en el que intensifican el esfuerzo desde los primeros pasos cautelosos hasta la implementación completa.

Su entorno consiste en un proceso estable, un modelo de negocio conocido y socios de confianza para experimentar con los aspectos más probados de la tecnología y sus implicaciones comerciales descentralizadas.

No había espacio para mostrar la aplicación de un modelo de negocio descentralizado completo, si desea un ejemplo asegúrese de leer el ejemplo del mercado de Augur Predication en el Capítulo 16.5. (Lin Lim, Janse, 2021).

5.3 ¿Cuándo tiene sentido la implementación de Blockchain?

De los ejemplos anteriores está claro que ciertas condiciones deben existir para implementar Blockchain con éxito.

Hay una serie de criterios que puede considerar para decidir si Blockchain es un caso significativo para su negocio. Estos criterios tienen como objetivo eliminar las fricciones con los datos o el tráfico de datos, o crear oportunidades con el tráfico de datos y datos entre las partes. Como regla general, los criterios pueden resumirse de la siguiente manera:

1. **La innovación digital** es parte de la estrategia.
2. Diferentes partes **comparten datos**.
3. Estos datos y sus transacciones se refieren al **valor monetario**.
4. Los datos son **confidenciales**.
5. Diferentes partes editan datos.
6. Los datos deben ser verificados.
7. Hay un retorno **claro y suficiente de la inversión** que debe calcularse.
8. La verificación es **compleja, costosa o aumenta el tiempo**.
9. La solución para elegir Blockchain es la **solución más simple** para superar el problema.

10. La solución influye en la estructura organizativa existente.
11. La solución afecta al flujo de trabajo existente.
12. La solución afecta al ecosistema existente.
13. La solución técnica está cerca o puede integrarse con los sistemas existentes.
14. La solución es intensiva en datos pero escalable. Piense en diferencias de 1k, 10k, 100k, 1 millón o> 10 millones de transacciones por hora.

Una vez que vea la oportunidad de implementar Blockchain basado en estos criterios, puede continuar con la comprensión de las utilidades de usuario subyacentes que se necesitan, así como los bloques de construcción que componen estas utilidades. Por ejemplo, el bloque de construcción del «token de pago» tiene un impacto en la facilidad, la velocidad y la transparencia de las transacciones de pago. Otros ejemplos de bloques de construcción son billeteras, contratos inteligentes, dApps, tipos de tokens, oráculos, etc.

Actualmente, el impacto de Blockchain en las empresas se centra principalmente en la eficiencia, la desintermediación y el registro. Y el impacto es mayor allí donde las partes cooperantes desbloquean y crean nuevos datos. En el futuro, se espera que las implementaciones de Blockchain complejas que impulsen la descentralización y la integración de los ecosistemas vean los mayores beneficios de Blockchain.

Puede utilizar el siguiente árbol de decisiones simplificado para estimar el uso de un proyecto Blockchain:

