Universidad Politécnica
de Madrid

Escuela Técnica Superior de
Ingenieros Informáticos

Grado en Ingeniería Informática

Trabajo Fin de Grado

Finanzas descentralizadas: Análisis de la descentralización, escalabilidad y seguridad de la blockchain para la DeFi

Autor: Eduardo Labrador Santos

Tutor(a): Francisco Rosales García

Madrid, Junio 2023

Este Trabajo Fin de Grado se ha depositado en la ETSI Informáticos de la Universidad Politécnica de Madrid para su defensa.

Trabajo Fin de Grado
Grado en Ingeniería Informática
Título: Finanzas descentralizadas: Análisis de la eficiencia y seguridad de los protocolos de DeFi
Junio 2023

Autor: Eduardo Labrador Santos

Tutor: Francisco Rosales García
Arquitectura y Tecnología de Sistemas Informáticos
ETSI Informáticos
Universidad Politécnica de Madrid

Resumen

Las criptomonedas se han vuelto una moda, especialmente por la especulación que los acompaña. ¿Pero cuántos de esos usuarios de criptomonedas conocen exactamente la tecnología que permite la existencia de las criptomonedas? Con la aparición y posterior automatización de los Contratos Inteligentes, este soporte distribuido ha generado un entorno seguro, democrático y eficiente que ha respaldado el crecimiento de los mercados descentralizados.

Es por esto, que estudiar a fondo las bases técnicas de esta tendencia debería ser obligado para poder entender la magnitud de esta tecnología disruptiva. A lo largo de este trabajo se pretende hacer un estudio en profundidad de lo que es la tecnología blockchain (la tecnología detrás de las criptomonedas). Pasando por los contratos inteligentes, que son lo que han permitido el salto a una nueva realidad de posibilidad en la blockchain. Estudiaré su potencial, sus bases tecnológicas y las debilidades que tienen y que deben ser optimizadas.

También aprovecharé para estudiar la nueva tendencia del sector cripto, las finanzas descentralizadas (DeFi). Esta nueva corriente, usa como medio la tecnología blockchain para crear un marco financiero descentralizado. Entonces creo que poder profundizar en las bases técnicas de este sector es algo clave que complementaría la profundidad de conocimiento adquirida en la primera parte del proyecto.

Por último, tras haber hecho una investigación y centralización de la información acerca de la blockchain, los contratos inteligentes y las DeFi, haré un estudio del trilema cripto con un posterior análisis de las principales y más interesantes blockchains del sector. Para de esta forma poder ver en qué variables (descentralización, seguridad, escalabilidad) sería mejor cada red. Y por tanto cual podría tener un mejor desempeño en el largo plazo para las DeFi.

Palabras Clave: *Blockchain, Ethereum, Bitcoin, DeFi (Finanzas Descentralizadas), Contratos Inteligentes, Trilema Cripto, Capital Bloqueado, Nodos, Consenso, Protocolo.*

Abstract

Cryptocurrencies have become a trend, especially due to the speculation that accompanies them. But how many of these cryptocurrency users exactly understand the technology that enables the existence of cryptocurrencies? With the emergence and subsequent automation of Smart Contracts, this distributed support has generated a secure, democratic, and efficient environment that has supported the growth of decentralized markets.

That is why studying the technical foundations of this trend should be mandatory in order to understand the magnitude of this disruptive technology. Throughout this work, an in-depth study of blockchain technology (the technology behind cryptocurrencies) will be conducted. This includes an examination of Smart Contracts, which have facilitated a leap into a new realm of possibilities within the blockchain. Their potential, technological foundations, and weaknesses that need to be optimized will be explored.

Furthermore, an opportunity will be taken to study the new trend in the crypto sector, Decentralized Finance (DeFi). This emerging movement utilizes blockchain technology to create a decentralized financial framework. Thus, delving into the technical foundations of this sector is essential to complement the depth of knowledge gained in the first part of the project.

Finally, after conducting research and gathering information about blockchain, Smart Contracts, and DeFi, an analysis of the crypto trilemma will be performed, followed by an examination of the sector's main and most intriguing blockchains. This will help determine which variables (decentralization, security, scalability) each network excels in and, consequently, which one may have better long-term performance for DeFi.

Keywords: *Blockchain, Ethereum, Bitcoin, DeFi (Decentralized Finance), Smart Contracts, Crypto Trilemma, Locked Capital, Nodes, Consensus, Protocol.*

Índice de contenidos

Índice de Figuras

1 Introducción

Comenzaré el trabajo explicando cual es el contexto en el que se enmarca el trabajo y también la motivación que hay detrás del proyecto, para realizarlo. También en esta primera parte se presentan los objetivos que se quieren cubrir y por tanto alcanzar, así como la estructura de contenido que se seguirá.

1.1 Contexto y Motivación

Las criptomonedas se han puesto de moda en los últimos años, y cada vez más y más gente las descubren y se interesa por ellas [1]. Y lo que ha ayudado a que llegara a conocerse tan rápido han sido las increíbles rentabilidades que han conseguido. Y es esta la razón que hizo que me interesase a mí también. Además, el hecho que esté tan relacionado con la tecnología, basándose en la tecnología blockchain hizo que me interesara aún más ya que tocaba una parte de la carrera que estudio.

La blockchain que es la tecnología bajo la que nacen las criptomonedas también se ha hecho más conocida gracias a esta tendencia, esto ha hecho que se busque nuevas utilidades donde poder usarla y mejorar sistemas antiguos. Y aunque el aumento de popularidad es claro, la mayoría de la población no conoce esta tecnología, ni su potencial ni sus limitaciones. Y no solo eso, sino que también es una gran desconocida para profesionales de la tecnología. Y yo, como estudiante de una carrera tecnológica tampoco es un tema que domino, pero si por el cual tengo un alto interés, por lo que me sumergiré en este mundo a través de un TFG.

Lograr aprender en profundidad en tecnologías tan novedosas y sobre todo tan especulativas. Aunque, como suele pasar con el comienzo de una nueva tecnología, existe mucha especulación a la vez que muy poca información, y además tiene un ritmo de evolución y modificación altísimo con nuevos y nuevos avances es más difícil aún aprender con claridad algo sobre el tema. Y este hecho hace que sea más motivador para mi estudiarlo.

Además, este sector no solo tiene una sinergia importante con mi carrera de ingeniería informática, sino que también lo tiene con la ADE, ya que el ecosistema de inversión que ha nacido a raíz de las criptomonedas es inmenso. Entonces lograr dominar la tecnología detrás de él puede ayudarme a tener un mejor conocimiento de los potenciales activos donde invertiría, ya que podría entender mejor el uso que tendrían.

Los activos financieros que nacen de esta nueva tecnología, como bien he mencionado antes, están logrando atraer grandes cantidades de capital para invertir [2], siendo las DeFi un sector de las criptomonedas que más capital está captando y más futuro tiene por delante.

Las DeFi o finanzas descentralizadas nacen con la aparición de Ethereum y con ellas se crea un abanico enorme de posibilidades donde invertir y de plataformas que usan la blockchain para poder crear estos activos nuevos. Esta novedosa tendencia puede ser un cambio en las finanzas como las conocemos y entender la tecnología que lo sostiene es posicionar por delante de la mayoría.

Dentro de este contexto, las finanzas descentralizadas han surgido como una revolución en la forma en que se llevan a cabo las transacciones financieras y la gestión de activos. A través de la eliminación de intermediarios y la creación de servicios financieros descentralizados, la DeFi tiene el potencial de democratizar el acceso a servicios financieros y mejorar la eficiencia y transparencia de los actuales.

Sin embargo, también existen desafíos y riesgos asociados con DeFi. La seguridad y eficiencia de los protocolos son aspectos importantísimos que deben ser analizados y comprendidos para asegurar un crecimiento y fiable en esta industria emergente. En este sentido, la ingeniería informática juega un papel fundamental en el desarrollo y la evaluación de esta tecnología.

También es importante conocer las limitaciones que tiene esta tecnología, es por eso por lo que durante el trabajo no solo presentaré las DeFi, si no que intentaré conocer y aprender sobre el trilema cripto. Estas son los tres principales aspectos que intentan tener todas las blockchain, pero hoy en día no es posible, ya que al tener dos se desatiende una. Entonces lograr conocer estas limitaciones y si es posible solucionarlas o si ya existe una blockchain que cumplan las tres.

Aprovechando mi formación en el Doble Grado de Ingeniería Informática y Administración y Dirección de Empresas, recomiendo la lectura de mi otro TFG “Finanzas descentralizadas: Estudio de las estrategias de inversión en proyectos DeFi y su impacto en la diversificación de cartera”, para poder hacer una inmersión en las finanzas descentralizas desde una óptica más financiera.

1.2 Objetivo y Alcance

Este trabajo intenta ser una guía para adentrase y profundizar en el mundo de las criptomonedas. Esto significa que nace con la intención de que en primer lugar me sirva para conocer el funcionamiento de estas tecnologías y una vez terminado sirva al lector para que aprenda en la tecnología y tenga una rica base de este.

También este TFG busca ser la contraparte de mi otro TFG (el de ADE). Donde los dos hablaran de las criptomonedas, con una mirada en las DeFi. Pero la principal diferenciación es que uno será desde una visión técnica y el otro será con una intención más financiera. De esta forma mi intención es abarcar con profundidad la temática de la DeFi dentro del mundo blockchain.

El aporte de valor en este proyecto será el estudio en profundidad del trilema cripto, con un enfoque en el sector DeFi. Este se hará primero mediante el análisis de las principales blockchains y sus características. Para luego, poder hacer una comparativa entre ellas y poder entender los puntos fuertes de cada una y cual utilizar y que protocolos encajarían mejor en cada blockchain dependiendo de las necesidades del usuario.

Este proyecto intentará hacer un estudio y comparativa de las principales blockchains, y servir de esta forma, al menos como texto introductorio para quien se quiera iniciar en la tecnología. Estará más enfocado en la parte técnica, ya que como he mencionado antes, es el fin de este TFG al ser de ingeniería informática.

La metodología de evaluación que usaré intentara centrarse en los parámetros más comunes, para que de esta forma el estudio pueda servir para posteriores usos, ya que si lo hiciera con métricas que solo me interesaban a mi podría perder relevancia en el futuro, al no medir aspectos útiles.

También fruto de este estudio se pretende intentar descubrir proyectos de criptomonedas que puedan ser útiles si estas tuvieran desempeños favorables dentro de los parámetros medidos.

El alcance de este trabajo se limita a la investigación teórica y práctica de la blockchain y la DeFi.

Este trabajo intentará servir como un acercamiento a las tecnologías Blockchain, enfocándose en la DeFi y a través del estudio de las limitaciones de la blockchain a través del trilema cripto. Pretendo sumar a la literatura académica para ayudar y guiar a los que quieran iniciarse en el mundo de las criptomonedas, Blockchain y la DeFi.

El objetivo principal de este Trabajo Fin de Grado es: **Comprender la tecnología subyacente a las criptomonedas.**

La lista de objetivos secundarios que también atacara el TFG es la siguiente:

- Investigar la importancia y relevancia de DeFi en el contexto actual de las finanzas y la tecnología.
- Analizar y comparar las blockchains más comunes utilizadas en el ecosistema DeFi, teniendo en cuenta su descentralización, escalabilidad y seguridad.
- Proponer una metodología para evaluar la descentralización, escalabilidad y seguridad de blockchains.

2 Desarrollo

Este es el capítulo más teórico del proyecto, en el recojo toda la información clave para poder sentar unas bases de conocimiento, y poder entrar en profundidad en esta tecnología. Este es el capítulo principal y donde está el groso del proyecto, está dividido en tres partes, la primera es más teórica, en las segunda y tercera es donde ocurrirá el análisis de las blockchains.

2.1 Bases

Este capítulo establece unas bases de conocimiento mínimas para entender de mejor manera la blockchain, las criptomonedas y la DeFi. Es un trabajo de investigación y centralización de información para adquirir un nivel que permita entender las posteriores partes.

2.1.1 La blockchain y los contratos inteligentes

A lo largo de este punto presentare y entraré en profundidad de los dos temas del título, primero hablaré de la blockchain y después de los contratos inteligentes, que nacieron gracias a la aparición de la blockchain.

2.1.1.1 Introducción a Blockchain

En esta parte del trabajo intentaré introducir esta tecnología que nace con el Bitcoin y a partir de ahí ha revolucionado tanto el mundo tecnológico como el mundo financiero. A lo largo de esta sección haré un estudio de lo más básico a una profundidad técnica de lo que es la blockchain, para que de esta forma tengamos un conocimiento de su evolución y de su utilidad hasta hoy en día. [3]

De esta forma, con esta introducido lograré entender este concepto, para más tarde en mi proyecto poder ir en profundidad en otros temas que han nacido gracias a la aparición de esta tecnología.

Definición y características clave de la tecnología blockchain.

La tecnología blockchain a la que nos referimos hoy en día, es una tecnología innovadora que ha permitido el nacimiento de un sistema más trasparente, descentralizado, digital y seguro. Nace con la creación del Bitcoin en 2008 y desde entonces ha estado en continua evolución y mejora hasta llegar hoy en día. Además, a raíz del Bitcoin han nacido numerosas blockchains las

cuales han intentado corregir errores y necesidades que han aparecido con el tiempo, dando lugar a la creación de un ecosistema con múltiples posibilidades y alternativas donde elegir, pero sin ninguna que haya logrado opacar al Bitcoin. [2][3][10].

Como ya mencioné, desde su nacimiento, la tecnología de blockchain ha sido adaptada y aplicada a una variedad de contextos cada cual más diferente. Ejemplos de esto podría ser el desarrollo de nuevas criptomonedas, plataformas de contratos inteligentes o sistemas de registro y verificación de identidad, entre otros [11][3][10].

La tecnología de blockchain tiene unos principios fundamentales que garantizan su seguridad, transparencia y descentralización, estos serían [8][3]:

- Descentralización: A diferencia de los sistemas centralizados, la tecnología de blockchain reparte la responsabilidad de la verificación y el registro de datos entre todos los nodos participantes en la red. Esto garantiza la transparencia y dificulta la manipulación o el control indebido de los datos.
- Inmutabilidad: La información almacenada en una blockchain es prácticamente inmutable, no puede ser modificada ni eliminada sin el consenso de la mayoría de los nodos. Esto se consigue mediante el uso de funciones criptográficas de hash y que cada bloque este vinculado a su bloque anterior.
- Transparencia: Todos los datos almacenados en una blockchain son visibles para todo el mundo, esto logra garantizar la transparencia y da la posibilidad a quien lo desee de verificar la integridad de los datos.
- Seguridad: La tecnología de blockchain utiliza criptografía avanzada y algoritmos de consenso para garantizar la seguridad de los datos y las transacciones. Además, la naturaleza descentralizada de la red dificulta los ataques malintencionados, ya que un atacante necesitaría controlar la mayoría de los nodos de la red para tener éxito.

Una blockchain está compuesta por una serie de bloques y cada uno contiene un conjunto de transacciones. En cada bloque hay un encabezado y un cuerpo. El encabezado contiene metadatos importantes, como la versión del bloque, la marca de tiempo, el valor hash del bloque anterior y un valor hash único que presenta el contenido del bloque. El cuerpo del bloque almacena las transacciones en sí de ese bloque [10][15][3].

Los bloques están unidos entre sí en secuencia por el valor hash del bloque anterior, que está en el encabezado del bloque actual. Esta conexión crea una cadena de bloques que se extiende desde el primer bloque hasta el bloque más reciente de todos. La estructura de la cadena de bloques garantiza la

inmutabilidad de los datos, porque cualquier intento de modificar un bloque requeriría recalcular los valores hash de todos los bloques subsiguientes, lo que lo hace prácticamente imposible [10][15][3].

La blockchain está formada por nodos y cada uno de los cuales almacena una copia completa de la cadena. Además, participa en el proceso de validación y registro de transacciones. Los nodos pueden ser de varios tipos; nodos completos, nodos ligeros y nodos mineros. Esto será según la función que desempeñen, el nivel de almacenamiento y recursos computacionales que usen [10][15][3].

Los nodos completos guardan una copia entera de la cadena de bloques y verifican todas sus transacciones que se realizan en ella, y los bloques nuevos en función de las reglas del protocolo del que formen parte. Los nodos ligeros almacenan solo una parte de la cadena de bloques y confían en otros nodos para obtener información adicional, esto ayuda a reducir sus requisitos de almacenamiento y recursos computacionales que necesitan. Los nodos mineros solo aparecen en las blockchains que usan prueba de trabajo. Estos compiten para agregar nuevos bloques a la cadena al resolver problemas matemáticos complejos, y reciben recompensas en forma de criptomonedas por el trabajo realizado [10][11][3].

Las transacciones son la unidad básica dentro de una blockchain. Estas aportan intercambio de información y sobre todo dan el valor en una blockchain. Una transacción normal incluye información como la dirección del remitente, la dirección del destinatario, la cantidad que se va a transferir y una firma digital única, generada por el remitente utilizando criptografía de clave pública y privada [10][11][3].

La criptografía juega un papel clave en la autenticación y la seguridad de las transacciones en una blockchain. Las claves públicas y privadas están asociadas a cada usuario, y gracias a esto, permiten la verificación de la propiedad y la autorización de transacciones sin necesidad de revelar la identidad del usuario. Además, las funciones de hash criptográficas se utilizan para vincular bloques y garantizar la inmutabilidad de los datos almacenados en la cadena de bloques [10][11][3].

Una vez que se crea y se firma una transacción, se transmite a la red y a continuación se envía a los nodos para su validación. Los nodos verifican la validez de la transacción comprobando si se cumplen ciertos criterios marcados por la blockchain, como, por ejemplo; la disponibilidad de fondos suficientes, la autenticidad de la firma digital del remitente y que no haya una duplicidad de la transacción [10][11][3].

A continuación, mostraré un pequeño esquema donde mostré de una forma sencilla el funcionamiento de la blockchain según he explicado a lo largo de ese punto.

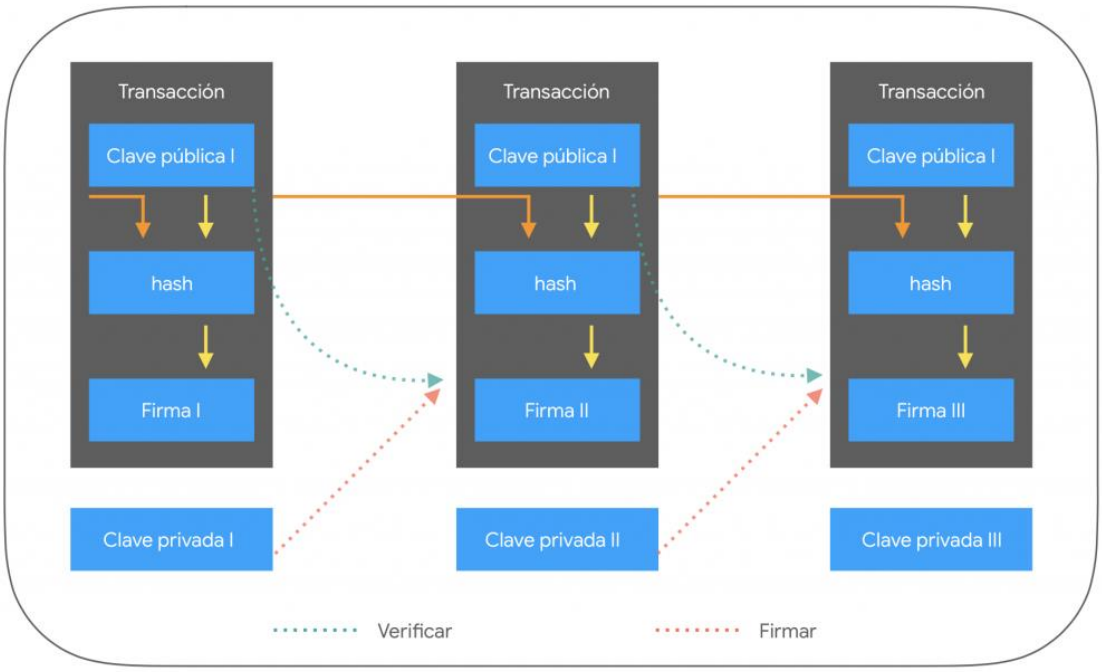

Figura 1. Esquema sobre el funcionamiento de las transacciones [166]

Por último, es importante hablar del consenso dentro de la blockchain. Este punto es fundamental, ya que es el modelo que sigue la blockchain para elegir quién publicará el siguiente bloque nuevo. En las blockchains públicas, que son las más famosas y sobre las que hablaremos en profundidad en este trabajo, los algoritmos de consenso intentan buscar un ganador entre una competencia de usuarios para publicar el siguiente bloque. Las dos principales son la prueba de trabajo y la prueba de participación. La primera busca ganadores entre aquellos que resuelven problemas matemáticos de altísima complejidad, mientras que la segunda se basa en sorteos entre los usuarios que tienen grandes cantidades de la moneda de esa blockchain, poniendo en riesgo su capital si realizan un acto malintencionado. Aunque existen muchos otros tipos de algoritmos de consenso que analizaré más adelante en el apartado correspondiente [10][11][3].

Cómo funcionan la criptografía detrás de las blockchains [3].

Las blockchains se basan en conceptos criptográficos que permiten su funcionamiento, es por eso por lo que es necesario entenderlos, ya que son la base de esta tecnología y lo que permite su funcionamiento. Estos conceptos son para entender cómo se gestiona la confianza en la información, que se traduce en cómo se almacena, como se envía o que la información no haya sido editada por el camino. La herramienta clave son las funciones resumen o

funciones hash. Aun así, es necesario presentar las demás partes para entender los mecanismos que permiten el funcionamiento de la blockchain.

Es importante comenzar explicando que hay que elegir un sistema de numeración especifico dentro de la criptografía según las necesidades que tengamos. Si bien es común que usemos el sistema decimal en la vida cotidiana, en criptografía también son populares los sistemas de numeración binaria y hexadecimal, donde se elegirán según las utilidades que necesitamos de ello, y no arbitreramente. Existen muchos otros tipos, prueba de ello sería que el Bitcoin usa la base58 con una pequeña modificación, que se llama Base58Check. Esto da a entender que, pese a que predomine la base decimal, hay numerosos tipos y habrá que elegir una dependiendo del uso que le queramos dar dentro del método de criptografía que hayamos elegido.

Las funciones hash son operaciones criptográficas que transforman un mensaje de longitud variable en otro de longitud fija. Aunque no pueden cifrar ni descifrar mensajes, son cruciales para garantizar la exactitud de los datos. Nacieron junto con procedimientos de firma electrónica para lograr aumentar su eficacia. Pero más tarde, su uso se amplió a otros ámbitos que estarían relacionados con la protección de la información.

Todos los componentes del mensaje deben estar presentes para que las funciones de resumen unidireccional funcionen. Para que así se pueda garantizar su seguridad e integridad, deben cumplir propiedades como la fuerza de preimagen, la fuerza de segunda preimagen y la fuerza de colisión.

Los principales tipos que se usan de funciones hash son tres; SHA-1, MD5 y SHA-2. SHA-1 se sigue utilizándose, aunque tiene algunos fallos, sin embargo, MD5 y la familia SHA-2, son actualmente los más populares por su mayor seguridad, y esto los hace las funciones hash más utilizadas. La familia SHA-3, es conocida por su adaptabilidad a diversos usos y sería la más nueva y que más crecimiento está teniendo.

También existen otros algoritmos hash, como Adler32, Haval, RipeMD128, RipeMD160, Tiger y Whirlpool, aunque algunos de ellos, como CRC, no están pensados para la seguridad o la integridad.

La firma electrónica es muy similar a la firma manuscrita, pero en formato electrónico. La firma electrónica es un mecanismo para garantizar la autoría de un documento. Este método se desarrolló para garantizar la legitimidad y el origen de los mensajes y documentos electrónicos. Basada en protocolos criptográficos, la firma electrónica es actualmente el protocolo criptográfico más popular y usado.

La firma electrónica, la firma electrónica avanzada y la firma electrónica reconocida son las tres variedades reconocidas por la Ley 59/2003. La firma electrónica se compone de un conjunto de datos electrónicos que permiten

identificar al firmante. Gracias a la firma electrónica avanzada es posible reconocer al firmante y rastrear las alteraciones de los datos que han sido firmados. Una firma electrónica reconocida es una firma electrónica mejorada que se crea utilizando una herramienta de creación de firma segura y se basa en un certificado electrónico reconocido.

Existen diferentes tipos de firma que se agrupan en: la firma en anillo, la firma en grupo y la firma múltiple. Los sistemas de firma múltiple permiten que varias personas firmen colectivamente una misma comunicación. Las firmas de grupo se producen cuando un miembro de un grupo concreto firma anónimamente un mensaje en nombre de todos los miembros del grupo, haciendo falta una sola firma para validar al grupo entero. Las firmas en anillo son firmas digitales que pueden ser creadas por cualquier miembro de un grupo específico y hacen imposible determinar qué clave pertenecía a qué miembro del grupo cuando se creó una firma determinada, ayudan a generar un mayor anonimato.

Primero la producción de la firma y luego la verificación de la firma son las dos etapas que forman parte del proceso criptográfico de la firma electrónica. Estos protocolos exigen la creación o verificación de un criptosistema asimétrico (o de clave pública), que obliga a tener la posesión tanto de la clave privada como de la clave pública asociadas del firmante.

Para crear la mayoría de las firmas digitales, se utilizan sistemas de criptografía asimétricos, como el RSA o los basados en criptografía de curvas elípticas. El algoritmo estándar de firma digital de curva elíptica, conocido como ECDSA (Elliptic Curve Digital Signature Algorithm) utilizando la curva secp256k1, es el que se emplea en las blockchains más populares, como Bitcoin y Ethereum.