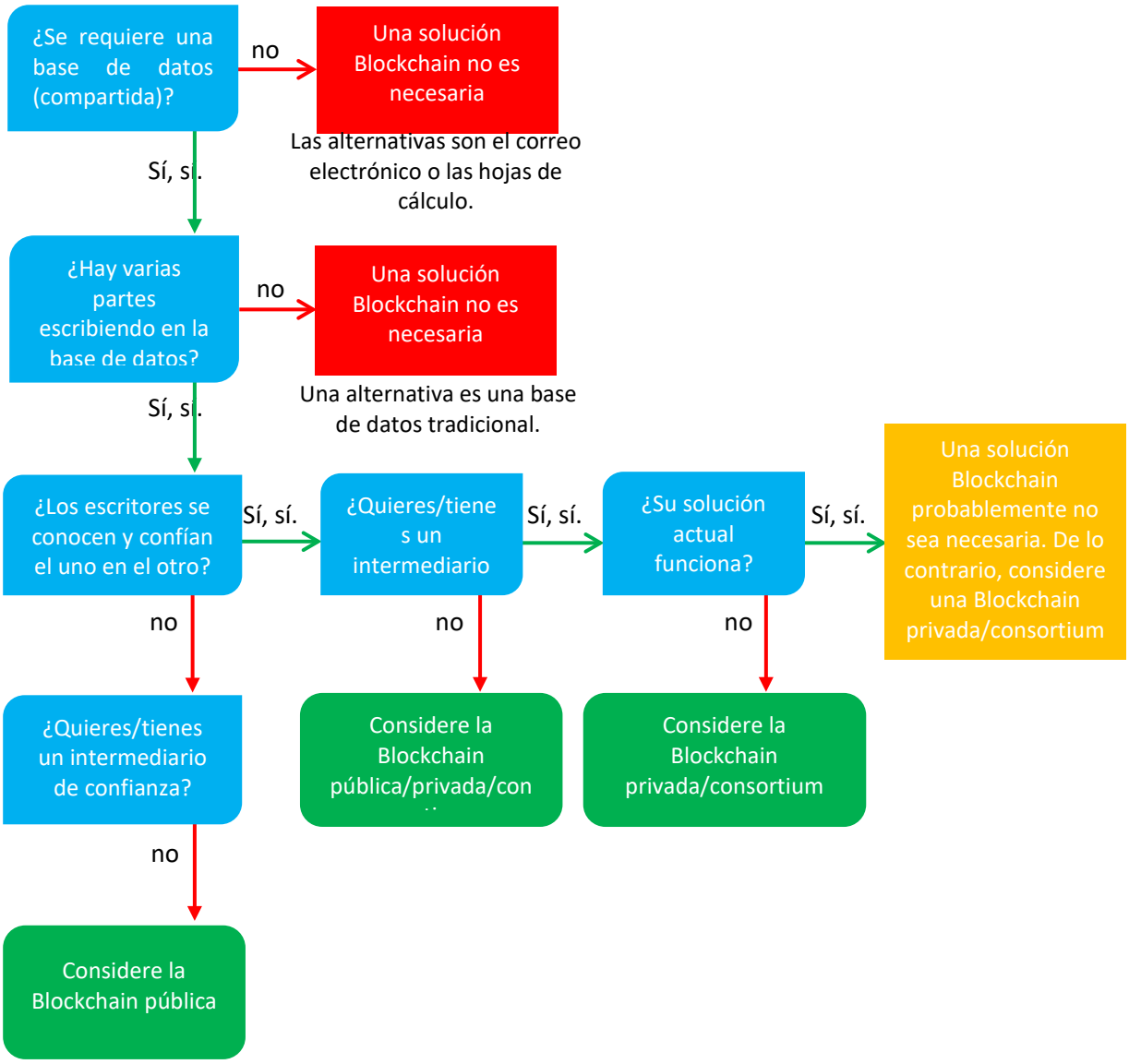


Figura 12: Árbol de decisiones simplificado si usar o no Blockchain (Fuente: Lin Lim, C., Janse, A., Blockchain Basics, 2021).

6 Referencias y fuentes para lecturas adicionales

Ackermann, J. & Meier, M. (2018). *Blockchain 3.0: La próxima generación de sistemas Blockchain.*

Advanced Seminar Blockchain Technologies, Summer Term 2018, Technical University Munch.

AI Sweden, Lantmäteriet (2020, noviembre). *La creación de un modelo de confianza en la IA para el sector público,*

Consultado desde https://www.ai.se/en/node/85154

Antonopoulos, A. M. (2016). *El Internet del dinero: charlas de*. Merkle Bloom Llc.

Augur. (n.d.). *Visión general*. Consultada el 23 de diciembre de 2019, desde https://docs.augur.net/#overview

Augur. (2018, 9 de julio). *Prevision Foundation OU Política de privacidad*. Consultado el 23 de diciembre de 2019, desde el sitio web Augur.net: https://www.augur.net/privacy-policy/

Baraniuk, C. (2020, 11 de febrero). *Blockchain: La revolución que no ha ocurrido del todo*. Consultado desde https://www.bbc.com/news/business-51281233

Bitcoin Block Reward Halving Countdown (en inglés). (2019). Consultado el 23 de diciembre de 2019, desde

Sitio web de Bitcoinblockhalf.com: http://www.bitcoinblockhalf.com

BMW, (2019, 14 de octubre). Cómo las soluciones Blockchain pueden ayudar al conductor. Consultado desde https://www.bmw.com/en/innovation/blockchain-automotive.html

BMW Pressclub Global (2020, 31 de marzo). *BMW Group utiliza Blockchain para impulsar la transparencia de la cadena de suministro.* Consultado desde https://www.press.bmwgroup.com/global/article/detail/T0307164EN/bmw-group-uses-blockchain-to-drive-supply-chain-transparency.