Con una técnica criptográfica denominada firma electrónica, se puede garantizar la autenticidad e integridad de los documentos electrónicos. Las firmas electrónicas se presentan en diversas formas y según diversos requisitos de seguridad y privacidad.

Como ya mencioné, la preparación de la firma y la verificación de la firma son los dos componentes clave de ECDSA. Adema la función de resumen, una curva elíptica, un cuerpo finito base, un generador del conjunto de puntos de la curva y las claves pública y privada del firmante son algunas de las entradas esenciales. La clave pública, que el generador multiplica por la clave privada, es un punto de la curva y la clave privada es un número entero.

El firmante realiza las siguientes acciones para firmar un mensaje:

1. Determina el compendio del mensaje en el paso 1.

2. Produce una clave de sesión aleatoria.

3. Determina dos valores utilizando la clave de sesión y el generador.

4. Determina un nuevo valor calculando la inversa de la clave de sesión.

5. Un par de dígitos obtenidos en los pasos anteriores conforman la firma.

El verificador realiza pasos similares para comprobar la firma, y si se cumple un requisito concreto, la firma se considera real y legítima.

Las cadenas de bloques son sistemas de almacenamiento de datos compuestos por bloques de información conectados mediante operaciones hash. El hash del bloque anterior se incorpora a cada bloque nuevo para crear el enlace, lo que da lugar a una lista enlazada de bloques de datos.

Los árboles de Merkle aparecieron con la idea de aumentar la eficacia del almacenamiento y la búsqueda de datos, ya que la búsqueda de información en listas enlazadas con hash no es ideal, especialmente con un elevado número de bloques. Los árboles de Merkle son estructuras de datos que combinan árboles binarios y funciones hash. Ralph Merkle sería el creador y el que daría nombre a esta idea por primera vez en 1979.

Un árbol binario es un grafo en el que cada nodo tiene un máximo de dos hijos y tiene forma de árbol sin ciclos. Sólo los nodos hoja de los árboles de Merkle reciben valores, y el valor de cada nodo intermedio viene determinado por una función hash que suma los valores de todos sus nodos hijos. No es necesario publicar todos los valores del árbol para verificar que se han incluido valores específicos, gracias al aspecto de dependencia de bits de las funciones hash. Esto ayuda a poder disminuir la cantidad de datos que hay que transmitir.

En lugar de agregar el valor de todos los datos protegidos por los bloques, los árboles de Merkle en el contexto de las cadenas de bloques permiten controlar la integridad de la información con sólo incluir el valor del nodo raíz del árbol de Merkle asociado a esa información en los bloques. De ello se derivan importantes ventajas, como la posibilidad de construir clientes mucho más ligeros y la reducción de la cantidad de información que se proporciona explícitamente en la cabecera de un bloque.

Tipos de blockchain [3][4][6][15][5][18]

Hay numerosas formas de clasificar y compara las blockchains entre sí, pero una de las dos formas más comunes es según el tipo de permisos que tiene para participar en ella y la accesibilidad que existe para participar en esa blockchain.

La primera forma de enmarcar los tipos de blockchains que analizaré, será según los tipos de permisos que tiene, lo que significaría quien puede

publicar los bloques en una red. La comparación con la generación pasada de interconexiones sería por ejemplo tener una red privada (intranet) o tener internet. Los tres tipos serian:

- Permissionless:

  Estas son blockchains las cuales carecen de permiso necesario para poder participar en ellas. Este tipo de redes permiten el uso de cualquiera usarlo, como si fuera una aplicación gratuita. Como ya he mencionado, cualquier persona puede ser parte de la blockchain, lo que significa que cualquiera puede leer o escribir en ella, también participar como emisor o receptor.

  Esto genera la necesidad de crear un sistema de protección para el sistema ya que cualquiera puede intervenir en él, sino sería muy vulnerable a ataques y a agentes maliciosos. Esta es la razón por la que nacieron los modelos de consenso, ya que son los encargados de controlar que nadie se aproveche de estos sistemas tan abiertos.

- Permissioned:

  Al contrario del punto anterior, este tipo de blockchains se caracterizan por la necesidad de permisos o autorizaciones para poder publicar bloques dentro de la red, aun así, estos permisos pueden ofrecerse de manera centralizada o descentralizada.

  El hecho que mejor define y por ende la diferencia a esta tipología de redes, es primero la publicación y a raíz de esto la verificación de la identidad de los usuarios que forman parte de la red. De esta forma se le da al usuario autoridad, capacidades y competencias dentro de un sistema. Estas pueden específicas para el usuario o iguales a que a otros usuarios. A raíz de la publicación de la identidad, se repercute en el anonimato en la red, y, por ende, frenando la confianza distribuida. Este hecho supone una desventaja de este tipo de blockchains, pero también esto permite un abanico nuevo de ventajas, como serian:

  - Primero, conocer la identidad y tener el control de los permisos, te permite controlar hasta qué punto puede un usuario actuar dentro de la blockchain, ya que se podría poner permisos de solo lectura, por ejemplo, para así tener un mejer control de loque realizan los usuarios en la blockchain.
  - En situaciones, donde se quiera primar la centralización y la seguridad, por ejemplo, en empresas privadas, es una gran ventaja ya que no necesitarías un modelo de consenso.

- Al ser publica la identidad del usuario, esto genera un desincentivo claro a querer realizar ataque o acciones maliciosas, ya que se conocería con facilidad el usuario que las perpetró.
- El gasto energético y de hardware se reduce, esto se debe a que al no necesitar modelos de consenso no hacen frente al gasto que supone mantenerlos

- Híbridas: Puede existir la posibilidad de que un nodo participe en una blockchain permissionless y en una blockchain permissioned para facilitar la comunicación entre blockchains, lo que se conoce como interoperabilidad. Este hecho puede denominarse hybrid blockchain o blockchain hibrida. Una blockchain puede configurarse para soportar con permiso y/o sin permiso sin permiso, permitiendo que se diera la posibilidad de mezclar los dos tipos anteriores a la vez. De esta forma se podrían obtener las ventajas de ambos sistemas, aunque esto no significa que desaparecerían los problemas de estas.

El segundo tipo de blockchains donde se pueden separar y analizar, sería según la accesibilidad que estas blockchains permiten para ellas. Esto permite hacer un estudio separado analizando el nivel de acceso control y el uso que se les podría dar. Existen 4 tipos actualmente, siendo estos:

- Blockchain pública:
  Una blockchain pública es aquella red que es descentralizada y distribuida, donde cualquiera puede participar, crear y validar transacciones, además de agregar nuevos bloques a la cadena. Este tipo redes son completamente abiertas al público y no necesitan permisos para poder acceder. Lo que se traduce en que cualquier usuario del mundo con acceso a Internet puede unirse, y formar parte del mantenimiento y la seguridad de la red.

  Las blockchains públicas suelen tener algoritmos de consenso como la prueba de trabajo o la prueba de participación para poder asegurar la integridad, la descentralización y también la seguridad de la red, sin restringir el acceso a esta. Y gracias a este hecho, pueden dar a cambio un alto grado de transparencia e inmutabilidad. Aunque también pueden tener problemas de escalabilidad y eficiencia por culpa de su naturaleza abierta y descentralizada.

- Blockchain privada
  Una blockchain privada es una red en la que solo un grupo de participantes tiene acceso y control sobre la creación y validación de transacciones y bloques. Estas redes están generalmente controladas por una entidad centralizada y están diseñadas para casos de uso específicos en los que se requiere una mayor cantidad de control y privacidad que en una red pública.
  Las blockchains privadas utilizan algoritmos de consenso como prueba de autoridad o algoritmo de consenso de federación práctica para poder garantizar la seguridad y la eficiencia en la red. Si bien las blockchains privadas ofrecen un mayor grado de control y eficiencia en comparación con las blockchains públicas, también son menos descentralizadas y transparentes. Pero este hecho no les hace no necesitar un método de consenso, a que seguirá habiendo numerosos usuarios que tengan acceso a esta red de igual manera.

- Blockchain de consorcio o federada
  Una blockchain de consorcio es una red en la que un grupo de organizaciones colaboran y comparte el control de mantener y validar la cadena de bloques. Estas redes están diseñadas para casos de uso específicos en los que se requiere un mayor grado de confianza y cooperación entre los participantes.

  El proceso de validación y consenso se distribuye entre un conjunto de nodos autorizados, generalmente pertenecientes a diferentes organizaciones. Esto garantiza un nivel de descentralización y transparencia, al tiempo que permite un mayor control y eficiencia en comparación con las blockchains públicas, la intención es crear una pseudo blockchain publica, la cual tiene numerosos y diferentes actores, pero que sacrifica descentralización a cabio de un mayor control.

  Las blockchains de consorcio suelen utilizar algoritmos de consenso como prueba de autoridad, algoritmo de consenso de federación práctica o prueba de participación delegada.

- Blockchain híbrida
  Una blockchain híbrida es una combinación de blockchains públicas y privadas que busca aprovechar las ventajas de ambos tipos de redes. Los usuarios pueden realizar transacciones y compartir datos de forma privada y segura dentro de un entorno controlado, al mismo tiempo que

interactúan y se comunican con usuarios y recursos en una red pública más amplia.

Una blockchain híbrida permite a las organizaciones mantener el control y la privacidad de sus datos y transacciones internas mientras se benefician de la transparencia, la descentralización y la seguridad de una red pública.

Este enfoque también puede ayudar a corregir los problemas de escalabilidad y eficiencia, ya que permite que las transacciones y los datos se procesen y almacenen de manera más eficiente en la red privada, mientras tanto las transacciones y los datos públicos se distribuyen en la red pública.

En conclusión, existen dos tipos principales donde se suelen dividir las blockchains, según sus permisos y según su accesibilidad.

Importancia y beneficios de la blockchain [8][3][15]

Como ya hemos visto, la blockchain es una tecnología novedosa, que ha logrado traer con ella numerosa cantidad de posibilidades, fruto de las facultades de esta creación. Y gracias a estas facultades han permitido generar unos rasgos que son novedosos y beneficios en la tecnología los cuales podemos intentar aplicar en numerosos sectores. Estos potenciales beneficios que han transformado en la última década la tecnología son la transparencia, la inmutabilidad, menor intervención, seguridad y automatización son los que destacaré. Y gracias a estas facultades las que pueden permitir un sinfín de mejoras en la tecnología para muchos sectores. Explicaré los cinco grandes beneficios de la blockchain:

- Transparencia:
  La transparencia es una de las características clave de esta tecnología. La forma distribuida y que tengan un registro público permite garantizar una mayor transparencia y trazabilidad. Como cada nodo guarda una copia, esto permite a todos los usuarios auditar y verificar las transacciones que han tenido lugar. En sectores donde la trazabilidad y la auditoria son importantes, este beneficio de las criptomonedas resulta clave.

- Inmutabilidad:
  Otro beneficio de la blockchain es la inmutabilidad. Cuando un bloque es creado y agregado a la cadena, este ya no se puede modificar sin un consenso mayoritario. Esto unido a la descentralización dificulta mucho que se de esa mayoría total. Se convierte en inmutable por la dificultada

del consenso, como acabo de decir, que es necesario para editar el bloque que está escrito en todos los nodos y unido a los bloques anterior. Esto hace una acción que es prácticamente imposible de realizar.

- Reducción de la intermediación:
  Gracias a la transparencia y seguridad, la blockchain permite la eliminación de intermediarios para realización de transacciones. Esto se traduce en una reducción de los costes derivados de intermediación.
- Mayor seguridad:
  Que se combinen la criptografía, el consenso y la descentralización posibilita que las blockchains puedan ser altamente resistentes a ataques. La criptografía de clave pública asegura la identidad y privacidad de los usuarios, luego los mecanismos de consenso, como puede ser la prueba de trabajo, garantizan la integridad y el orden de las transacciones. Además, el hecho que sea una tecnología distribuida dificulta los ataques de un solo punto de fallo, lo que aumenta la seguridad general del sistema.

- Facilita la automatización:
  Una ventaja de la blockchain es que gracias a ella aparecieron los contratos inteligentes, y gracias a estos ha aparecido numerosas posibilidades tanto de eliminar intermediarios, como mencioné en un punto anterior, como de automatizar muchos procesos gracias a mezclar los contratos inteligentes y la blockchain.

2.1.1.2 Historia de la Blockchain

Durante este punto realizaré una puesta a día, desde los pasos previos al nacimiento del Bitcoin, hasta hoy, viendo las distintas fases que ha vivido la blockchain para llegar a donde está hoy.

¿Qué pasó antes del Bitcoin? [25][3][26][27]

Conocer los avances previos a la aparición de la blockchain es fundamental para entender de manera total el desarrollo y evolución que han experimentado las criptomonedas a lo largo del tiempo, así como para identificar cuál fue el punto de partida que les permitió llegar al estado actual en el que se encuentran hoy en día.

Los primeros intentos vienen de conceptos relacionados con la descentralización y la criptografía, como puede ser el trabajo de David Chaum en la década de ochenta sobre el dinero electrónico y el sistema de "hashcash" de Adam Back a finales de los noventa, que serían las bases de la tecnología blockchain. Estos primeros intentos antes de la llegada el Bitcoin y por tanto el comienzo de las criptomonedas como las conocemos se puede dividir en 4 puntos clave:

1. Criptografía y seguridad de la información:

   Antes de la llegada de la tecnología blockchain, ya hubo un interés que iba poco a poco creciendo por la criptografía, la seguridad y protección de la información. La criptografía nos permite proteger la información codificando el mensaje, lo que significa que sólo los destinatarios deseados puedan verlo. Con el paso del tiempo, la criptografía se ha utilizado con numerosas aplicaciones, desde la protección de mensajes militares hasta la protección de transacciones financieras y de datos personales.
2. David Chaum y el dinero electrónico:

   En la década de los ochenta, David Chaum propuso la idea del dinero electrónico para intentar mejorar la privacidad y seguridad de las transacciones financieras. El desarrolló un sistema que lo llamaría "ecash". Este permitiría a los usuarios realizar transacciones anónimas en Internet. Aunque ecash no tuvo éxito prácticamente, sus ideas y esos conceptos sirvieron en las investigaciones y desarrollos posteriores en la tecnología blockchain.
3. Hashcash y la prueba de Trabajo:

   A finales de los noventa, Adam Back presentó el sistema "hashcash", que se basaba en exigir a los usuarios que realizaran un trabajo computacional para así enviar correos electrónicos, y de esta forma de combatir el spam. Esto se conocería como prueba de Trabajo, y se convertiría en un componente clave en la creación de Bitcoin. La prueba de Trabajo se usa para validar y proteger la integridad de las transacciones en la cadena de bloques.
4. B-Money y Bit Gold:

   Entre finales de los noventa y principios de los 2000, se propusieron otros conceptos relacionados con el dinero digital descentralizado que influirían enormemente en la creación de Bitcoin y la tecnología blockchain. Wei Dai crearía el llamado "B-Money" en el 98, que creaba la idea de un sistema de dinero digital descentralizado, el cual funcionaria mediante criptografía. Ya en el 2005 Nick Szabo propuso "Bit Gold" que era un sistema de dinero digital que utilizaba una cadena de bloques para registrar y proteger las transacciones.

Origen de la tecnología blockchain: Bitcoin. [10][12][11][13][14][17]

La tecnología de blockchain como la que conocemos hoy en día, es una innovación que ha posibilitado la creación de un nuevo tipo de sistema digital transparente, seguro y descentralizado. Esta tecnología nace en el año 2008, cuando Satoshi Nakamoto publicó el documento técnico de Bitcoin, conocido como el white paper de Bitcoin. En él se explicaba como una criptomoneda que se basa en la tecnología de blockchain, y se aprovecha de ella para poder tener un funcionamiento descentralizado, a lo largo de todo el documento explica cómo sería el funcionamiento y la tecnología que sustentaría esta nueva criptomoneda. Desde ese momento temporal, la tecnología de blockchain ha evolucionado y se ha ido adaptado a una amplia gama de aplicaciones mucho más allá de las criptomonedas. La publicación del documento técnico de Bitcoin en 2008 fue la primera piedra que permitiría que fuera lo que realmente llevó la idea a la práctica. Haciendo posible la creación de la primera blockchain en 2009, el Bitcoin. Bitcoin combinaría técnicas de criptografía avanzadas, con tecnologías de redes (P2P).

Bitcoin fue diseñado como un sistema monetario digital que no dependiera de intermediarios centralizados, para garantizar la seguridad y la integridad de las transacciones. Este utiliza una red descentralizada de nodos, los cuales verifican y registran las transacciones en una cadena de bloques, asegurando así la transparencia y la inmutabilidad de los datos. Y como ya he mencionado antes, sería la primera blockchain y el padre de esta tecnología, pese a ser primero, Bitcoin sigue siendo el primer proyecto y el más importante [2] no solo en términos de capitalización de mercado, sino que también en términos de seguimiento.

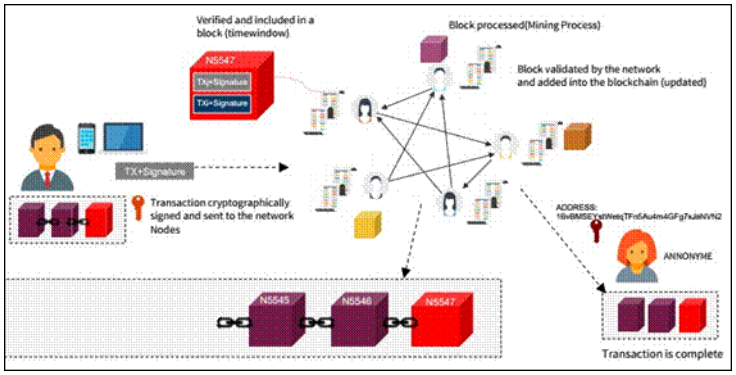

Figura 2. Esquema de funcionamiento de una blockchain [166]

Esta foto resume muy bien como es el funcionamiento del Bitcoin, y por ende el funcionamiento más básico de la blockchain.

Ya entrando un poco más en su evolución hasta hoy, y viendo lo que ha sido la historia de Bitcoin, podemos ver que su historia se dividirá en tres fases claras:

1. 2007 - mediados de 2011:
   En este tiempo Bitcoin era algo desconocido y usado por una pequeña parte de la población, era algo conocido por muy poca gente del sector tecnológico y tanto los gobiernos como las organizaciones no estaban interesados en él.
2. Finales de 2011 - 2015:
   Debido al anonimato de las transferencias, Bitcoin empezó a ser utilizado por terroristas y delincuentes, lo que provocó el rechazo institucional y una mala reputación. La dificultad de establecer políticas contra el blanqueo de capitales en el ecosistema Bitcoin fue otro de los problemas sobre los que alertaron los bancos centrales.
3. 2015 en adelante:
   En esta fase, fruto de la recomendaciones y menciones de expertos, el Bitcoin apareció en la vida de números usuarios y se empezó a dar a conocer. Gracias a estos cambios, comenzó su época de fama y su crecimiento tanto en precio como en usuarios.

Debido a que los bancos tradicionales perdieron clientes tras la crisis financiera del 2008, Bitcoin pudo experimentar un éxito inicial. Después llegaron proyectos empresariales que incorporaron Bitcoin a sus estructuras de negocio, como puede ser el ejemplo de BitPesa en Kenia. Cuando se creó BitPesa en el 2013, su objetivo era aprovechar la popularidad de la plataforma M-Pesa, que facilitaba las transacciones financieras a través de dispositivos móviles. Utilizando Bitcoin, BitPesa pretendía expandir el concepto de M-Pesa más allá de las fronteras internacionales, intentando conseguir un volumen considerable de transferencias internacionales en África. Sin embargo, la relación entre M-Pesa y las empresas basadas en la tecnología Bitcoin finalizó en 2015, después de que el Banco Central de Kenia declarara que BitPesa infringía las normas del sector [12,13]. Este sería uno de los ejemplos más importantes de empresas que ayudarían al desarrollo y popularización del bitcoin y la blockchain en sus inicios.

Evolución y adopción de la tecnología blockchain hasta la fecha. [3] [7][12][5][9]

Tras enunciar como nació la tecnología blockchain gracias al Bitcoin y la historia previa a este. Ahora enunciare que ha ocurrido desde la aparición del Bitcoin hasta nuestros días, intentando seguir un orden cronológico de más antiguo a más reciente. Lo he dividido en siete momentos clave:

1. Nuevas criptomonedas y blockchains.
   Con la aparición del Bitcoin y su posterior éxito, trajo con él la aparición de gran cantidad de criptomonedas y blockchains, algunas en forma de broma como pudo ser Dodge Coin y otras siendo proyectos serios que trataban de suplir fallos de Bitcoin o incluso mejorarlo. Un ejemplo claro de esto último sería Ethereum, el cual nació en el 2015 con la idea de llevar las criptomonedas y la blockchain mucho más allá de simples transacciones financieras. La intención de esta blockchain en su nacimiento (y sigue siendo así hoy en día) era introducir los contratos inteligentes y las aplicaciones descentralizadas. Este sería el primer evento clave tras la aparición de Bitcoin, que ha permitido que haya una enorme cantidad de activos, y sobre todo ha ayudado a que se popularicen las criptomonedas.

2. Contratos inteligentes.
   Los contratos inteligentes fueron introducidos por Ethereum y tras el aparecieron numerosas blockchains que le copiarían y lo adoptarían, siendo una parte clave de la mayoría de blockchain que existen. La llegada de los contratos inteligentes permitió la aparición de las dApps (aplicaciones descentralizadas). Estas dApps se aprovechan de la descentralización inmutabilidad y transparencia de las blockchains para poder desempeñar sus funciones, en sectores tan diversos como puede ser el financiero o el de los videojuegos.

3. Adopción institucional.
   Ya tras la aparición de las criptomonedas, las distintitas instituciones las fueron siguiendo, al principio desconfiando, pero más tarde y poco a poco se fueron uniendo al sector, hasta llegar al punto que existen fondos especializados únicamente en cripto activos. La entrada de capital institucional ha sido clave para el desarrollo ya que ha financiado proyectos y le ha dado al sector un halo de fiabilidad del que carecía antes. También numerosas instituciones están pensando o ya han introducido mejoras en su tecnología, que están relacionadas con el sector blockchain.

4. Desarrollo de soluciones de escalabilidad.
   La expansión de las redes blockchain ha planteado problemas de escalabilidad que en los inicios no se planteó. Las soluciones que se han propuesto incluyen la sharding, que divide la red en partes más pequeñas para aumentar la eficiencia, las cadenas laterales, que son cadenas de bloques paralelas que pueden interactuar con la cadena de bloques principal, y las soluciones de segunda capa o de capa dos, como podría ser la Lightning Network de Bitcoin o Arbitrum con Ethereum, que

permite que las transacciones se realicen fuera de la cadena de bloques principal.

5. Avances en mecanismos de consenso.
   Los mecanismos de consenso son vitales para el correcto funcionamiento de una blockchain, ya que es lo que valida las transacciones de esta y que esté correctamente construida hace que esta parte sea vital para el éxito de dicha blockchain. La primera que existió fue la prueba de trabajo, es la que usa Bitcoin. Años más tarde, en las blockchains publicas aparecería la prueba de participación, la cual es menos ineficiente energéticamente, lo la ha hecho ser uno de los algoritmos de consenso más utilizados.

6. Adopción por parte del público en general.
   Desde el nacimiento de la tecnología hasta hoy, las criptomonedas se han hecho más accesibles y sobre todo más fáciles de usar, lo que ha permitido un acercamiento al público general. Y por tanto un crecimiento exponencial en su uso y en sus usuarios. Esto ha sido posible gracias a la aparición de empresas que han traído productos y servicios que lo han facilitado, como pueden ser billeteras digitales, casas de cambio y plataformas de pago. También ha ayudado enormemente la entrada de capital institucional, ya que eso le ha dado una enorme fiabilidad y legitimidad al sector, atrayendo así al público general.

7. Tendencias actuales y desarrollos.
   Las tendencias más recientes y que serán la base del desarrollo futuro serian:
   a. Finanzas descentralizadas (DeFi):
      Las DeFi son plataformas financieras que permiten a los usuarios realizar transacciones, préstamos y otras actividades financieras sin necesidad de intermediarios utilizando la blockchains como Ethereum. El aumento del número de proyectos y usuarios participando de la DeFi ha provocado un rápido crecimiento del sector.
   b. Tokens no fungibles (NFT):
      La aparición de los NFTs permitió darles propiedad y autenticidad a los objetos digitales, como el arte, la música, los bienes virtuales o coleccionables. Estos son únicos e indivisibles. Su popularidad ha sido tan alta fruto de las nuevas oportunidades que trae consigo para coleccionistas, creadores y los seguidores de esta tecnología.
   c. Privacidad y gobernanza descentralizada:

Debido a la creciente preocupación por la seguridad y la privacidad de los datos, las iniciativas de blockchain están desarrollando soluciones para poder proteger la información de los usuarios, apoyar y promover la gobernanza descentralizada. Esto implica crear sistemas de gobernanza basados en votaciones y propuestas de los usuarios de la red o también mecanismos de privacidad como transacciones privadas y pruebas de conocimiento cero.

2.1.1.3 Funcionamiento detallado de la Blockchain

Durante este punto se explicaré todo lo relacionado con un análisis más detallado del funcionamiento de la blockchain, pero centrándome en las facetas que no hemos tocado aún, son vitales de explicar y por eso necesitaban de un apartado.

Consensos en la blockchain [3][15][16]

La eficacia y la seguridad de la cadena de bloques se mantienen en gran parte gracias al algoritmo de consenso. El rendimiento de una aplicación blockchain puede mejorar significativamente con el uso del algoritmo adecuado. Como ya veníamos comentando en puntos anteriores, esto es un apartado muy importante, ya que las posibilidades de futuro de esa blockchain van en función de la calidad y de la elección de estos.