Buterin, V. (2013). *Libro blanco de Ethereum: un contrato inteligente de próxima generación y una plataforma de aplicación descentralizada* [White paper]. Consultado el 27 de diciembre de 2019, desde Blockchainlab: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2014, 6 de mayo). *DAOs, DACs, DA y Más: Guía Terminológica Incompleta.*

Consultado el 27 de diciembre de 2019, desde el sitio web Ethereum.org: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

ChainTrade (en inglés). (2017, 27 de diciembre*). 10 Ventajas de usar contratos inteligentes*. Consultado el

27 de diciembre de 2019, desde el sitio web de Medium: https://medium.com/@ChainTrade/10-ventajas-de-usar-smart-contracts-bc29c508691.a

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin y el ascenso

de organizaciones autónomas descentralizadas. Journal of Organization Design, 7(1).

https://doi.org/10.1186/s41469-018-0038-1

Kaoris Future (en inglés). (2017) *El Registro de la Propiedad en la cadena de bloques — testbed*. Consultado desde https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lantmäteriet, Telia, ChromaWay & Kairos Future. (2016). *El Registro de la Propiedad en la cadena de bloques.* Consultado desde http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Ledger Insights (2020, 31 de marzo). *BMW amplía la cadena de bloques de la cadena de suministro para la trazabilidad de piezas.* Consultado desde https://www.ledgerinsights.com/bmw-blockchain-supply-chain-parts-traceability/

Ledger Insights (2020, 15 de octubre), *Singapore Airlines amplía su billetera digital de recompensa basada en blockchain*. Consultado en https://www.ledgerinsights.com/singapore-airlines-extends-its-blockchain-based-reward-digital-wallet/

Lin Lim, C., Janse, A., *Blockchain Handbook*, septiembre 2021, Capítulo 10. Editor: De boekdrukker Amsterdam. ¿POR QUÉ? 781 ISBN: 978-90-80866140 https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain-basisboek-digitale-versie-2.pdf

Microsoft, 2021, 14 de mayo). *Acción requerida: Migre sus datos de Azure Blockchain Service antes del 10 de septiembre de 2021*. Consultado en https://azure.microsoft.com/en-us/updates/action-required-migrate-your-azure-blockchain-service-data-by-10-september-2021/

Microsoft (2019, 2 de mayo), *Singapore Airlines transforma la lealtad de los clientes con blockchain en Azure*. Consultado el 4

ES UN MOBI. (2019). *Estándar de Identidad del Vehículo*. Consultado desde https://dlt.mobi/wp-content/uploads/2019/07/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Nakamoto, S. (2008). *Bitcoin P2P e-cash paper.* Consultado el 23 de diciembre de 2019, desde Sitio web de Metzdowd.com: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (2010, 30 de septiembre). *Re: Me rompí la billetera, los envíos nunca lo confirman ahora.* [En línea comentario del foro]. Mensaje publicado en https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

Parker, L. (2015, 1 de noviembre). El*reciente corte de energía de PayPal impulsa la adopción de bitcoins*. Consultado el 23 de diciembre de 2019, desde el sitio web Bravenewcoin.com: https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Rauchs M., Blandin, A., Bear, K., McKeon, S. (2019). 2.º *estudio de benchmarking Global Enterprise Blockchain*. Consultado desde https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf

Schnuer, C. (2020, 7 de diciembre). *Cambiar el mercado inmobiliario a través de blockchain*. Consultado desde https://delano.lu/article/delano_changing-property-market-through-blockchain

Estratega. (n.d.) *Modelo de Negocio Canvas*. Consultado el 23 de diciembre de 2019, desde https://www.strategyzer.com/canvas/business-model-canvas

Sultan, K., Ruhi, U., & Lakhani, R. (2018). *Conceptualización de Blockchains: Características &*

Aplicaciones. 11.a Conferencia Internacional de Sistemas de Información de IADIS 2018, 49–57

Vigna, P., & Casey, M. (2015). *La era de la criptomoneda: cómo son Bitcoin y la cadena de bloques*

desafiando el orden económico global. Nueva York, Nueva York: Picador/St. Martin's Press.