El momento en el que los sistemas de consenso aparecen en escena, es cuando la transacción se coloca con otras transacciones válidas en un nuevo bloque después de ser validada. Los nodos deben llegar a un acuerdo utilizando un mecanismo de consenso diseñado específicamente para cadenas de bloques antes de poder añadir este bloque a la cadena.

Todos los nodos de la red deben coincidir en el orden y la validez de la posición de cada bloque a través del mecanismo de consenso. Esto evita posibles conflictos o bifurcaciones de la cadena de bloques. El consenso también dificulta a terceros malintencionados la alteración de los datos almacenados en la cadena de bloques, ya que para ello necesitarían tener un control total sobre los nodos de la red.

Con esta tecnología existen dos sistemas de consenso que predominan sobre el resto, estos son el método de prueba de trabajo y el de prueba de participación, ambos son de blockchain abiertas y permissionless y son las dos más famosas. Pero existen otros métodos de consenso menos famosos que presentare ahora:

- Prueba de Autoridad (PoA)
  Una blockchain privada que utiliza el método de consenso de Prueba de Autoridad (PoA) asigna la tarea de validar y añadir nuevos bloques a la blockchain a un grupo predeterminado de nodos autorizados. Estos nodos autorizados, a menudo denominados validadores, se eligen en función de su prestigio, fiabilidad y nivel de experiencia en el campo.

  PoA está menos descentralizado que PoW y PoS, pero ofrece un alto nivel de eficiencia y control en situaciones restringidas. PoA funciona mejor para aplicaciones empresariales y determinados casos de uso que requieren un control centralizado y un consenso rápido.

- Prueba de participación delegada (DPoS)
  La Prueba de Participación Delegada (DPoS) es una versión del algoritmo PoS que añade un sistema representativo. Los titulares de criptomonedas emiten votos para elegir a un representante que se encargará de validar y añadir nuevos bloques a la cadena. Los representantes actúan de forma honorable, ya que corren el riesgo de ser sustituidos por otros representantes si no cumplen con sus obligaciones determinadas por la comunidad.

  El objetivo del DPoS es maximizar la eficiencia y los beneficios de la descentralización minimizando el número de nodos necesarios para alcanzar el consenso. Algunos ejemplos de redes que utilizan DPoS son EOS o Lisk.

- Prueba de tiempo transcurrido (PoET)
  Este es un mecanismo de consenso denominado Prueba del Tiempo Transcurrido (PoET), se basa en el tiempo y no en la capacidad de procesamiento o la interacción del usuario. Antes de proponer un nuevo bloque, cada nodo genera un número aleatorio y espera un tiempo proporcional a ese número. El primer nodo que propone un nuevo bloque y lo añade a la cadena de bloques es el que espera el mínimo tiempo necesario.

  PoET pretende reducir el consumo de energía al tiempo que intenta igualar las posibilidades de propuesta de bloques entre los nodos de forma equitativa. PoET se utiliza principalmente en redes blockchain impulsadas por Intel SGX, incluyendo Hyperledger.

- Algoritmo de consenso de federación práctica (PBFT)
  Para blockchains privadas y de consorcio, el algoritmo de consenso de federación práctica (PBFT) es un algoritmo de consenso bizantino

tolerante a fallos. En el PBFT, los nodos interactúan entre sí mientras participan en múltiples rondas de votación para determinar si las transacciones y los bloques son auténticos.

Mientras el número de nodos maliciosos se mantenga por debajo de un umbral establecido (a menudo inferior a 33%), PBFT protege la seguridad y la integridad de la red incluso frente a nodos maliciosos y fallos del sistema. Las soluciones de cadena de bloques como Hyperledger Fabric utilizan PBFT.

Tras haber visto otros tipos de algoritmos de consenso, los cuales son menos famosos. Hare un estudio más pormenorizado de los dos algoritmos más famosos e importantes, además que son los dos principales dentro de las blockchains públicas, las cuales son el objeto de estudio principal dentro del proyecto.

- Prueba de trabajo (PoW):
  Este modelo se caracteriza por numerosos nodos (mineros) están permanentemente solucionando costosos problemas matemáticos, con la intención de ser el primer que lo consigue, y que este esfuerzo se la prueba de su trabajo. El problema que se resuelve esta creado de tal forma que lo difícil es resolver el problema matemático, y no validar el bloque, por lo que cuando el nodo ganador publique el bloque los demás nodos no les costará validarlo.

  El problema más común que se suele ofrecer es que el hash de la cabecera del futuro bloque sea menor que un valor dado. Los miembros intentan lograr la alteración del hash de la cabecera que dé con el objeto de que modulan el valor nonce, que es uno de los parámetros del input del cálculo. Encontrar un hash n suele ser muy difícil, pero ir recorriendo por cada nonce que se va a probar si se hace mucho más tedioso. El valor dado se va cambiando con el paso del tiempo para que de esta forma se suba o baje la dificultad de minado, también dependerá con la velocidad que se quiera crear un bloque y de la densidad de nodos en la vez. A menor número más difícil será el cálculo.

  Cuando un nodo se convierte en ganador (da con la solución), compartirá el nuevo bloque con el nonce calculado al resto de los nodos de la red. El resto de los nodos verificaran que la solución dad es la correcta y calcularán también el hash igual que le nodo ganador, para cerciorarse de que la respuesta ha sido correcta. Tras esto el nodo ganador añadir el nuevo bloque a la red y lo propagarán sus nodos pares para que llegue rápidamente a toda la red.

La característica clave de este modelo de consenso es que resolver un problema no aumenta la probabilidad de resolver los siguientes. Los demás nodos dejarán de buscar la respuesta una vez que un nodo la haya encontrado y haya tomado el relevo como nodo publicador, momento en el que comenzarán a integrar el nuevo bloque. En consecuencia, la probabilidad de convertirse en el nodo publicador se distribuye.

Además, este modelo protege contra los ataques de seguridad que pretenden tomar el control de numerosos nodos o identidades para ejercer influencia sobre la red. Un ataque de este tipo a Blockchain requiere una gran cantidad de potencia computacional, que sólo es posible con una inversión desproporcionada en hardware. Además, siguen sujetos a un sistema de sorteo lo que significa que a cuanta más potencia computacional se tenga, más probabilidades hay de encontrar la respuesta, pero tampoco es una garantía.

Ese algoritmo de consenso crea un sistema de incentivos, porque los ganadores logran un premio por el esfuerzo realizado para encontrar la solución. Esta lucha por ser el primero en solucionar el problema se conoce como minería.

- Prueba de validación (PoS):
  El algoritmo de prueba de participación aparece como contraposición l de prueba de trabajo, la principal razón de su aparición es por la ineficiencia energética que tiene el sistema de prueba de trabajo, haciendo que se consuman cifras desmesuradas para la creación de un bloque. En el caso del Bitcoin al ser la mayor blockchain este hecho es mucho más llamativo.
  La intención de esta altísima necesidad energética para la creación de bloques es esa misma, limitar el acceso y la capacidad de generación mientras se distribuye la responsabilidad de crearlos. Aun así, el consumo no deja de ser extremo, para algo tan sencillo como es encontrar un publicador.

  La forma de elegir nodo que publique el bloque en la prueba de participación es dándole peso a la aleatoriedad según la participación. Esto significa que, a mayor cantidad de criptomonedas de la blockchain en concreto, mayor será su participación. Esto quita de la ecuación el gasto de tiempo y energía de la prueba de trabajo. Además, al no ser necesario un gasto tan alto de recursos, no es necesario unas tasas altas, por lo que el coste de transacción se reduce.

Entonces, este sistema no solo reduce el malgasto energético y de hardware, sino que al ser elegidos según la cantidad de criptomonedas con las que participes, el nodo está interesado en el correcto funcionamiento de la red. Esto es así porque si el intentara aprovecharse de esa mayor participación, para un acto malicioso, se podía perder credibilidad en el proyecto y, pero ende el perder el valor de su aportación.

El defecto de este sistema es que tiende a beneficiar a los grandes tenedores, y en algunos casos la descentralización no sería tan clara. Es por eso por lo que también se intentan buscar variaciones dentro de esta aleatoriedad para no beneficiar siempre a los mismos.

El papel de los nodos en la blockchain [3][17][7]

Un libro mayor lleva el apunte de todas las transacciones que se hacen. Esta técnica de seguimiento de registros se ha utilizado durante mucho tiempo, tanto con los sistemas analógicos y como con los digitales. Y en diversos contextos, con una presencia significativa en el ámbito financiero. En la era digital se ha seguido utilizando y no ha cambiado su forma: centralizada, Aunque está empezando a evolucionar.

Si todos los nodos de la red compartieran una única copia de los registros del libro mayor, haría que el acceso, la validación y la actualización fueran simultáneos para estos nodos. Tras el éxito del Bitcoin, a esta tecnología se le dio el nombre de Tecnología de Libro Mayor Distribuido (DLT) y está creciendo su uso enormemente. Un tipo de DLT es el blockchain.

Debido a la seguridad, fiabilidad y confianza que ofrecen los libros de contabilidad distribuidos frente a los centralizados, el interés por ellos ha aumentado con esta innovación:

- Es posible destruir un libro de contabilidad central.
- La homogeneidad en hardware, software y arquitectura de red que proporciona un registro central reduce la resistencia a los ataques ya que permite repetir ataques similares en sistemas similares.
- Dado que un registro central suele estar conectado a una zona geográfica concreta, el contexto geográfico determinará cómo se utiliza la información y de qué manera.
- El usuario debe tener fe en que todas las transacciones se registran de forma precisa y legal en un registro central y en que no se están modificando transacciones anteriores.

Debido a su carácter centralizado, un registro central está, en definitiva, mucho más abierto a los ataques: un único objetivo de asalto puede representar

amenazas de seguridad mucho mayores que un sistema distribuido formado por miles de nodos.

Cada nodo de la red tiene depósito temporal de transacciones, que funciona como una especie de buffer duplicado donde se recogen todas las transacciones de la red. Las transacciones de este repositorio se liberan para unirse al nuevo bloque creado, el cual nace de uno de los nodos de la red, una vez que hay suficientes transacciones como para formar un bloque.

La validez y autenticidad de las transacciones se comprueban en el momento de la generación del bloque, esto es así porque cada transacción tiene el formato correcto y además está firmada criptográficamente por el proveedor del activo digital utilizando su clave privada. El bloque entero se rechaza si se rechaza una sola de las transacciones de la lista.

Un conjunto de transacciones que han sido verificados y certificados por la blockchain se almacenarán en el contenido del bloque, mientras que la cabecera del bloque contiene metadatos que sigue unos formatos. Los formatos habituales de las cabeceras de bloque son los siguientes:

- El número de bloque.
- Una representación hash de los datos del bloque.
- El valor nonce.
- Marca de tiempo.
- Dimensiones del bloque.
- El hash del bloque anterior a la cabecera.

El valor hash de los datos de bloque puede descubrirse utilizando diversos métodos. El Árbol de Merkle (el cual se presentó en la parte de criptografía) es uno de los más populares.

Dependiendo de la red y de la versión de Blockchain, el formato de la cabecera puede cambiar. Para que la red pueda entender bajo qué protocolo funciona esa blockchain, se suele incluir en la información de la cabecera un elemento que especifica la versión de la blockchain.

Estas características ayudarán a preservar la coherencia e integridad de la estructura y su contenido a medida que crece. Se establece específicamente que el hash de la cabecera del contenido del bloque X servirá como "resumen" distintivo de su contenido. El bloque Y contendrá entonces un hash del encabezamiento del bloque X. Como resultado, si el bloque X experimenta algún tipo de violación de la integridad de los datos, el bloque Y detectará la violación.

Por lo tanto, si se modifica cualquier información de un bloque anterior, el hash de este bloque cambiará, y los bloques posteriores también cambiarán en consecuencia. Como resultado, es relativamente sencillo reconocer los bloques alterados y eliminarlos. Hay que tener en cuenta que cada vez que se

modifica un bloque en un nodo, se guarda una copia del bloque modificado en todos los demás nodos. Por eso los algoritmos de consenso son claves, ya que permiten la detección de estas alteraciones.

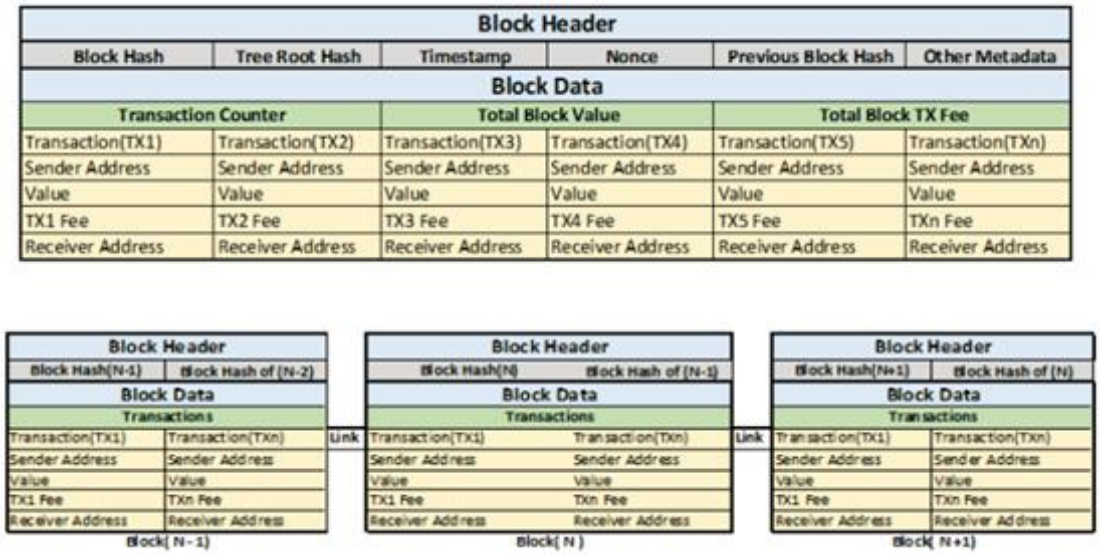

Figura 3. Esquema de funcionamiento de la conexión entre bloques [17]

Problemas comunes y soluciones

Como todo tipo de innovaciones y tecnologías, ninguna es perfecta ni tampoco es infalible. Es por esto, por lo que me gustaría enunciar las tres principales problemáticas a las que se puede enfrentar una blockchain. Aunque la mayoría de las veces estos problemas no tengan una repercusión positiva en la red, se puede dar la situación en que sea por un fin beneficioso. Como sería la bifurcación de Ethereum en la actualización 2.0.

Bifurcación [15][19][20][22]

Dentro del sector de las redes blockchain, la "bifurcación" tiene dos potenciales significados. Ambos tratan la existencia de conflictos transitorios en el registro de bloques en una blockchain, cuando dicho conflicto se mantiene por varios nodos. Sin embargo, existen dos escenarios en los que puede darse esta circunstancia.

La situación donde ocurriría sería si se liberaran varios bloques simultáneamente, prácticamente al instante y cerca unos de otros, algo es parcialmente probable. Esto podría llevar a que se añadieran bloques diferentes en una Blockchain en varios nodos de la red diferentes, lo que daría lugar a varias copias del registro diferentes unas de otras. Es importante no olvidarse

que las transacciones que aún no se han añadido a la blockchain, están esperando a que se genere un nuevo bloque y se guardan en un repositorio que es temporal.

Un bloque A' que contiene las transacciones 1, 2 y 4 podría ser publicado por el nodo A, mientras que un bloque B' con las transacciones 1, 2 y 3 podría ser publicado por el nodo B. Ambos bloques son válidos, pero el hecho de que existan podría ir en contra del principio de integridad, ya que una versión de la Blockchain podría afirmar que ciertos activos digitales se han transferido mientras que la otra versión podría mostrar que no lo han hecho, dependiendo del nodo que estuviéramos mirando.

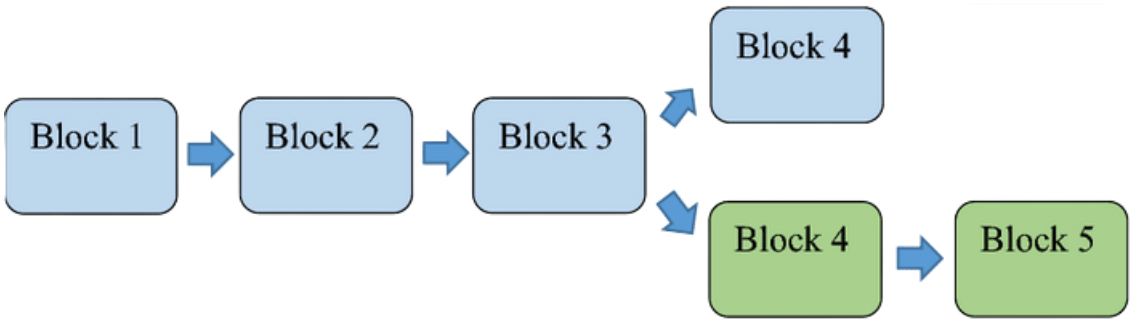

Figura 4. Esquema de bifurcación simplificado

El siguiente bloque se generará normalmente para solucionar este problema, y se elegirá la versión más larga de la Blockchain. Para que se incluya en el siguiente bloque. Las transacciones que no estén cubiertas por la versión seleccionada serán devueltas al repositorio temporal de transacciones. Por esta razón, una transacción no suele confirmarse hasta que se han colocado varios bloques por encima del bloque que la contiene.

Las bifurcaciones o forks también puedes ser modificaciones y actualizaciones de los protocolos y de la arquitectura de la tecnología Blockchain. En este caso también existen conflictos entre las distintas implementaciones de Blockchain en los nodos, pero son provocados por un cambio en el software y no por un conflicto con la publicación de bloques.

Es crucial tener en cuenta que el tamaño de la red afecta a la facilidad con la que se propagan las actualizaciones y se consigue el apoyo de todos los usuarios para dichos cambios. A más tamaño mayor será la dificultad.

Las bifurcaciones pueden ser de dos tipos: bifurcaciones blandas y bifurcaciones duras. En el primer caso se permite la compatibilidad entre nodos actualizados y no actualizados. En otras palabras, los nodos que no han recibido una actualización no tendrían ningún problema para hacer transacciones con los nodos que sí la han recibido. De hecho, si un número

significativo de nodos no adoptara la actualización, las modificaciones se desharían, manteniéndose la versión anterior.

En cambio, las bifurcaciones duras prohíben la compatibilidad con versiones anteriores de manera total. Los nodos no actualizados no podrán seguir desarrollándose junto a los demás miembros de la red nueva, ya que no aceptarán la nueva estructura de bloques. Tendrán que actualizarse para poder aceptar los cambios y seguir comunicándose con los demás usuarios de la red. Si no ocurriera esto, se formarían una red nueva. Y pasarían a existir dos redes, la original y la bifurcada fruto del cambio.

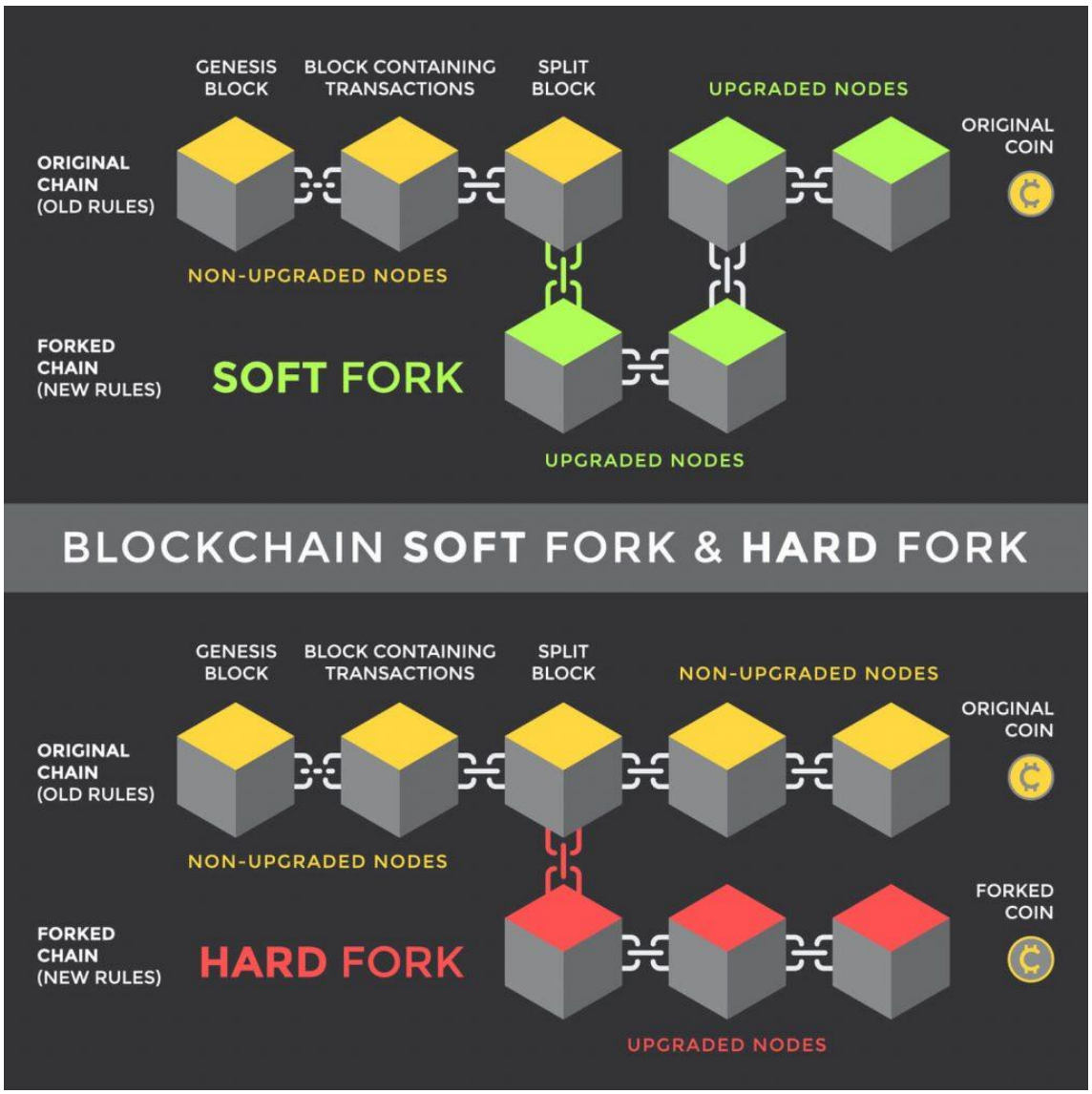

Figura 5. Esquema de diferenciación de bifurcación dura y blanda [167]

En este diagrama se puede diferenciar muy bien las dos formas de bifurcaciones que hay. También se entiende cuando se genera una red nueva y cuando no lo hace.

Ataque del 51% [23][21][3]

Un ataque del 51% es el que se conoce cuando unos mineros logran controlar más del 50% de la tasa de hash de una blockchain y bajo esta premisa realizan su ataque. Los gobernantes tienen autoridad para cambiar la blockchain porque controlan el 51% de los nodos de la red.

Los atacantes podrían prohibir la confirmación de nuevas transacciones, lo que les permitiría detener los pagos entre algunos o todos los usuarios. Mientras estén al mando, también podrían deshacer transacciones realizadas. Uno de los problemas causados para evitar mecanismos de consenso como la prueba de trabajo era que las transacciones inversas podían permitir gastar monedas dos veces.

En una blockchain con un alto índice de participación, lanzar un ataque del 51% es una empresa extremadamente exigente y difícil. La mayoría de las veces, el grupo atacante debería ser capaz de mantener el 51% de la participación requeridos y tener una blockchain de respaldo preparada que pueda instalar cuando sea necesario. A continuación, más tarde, tendrían que superar con éxito el hash de la red principal. Una de las consideraciones más cruciales para evitar un ataque del 51% es el coste de recursos para poder hacerlo.

Además de los gastos, un grupo que intente un ataque del 51% a la red no sólo debe poseer el 51% de la red, sino también lanzar la blockchain modificada en un momento preciso. Es posible que no puedan seguir el ritmo de generación de bloques de la red o introducir su propia cadena antes de que la red "original" genere nuevos bloques legítimos, aunque se controle el 51% de la tasa de hash de la red.

Es por esto por lo que debido a las menores tasas de hash y a la menor participación, esto es concebible en redes más pequeñas y es casi imposible establecer una cadena de bloques modificada en redes grandes.

Problemas de escalabilidad [3][24]

El problema de la escalabilidad de la red es uno de los inconvenientes actuales del uso de algunas redes grandes a la hora de realizar transacciones. En teoría, cada nodo del sistema descentralizado tiene que verificar cada transacción cuando se trata de la red. La escalabilidad es un reto ya que una determinada red sólo puede manejar un cierto número de transacciones en un periodo de tiempo determinado.

La capacidad de la red para gestionar un número considerable de transacciones se conoce como escalabilidad. El rendimiento, los tiempos de transacción, la latencia (el tiempo que tarda un paquete de datos en viajar por la red) y la seguridad son factores de escalabilidad.

La red de una criptomoneda debe ser capaz de manejar un volumen específico de transacciones sin encontrar problemas de procesamiento o retrasos para incentivar el uso de criptomonedas en las transacciones diarias. Para mantener a los mineros motivados y competitivos, una red blockchain también debe ofrecerles incentivos en forma de tarifas y velocidad de transacción.

Dado que las criptomonedas como Bitcoin y Ethereum procesan menos transacciones por segundo (TPS) que los procesadores de pagos tradicionales, es importante reconocer que para los clientes acostumbrados a la banca tradicional se les ofrece un paradigma menos cómodo y moderno. Y es por esto por lo que es necesario mejorar la escalabilidad de las redes y por lo que se le reconoce como un problema de la blockchain.