Young, S. (2018). *Hacer cumplir los derechos constitucionales a través del código informático.* Consultado desde

Cua Law Scholarship Repository sitio web: https://scholarship.law.edu/jlt/vol26/iss1/5/

Anexo I — Glosario de términos

51 % de ataque: Un ataque a la Blockchain que se logra al obtener más del 51 % de toda la potencia informática de la red.

Modelo cliente-servidor: El modelo en el que los clientes (usuario) están conectados a un servidor. El servidor contiene datos relevantes para los clientes. Los clientes se conectan al servidor para acceder a estos datos. Esto hace que los clientes dependan del servidor.

Tecnología de Ledger Distribuido (DLT): Tecnología de contabilidad distribuida.

Doble gasto: Gastando un Bitcoin dos veces. Por ejemplo, que tienes 1 Bitcoin, pero con eso envías 1 Bitcoin a la persona A y 1 Bitcoin a la persona B.

Nodo completo: Un nodo que tiene una copia completa de la Blockchain.

Minero: Una computadora que proporciona potencia de cómputo para producir un bloque válido. Un bloque solo es válido si encuentra un nonce que conduce a un valor hash válido.

Nodo: Dispositivo que está conectado a una red informática.

P2P: Véase peer-to-peer.

Peer-to-peer: Una red informática donde las computadoras son iguales entre sí y pueden ofrecerse unos a otros servicios.

Prueba de trabajo: Un mecanismo de consenso que requiere que los mineros usen la potencia de la computadora para encontrar el valor hash correcto para un nuevo bloque. Al encontrar el valor hash correcto, se les permite agregar el bloque a la Blockchain y recibir una recompensa.

Punto único de fracaso (SPOF): La parte de una red que detiene el funcionamiento de toda la red en caso de un fallo.

SPOF: Ver Punto Único de Fallo.

Tercero de confianza (TTP): Intermediario de confianza.

TTP: Vea a terceros de confianza.

Libro blanco: Un documento que describe cómo se resuelve un problema específico. Satoshi Nakamoto ha escrito en el libro blanco de Bitcoin cómo Bitcoin resuelve el problema de doble gasto en una red distribuida.

Blockchain 1.0: La primera generación de Blockchains que se han utilizado principalmente para facilitar el almacenamiento y transferencia de criptomonedas.

Blockchain 2.0: La segunda generación de Blockchains que se centran más en habilitar contratos inteligentes, dApps y DAO.

Blockchain 3.0: La tercera generación de Blockchains que han resuelto un grupo de problemas con los que blockchain 2.0 todavía tiene que lidiar. Ejemplos de estas cuestiones son la escalabilidad, la interoperabilidad, la privacidad, la sostenibilidad y la gobernanza.

Gas: Costos de transacción para realizar una transacción en Ethereum Blockchain.

Aplicación descentralizada (dApp): Una aplicación que utiliza el almacenamiento de datos descentralizado de una Blockchain. La aplicación no se ejecuta a través de un servidor central,

sino a través de una red descentralizada de nodos. Al igual que una aplicación normal, a menudo tiene un front-end y una interfaz de usuario.

Organización Autónoma Descentralizada (DAO): Una entidad autónoma que también depende de la contratación de personas. Estos individuos pueden realizar ciertas tareas necesarias que la entidad no puede. La DAO tiene capital interno a su disposición para este fin, con el que ciertas actividades de estos individuos pueden ser recompensadas. Lo que hace que un DAO sea fundamentalmente diferente de una organización centralizada es que no tiene un equipo de alta dirección o un CEO. Es una organización no jerárquica.

Contrato inteligente: Un contrato con ciertos términos y condiciones que se establecen en el código. El contrato es autoejecutable, ya que realiza las acciones correspondientes apropiadas cuando se cumplen los términos y condiciones. Sin embargo, el contrato debe contener información suficiente de cada una de las partes implicadas en el contrato para privar a las partes de su capacidad de resolver el contrato. Hay dos tipos de contratos inteligentes: determinista y no determinista.

Solidez: El lenguaje de programación desarrollado específicamente para Ethereum para escribir contratos inteligentes.