Dos de los elementos clave que influyen en la reputación y la aceptación de una red de pago son la velocidad y la seguridad de la red. Por ello, la infraestructura de las redes debe aumentar adecuadamente para soportar tanto el aumento de usuarios como el crecimiento del volumen de transacciones.

La respuesta inicial al problema de la escalabilidad era sencilla: duplicar el número de transacciones que puede procesar una cadena de bloques duplicando la cantidad de datos que puede almacenar.

La dificultad de esta solución radicaba en que había que volver a pasar por todo el proceso una vez alcanzado el límite. En otras palabras, si se continúa con este protocolo, la cantidad de almacenamiento necesaria para mantener la blockchain ya no estará bajo el control de la red.

Tras intentar solucionar el problema del escalado de la cadena de bloques con soluciones de capa 1 (lo anteriormente explicado), se desarrolló un grupo de soluciones conocidas como soluciones de capa 2 (L2).

Las redes de capa 2 ayudan a la escalabilidad de forma que logran un mayor rendimiento de las transacciones fuera de la blockchain principal mientras que logran mantener la integridad de la blockchain de capa 1, lo que permite una mayor descentralización, transparencia y seguridad. Esto hace que se traduzca en una experiencia de usuario más asequible, rápida y cómoda, y por tanto, mejorada.

2.1.1.4 Los contratos inteligentes

Los contratos inteligentes son uno de los principales avances que han traído consigo un nuevo abanico de posibilidades dentro de la tecnología blockchain permitiendo numerosas innovaciones.

¿Qué son los contratos inteligentes o smart contracts? ¿Como funcionan? [3][15]

Son programas de ejecución automática, que forman parte de una cadena de bloques. Permitiendo la creación y ejecución de acuerdos digitales entre partes de una manera segura, descentralizada y transparente. Estos contratos están diseñados para facilitar, verificar y cumplir acuerdos y transacciones sin la necesidad de intermediarios.

El concepto de Smart Contracts (contratos inteligentes) nació como idea la primera vez, por Nick Szabo en el noventa y cuatro, antes de que apareciera la tecnología blockchain como tal. Él describió los smart contracts como "un conjunto de promesas, especificadas en formato digital, que incluyen protocolos dentro de los cuales las partes cumplen las promesas". La intención en su inicio era usar la lógica computacional y reglas predefinidas, para conseguir facilitar y lograr automáticamente la ejecución de acuerdos entre dos partes, y poder reducir la dependencia de intermediarios y aumentar la confianza entre las partes interesadas en el acuerdo.

Estos contratos se almacenan en la cadena de bloques y se ejecutará automáticamente cuando se cumplen ciertas condiciones predefinidas por ambas partes, lo que asegura la transparencia, la inmutabilidad y la seguridad de las transacciones que se llevan a cabo.

Cuando se implementa un smart contract en una cadena de bloques, se crea una dirección única que representa el contrato en la red. Los usuarios pueden interactuar con el contrato enviando transacciones a esta dirección, lo que desencadena la ejecución del código del contrato según las condiciones y reglas especificadas. Una vez que se completa la ejecución del contrato, los resultados se registrarán en la cadena de bloques y se distribuyen a todos los nodos de la red para que guarden la transacción.

Cuando se ejecuta un smart contract, el estado puede cambiar en función de las reglas y condiciones especificadas en el código. Un ejemplo podría ser un contrato de préstamo que podría cambiar su estado de "pendiente" a "aprobado" si se cumplen los requisitos predefinidos en el contrato inteligente. Estos cambios de estado se registran en la cadena de bloques y se distribuyen a todos

los nodos de la red, lo que garantiza la transparencia y la inmutabilidad de las transacciones y también de los datos asociados con el contrato.

En el momento que se han cumplido todas las condiciones y requisitos de un Smart Contract, este puede ejecutar automáticamente las acciones correspondientes, como transferir fondos, emitir tokens o actualizar registros en la cadena de bloques. Estas acciones se realizan sin la necesidad de intermediarios, lo que reduce los costos asociados con el cumplimiento y la liquidación de acuerdos y transacciones tradicionales.

Ya que manejan transacciones y datos importantes, es fundamental lograr garantizar la seguridad y la integridad del código del contrato. Los desarrolladores deben que seguir buenas prácticas a la hora de programar. Para que así puedan conseguir seguridad para evitar errores y vulnerabilidades en el código. Normalmente se realiza auditorías de seguridad de terceros antes de su implementación, para poder identificar y solucionar posibles problemas de seguridad y garantizar la protección de los fondos y datos de los usuarios.

Ejemplos de uso de los contratos inteligentes en diferentes industrias. [15][9][7]

La tecnología blockchain y los contratos inteligentes han evolucionado rápidamente y el impacto de dicha evolución se ha podido ver en muchas industrias y sectores. La capacidad de crear sistemas descentralizados, pudiendo tener la posibilidad de automatizar procesos mediante contratos inteligentes a su vez. Esto ha permitido una gran cantidad de aplicaciones innovadoras. Por esta razón voy a comentar los distintos casos de uso que se le pueden dar a los contratos inteligentes en la blockchain:

- Finanzas descentralizadas (DeFi): La DeFi es una de las aplicaciones con más futuro que usa los contratos inteligentes. Esto ha permitido la creación de servicios financieros descentralizados, como pueden ser los préstamos, intercambios, seguros y gestión de activos. Los contratos inteligentes permiten la automatización y la eliminación de intermediarios en el uso de estos servicios, lo que reduce los costos y aumenta la eficiencia.
- Cadena de suministro y logística: La tecnología blockchain puede utilizarse para mejorar la trazabilidad y la transparencia dentro de la cadena de suministro. Los contratos inteligentes pueden automatizar procesos, como sería el seguimiento de productos o el pago a proveedores. Esto logra una mejora en la eficiencia y reduce el riesgo de fraude y manipulación.
- Propiedad intelectual y derechos de autor: Los contratos inteligentes pueden utilizarse para proteger la propiedad intelectual y los derechos de

autor en el mundo digital. Los creadores pueden registrar sus obras en una cadena y utilizar contratos inteligentes para establecer términos de uso, licencias… De esta forma se logra garantizar la protección y el control del trabajo de sus creadores.

- Identidad digital y privacidad: puede utilizarse para crear soluciones de identidad digital descentralizadas y seguras donde los contratos inteligentes ayudarían a gestionar el acceso y la verificación de datos personales. Esto permitiría a los usuarios controlar y proteger su información en línea de una forma personalizada a cada usurario.
- Gobernanza y votación: también se puede utilizar para mejorar la transparencia y la eficiencia en la gobernanza y la votación. Los sistemas de votación basados en blockchain pueden asegurar la integridad y la privacidad de los votos a la hora de tomar decisiones que deban ser consensuadas. Mientras que los contratos inteligentes pueden automatizar la ejecución y el cumplimiento de las normas una vez hayan concluido las votaciones, dando esto una transparencia en la toma de decisiones para el sector público y privando.
- Mercados de predicción y apuestas: Los contratos inteligentes pueden utilizarse para crear mercados de apuestas descentralizados, permitiendo a los usuarios apostar. Esto ofrece una mayor transparencia al tiempo que reducen el riesgo de fraude de las casas de apuestas y de los usuarios.
- Internet de las cosas (IoT): la blockchain y los contratos inteligentes pueden utilizarse en dispositivos y sensores IoT para mejorar la eficiencia y la seguridad de los datos y la interacción entre los dispositivos. Podrán automatizar procesos, como el pago por el uso de recursos o servicios de manera individual, y asegurar la privacidad de los datos dando más capas de anonimato.
- Contratos y acuerdos legales: se pueden utilizar para automatizar y garantizar la ejecución de acuerdos legales de una forma segura y transparente. De esta forma se reduce la necesidad de intermediarios. Esto puede simplificar y agilizar procesos legales y reducir costos enormemente.
- Registros de tierras y propiedades: Los contratos inteligentes pueden ayudar a la automatización de las transferencias y los registros de propiedades. Este aspecto puede utilizarse para crear registros de propiedades descentralizados y así se podría traducir en una mejora de la eficiencia, reducción de los costos, prevención del fraude y la corrupción en la administración de propiedades dando una mayor transparencia al sistema.
- Salud y atención médica: las cadenas de bloques y los contratos inteligentes pueden ayudar mejorar la gestión de datos médicos de los pacientes, no solo desde la perspectiva de los clientes, también ayudaría

a los hospitales. Los contratos inteligentes pueden garantizar la privacidad y el consentimiento de los pacientes al compartir datos.

- Educación y certificación: La tecnología blockchain puede utilizarse para crear registros de certificación de una forma descentralizada y fiable por parte tanto del emisor como del receptor de la titulación. Los contratos inteligentes pueden automatizar la emisión y verificación de certificados, lo que facilitaría la validación, el reconocimiento de habilidades y conocimientos a nivel global, facilitando una educación más global y accesible sin que pierda un nivel de exigencia básico.

Beneficios y desafíos de los contratos inteligentes. [5][3][7][21]

Los contratos inteligentes han traído con ellos un nuevo mundo de ventajas y soluciones, pero también de limitaciones que deben ser conocidas y a ser posible resueltas. Enumeraré tanto las ventajas como los desafíos que tienen los contratos inteligentes:

Las principales ventajas que tienen y que hacen que los contratos inteligentes estén en pleno crecimiento son:

- Autonomía: los contratos inteligentes se ejecutan automáticamente y no requieren la intervención de terceras partes para que se puedan ejecutar. Una vez que se implementan en la cadena de bloques, los contratos funcionan de forma autónoma y se ejecutan automáticamente cuando se cumplen las condiciones previamente establecidas para su ejecución. Esto permite a las partes involucradas en un contrato tener un mayor control y autonomía sobre sus acuerdos y transacciones, sin depender de terceros que validen dichos contratos.
- Confianza: la naturaleza descentralizada y transparente de la tecnología genera un entorno de confianza a la hora de llegar a acuerdos. La información y los datos asociados al acuerdo se vinculan con un contrato que se almacena de manera inmutable en la cadena de bloques y son accesibles por todos los nodos de la red. Esto asegura la transparencia y evita la manipulación o alteración de datos.
- Seguridad: los contratos inteligentes se benefician de la seguridad de la cadena donde están implementados, usando de esta forma la fiabilidad que da dicha red para basar la seguridad de las transacciones necesarias de los contratos. La información y las transacciones asociadas con un contrato están protegidas por criptografía y la arquitectura descentralizada de la cadena, como es en todas las blockchains, es por esto por lo que los contratos inteligentes que se alberguen dentro de una red usaran también la arquitectura de dicha red por loque también usaran su seguridad. Aunque es importante mencionar que la seguridad de un contrato inteligente depende en sobre todo de la calidad y la

seguridad del código del contrato, y no solo de la calidad de la red donde se encuentran.

- Eficiencia y ahorro de costes: como permiten automatizar procesos y transacciones, esto puede aumentar la eficiencia y reducir los costos asociados a la ejecución de acuerdos. Al eliminarse los intermediarios, los contratos inteligentes pueden ser más rápidos y hacer más simples los procesos a la vez que reducen los costos para las partes que intervienen en el contrato.
- Exactitud en el cumplimiento: los contratos inteligentes se basan en reglas y condiciones predefinidas. Esto asegura que los tratos se ejecuten de manera precisa, exacta y consistente. Dado que los contratos se ejecutan siempre automáticamente y no están sujetos a interpretación humana, se reduce el riesgo de incumplimiento y disputas entre las partes, ya que tanto las cláusulas como las condiciones se conocen previamente y son imposibles de modificar.
- Flexibilidad y personalización: estos se pueden adaptar y personalizar según las necesidades de las distintas partes y las aplicaciones que intervengan. Los desarrolladores pueden preparar contratos para abordar una amplia variedad de casos de uso y escenarios diferentes.
- Interoperabilidad: los contratos inteligentes pueden interactuar entre sí (entre varios contratos inteligentes) y también con otros componentes del ecosistema blockchain, como pueden ser tokens y otras o las mismas aplicaciones descentralizadas. Esto permite la creación de soluciones mucho más complejas y sofisticadas, que puedan aprovechan la combinación de múltiples contratos en una cadena y lograr un abanico de posibilidades muy superior.
- Transparencia regulatoria: estos permiten una mayor transparencia en la gestión y el cumplimiento de las regulaciones. Al codificar las reglas y requisitos directamente en el contrato, se pueden asegurar real el cumplimiento, además que, al ser descentralizadas, el cumplimiento de las regulaciones es visible para todo aquel que quiera asegurarse.
- Innovación y crecimiento del ecosistema: Se está impulsando una ola de innovación y crecimiento en el ecosistema blockchain. La capacidad de crear y personalizar contratos inteligentes de una forma tan transparente y libre ha permitido a los desarrolladores y empresas diseñar servicios novedosos que pueden transformar industrias y modelos de negocio tradicionales aprovechando el potencial de esta tecnología, sin olvidar usos o utilidades de los negocios tradicionales.

Los desafíos o limitaciones que enfrentan los contratos inteligentes y tienen que hacer frente hoy en día son:

- Seguridad y vulnerabilidades: Como se mencionó en el punto de beneficios, la seguridad de un smart contract, no solo va en función de la calidad de la blockchain, sino también de la calidad del código del propio contrato. Uno de los desafíos más importantes en el desarrollo y en el uso de contratos inteligentes es garantizar la seguridad contra ataques maliciosos. Los errores en el código del contrato o los fallos de seguridad pueden ser explotados por atacantes, lo que puede resultar en la pérdida de fondos, datos o cambios en los parámetros del contrato, resultando en una pérdida de la confianza entre las partes interesadas. Para rebajar estos riesgos, es clave seguir buenas prácticas de programación y seguridad. También se deben realizan auditorías de seguridad antes de implementar un contrato en la cadena de bloques.
- Escalabilidad y rendimiento: La escalabilidad y el rendimiento pueden verse limitados por la capacidad de almacenamiento y la velocidad de los bloques de la red donde se encuentren los contratos inteligentes. En redes congestionadas o con tiempos de confirmación lentos, los contratos pueden tardar más tiempo en ejecutarse y consumir más recursos. Esto puede afectar la viabilidad y el costo de las aplicaciones basadas en contratos inteligentes, ya que los hacen menos eficientes y más inaccesibles para un público acostumbrado a transacciones rápidas. Una de las soluciones de escalabilidad que están naciendo son blockchains de segunda capa (L2), estas pueden ayudar a abordar estos problemas al permitir una mayor cantidad de transacciones por segundo y una ejecución más rápida de las transacciones.
- Interoperabilidad y compatibilidad: A medida que el ecosistema blockchain se expande y se desarrollan nuevas cadenas de bloques y protocolos en ellas, la interoperabilidad y la compatibilidad entre diferentes plataformas se convierten en un reto que puede permitir un sinfín de mejoras. Los contratos inteligentes creados en una plataforma pueden no ser compatibles en otra y esto podría limitar su uso y adopción en algunos casos de uso. La creación de soluciones de interoperabilidad es fundamental para garantizar la adopción y el crecimiento de los ecosistemas permitiendo una mayor interconexión entre redes y entre contratos inteligente, lo que facilita la adopción y permite nuevas posibilidades. Esta es uno de los mayores desafíos a los que hace frente y del cual más se está trabajando en él.
- Adopción y barreras tecnológicas: La adopción de contratos inteligentes para usos tradicionales puede verse obstaculizada por barreras tecnológicas y también de conocimiento. Las organizaciones y los usuarios pueden ser reacios a adoptar contratos inteligentes debido a la falta de conocimiento y confianza con la tecnología blockchain y las preocupaciones relacionadas con la seguridad que aún existen. La educación sobre los beneficios y los usos de los contratos inteligentes,

así como el desarrollo de herramientas fáciles pueden ayudar a superar estas barreras de entrada al público general.

- Regulación y cumplimiento legal: La naturaleza descentralizada y autónoma de los contratos inteligentes puede crear incertidumbre y por esa tanto crear preocupaciones en torno a la responsabilidad legal de lo ocurrido al ejecutarse el contrato, la protección del consumidor y el si se aplican las leyes existentes.
- Privacidad: los datos y las transacciones en una cadena de bloques pública son visibles y accesibles para todos los participantes de la red, esto puede ser un problema para aplicaciones que necesitan una privacidad o que buscan crear una privacidad y protección de datos. Una de las soluciones posibles son las cadenas de bloques privadas, pero estas no seguirían el concepto descentralizado de las cadenas públicas.
- Oráculos y datos externos: Los oráculos son servicios que proporcionan datos externos a los contratos inteligentes, ya que a menudo requieren información y datos para ejecutarse correctamente y poder conocer información del mundo real con exactitud. Pero pueden ser un punto de vulnerabilidad y un riesgo potencial para la seguridad de los contratos, ya que necesitaran oráculos de calidad y fiables de los que obtener dicha información. Garantizar la seguridad de los oráculos y de la información que proporcionan estos es esencial para un desempeño seguro de los contratos inteligentes.
- Actualizaciones: normalmente se ejecutan en un entorno inmutable y una vez se ha implementado, ya no se pueden modificar con facilidad. Esto puede ser problemas si se encuentran errores en el contrato, también si las partes desean modificar los términos del acuerdo, ya que al ser inmutable estos pequeños cambios son muy difíciles de implementar. Se podría solucionar este problema con diseños de contratos inteligentes con mecanismos de actualización y control de versiones. Esto permitiría cambios y mejoras sin comprometer la seguridad y la integridad del contrato.

Tras una explicación en profundidad de los contratos inteligentes, me gustaría comentar cuales son los principales lenguajes de programación que se usan, ya que puede ser de utilidad por si quisiéramos lazarnos a programar un Smart Contract. Existen varios lenguajes de programación y plataformas que permiten la creación, pero nombraré las principales o más famosas:

- Solidity: Es el lenguaje de programación más popular para crear contratos inteligentes en la plataforma Ethereum. Este es un lenguaje de alto nivel basado en JavaScript y C++, que permite a los desarrolladores crear y desplegar contratos inteligentes de manera rápida y eficiente.

- Vyper: Es un lenguaje de programación alternativo que también funciona en la red de Ethereum. Este lenguaje se centra en la seguridad y en la simplicidad. Por el contrario, Vyper es un lenguaje de bajo nivel basado en Python y no incluye características como herencia y modificadores, lo que facilita la lectura de los contratos por terceros que quieran analizar el código.
- Bitcoin Script: Es un lenguaje de programación poco flexible que permite la creación de contratos simples y seguros en la red Bitcoin. Es un lenguaje de bajo nivel.
- Chaincode: Es el lenguaje de programación utilizado para crear contratos inteligentes en la plataforma Hyperledger. Chaincode permite a los desarrolladores escribir en lenguajes de programación populares como pueden ser Go, JavaScript y Java. Esta característica es diferencial, ya que facilita la enormemente la adopción general enormemente, acercándose a los lenguajes más comunes.

2.1.1.5 Blockchain y contratos inteligentes: Casos de Uso Prácticos

La tecnología blockchain y los contratos inteligentes tienen la capacidad para producir registros inmutables, fiables y transparentes. Esto ha permitido que se haya encontrado una amplia gama de aplicaciones en numerosas industrias donde pueden utilizar esta tecnología para mejorar la industria. Entre las principales y más llamativas, las votaciones, la gestión de la cadena de suministro, los registros de la propiedad y las finanzas. En este apartado hablaré de algunos de estos casos de uso que ya se dan en el día a día. Haciendo hincapié en cómo la tecnología blockchain y los contratos inteligentes están revolucionando y generando nuevas posibilidades en diversos campos.

Uso de la blockchain y contratos inteligentes en las finanzas: DeFi. [28]

Actualmente es el sector en el que más se está utilizando este tipo de tecnología. La menguante confianza en las instituciones financieras, que no dejan de adquirir influencia y poder, o los obstáculos que impiden el acceso a determinados mercados y operaciones financieras son algunos de los elementos que han desencadenado la formación de un mercado descentralizado.

La arquitectura distribuida de Blockchain permite la automatización y la desintermediación en el sector financiero, reduciendo tiempo y gastos al tiempo

que antepone la seguridad y la transparencia. La interoperabilidad, la inclusión, la custodia de valor o derechos, así como un exceso de otras nuevas opciones que facilitan o democratizan el flujo de valor, son impulsadas por las finanzas descentralizadas.

Con la llegada de la DeFi, se ha introducido una nueva forma de financiación descentralizada más adaptable y eficaz. Algunos de los instrumentos y operaciones que se han reinventado o creado incluyen criptomonedas, tokens, activos digitales, financiación, préstamos, derivados, seguros, pensiones, fondos de liquidez, mercados automatizados y arbitraje.

Uso en la cadena de suministro y logística. [15][7][11]

La tecnología Blockchain tiene el potencial de resolver los problemas de auditoría, transparencia y trazabilidad de muchas mercancías diferentes en la cadena logística. Puede utilizarse tanto para mercancías de otro tipo como para las de la industria alimentaria, donde el origen y la trazabilidad son especialmente importantes.

Por ejemplo, comprender la gestión de la fabricación, la venta al por mayor, la distribución, las certificaciones, las normas de producción u otros elementos que intervienen en las distintas etapas de la cadena, desde la creación del producto hasta su recepción por el cliente, es crucial en el ámbito de la seguridad alimentaria.

La iniciativa Everledger, que confirma la procedencia de los diamantes utilizando Blockchain para detener la propagación de los diamantes de sangre, es una aplicación práctica más allá del negocio alimentario.

Uso en el registro de propiedades y títulos. [15][7][11]

La seguridad criptográfica de la tecnología Blockchain garantiza la exclusividad, fiabilidad e irrevocabilidad de las claves privadas. Los beneficiarios podrán dar fe veraz de su identificación o de cualquier certificación relacionada con ella bajo la asunción de la custodia responsable de dichas claves.

Prácticamente cualquier sector en el que se desee sustituir el almacenamiento convencional de bases de datos por una verificación más transparente y con soporte en redes blockchain puede aplicar este eficaz método de sellado de datos.

Además, el carácter centralizado de los sistemas de seguridad convencionales supone una amenaza para el respeto a la certificación de patentes, marcas, pruebas de autoría o autenticidad, licencias y otra serie de activos intangibles o derechos digitales.

Con la ayuda de la blockchain, que aprovecha las ventajas de la descentralización, los creadores y propietarios disponen ahora de nuevas herramientas para supervisar y gestionar estos activos, lo que garantiza una protección mucho mejor de los derechos legales sobre esta información sensible.

Uso en la votación y gobierno electrónico. [15][7][11]

Las nuevas oportunidades de gobernanza que puede ofrecer blockchain han sido ampliamente estudiadas en la literatura académica. Los procesos de consenso que sustentan los numerosos productos, servicios y redes son uno de los principales atractivos de la tecnología.

Empezando por una ilustración más sencilla, estas tecnologías podrían utilizarse como plataforma públicamente verificable para tabular los votos en unas elecciones. Más adelante, la descentralización podría permitir a una administración pública aprovechar la trazabilidad ciudadana en los procesos estatales y ser más eficaz. También puede anunciarse como un foro donde la gente puede expresarse libremente y sin miedo a la censura.

El término "Organización Autónoma Descentralizada", o DAO, se utiliza a un nivel superior. Estas organizaciones carecen de dirección y administración humanas, como su nombre indica. Los contratos inteligentes se utilizan para codificarlas como alternativa. También son organizaciones que representarán mucho más fielmente a la comunidad porque todos tendrán voz y voto a la hora de determinar su estrategia. Este tipo de estructura puede funcionar como una organización pública o privada.

Hay grandes promesas en torno a este tema, que se cita e investiga con frecuencia por las aplicaciones que podría ofrecer. Sin embargo, para demostrar su validez, no se cuenta con un historial probado ni con implementaciones macroscópicas significativas. El hecho de que en 2016 se produjera un ataque que supuso el robo de 60 millones de dólares en moneda Ether es una prueba de la inmadurez del DAO.

2.1.2 Definición de Finanzas Descentralizadas

Las Finanzas Descentralizadas (DeFi) son un método vanguardista e innovador de manejar el dinero que pretende transformar la forma en que la gente piensa y utiliza los servicios y bienes financieros. Con el fin de eliminar o disminuir la necesidad de intermediarios, como bancos, aseguradoras... La palabra "DeFi" se utiliza para definir una amplia idea de aplicaciones, protocolos y tecnología. [28][29][30][31][32]

El nacimiento de la DeFi ha sido impulsado por la rápida evolución, crecimiento y adopción de tecnologías blockchain, y por ende, las criptomonedas. También por el crecimiento del mercado de tokens y activos digitales. La naturaleza descentralizada de las redes blockchain ha permitido el desarrollo de aplicaciones basadas en contratos inteligentes, que automatizan y ejecutan acuerdos financieros sin la intervención de intermediarios. Esto ha permitido la creación de un ecosistema financiero más inclusivo, seguro y transparente, en el que los usuarios pueden acceder y participar en servicios financieros sin restricciones geográficas, barreras económicas o burocracia. Logrando dar un cambio inimaginable a uno de los sectores más centralizados, inaccesibles, opacos y con más intermediarios.

Tanto las comunidades tecnológicas y de criptomonedas como el sector financiero tradicional están interesados en DeFi. Esto ha suscitado mucha atención y debate sobre las oportunidades y debilidades que plantea, que se debe sobre todo a su potencial para revolucionar el acceso a los servicios financieros y la forma en que los particulares gestionan y utilizan su dinero. Las plataformas y protocolos DeFi suelen ser de código abierto, lo que fomenta la transparencia y da a los usuarios más poder y conocimiento sobre los servicios. Además, la transparencia permite reducir la probabilidad de fraude.

DeFi también tiene componibilidad y modularidad, que se refieren a la capacidad de integrar y combinar fácilmente varias aplicaciones, protocolos o servicios. Las aplicaciones y protocolos DeFi están pensados para ser modulares y componibles, lo que facilita su combinación e integración para desarrollar nuevos servicios y productos financieros. Con el uso de esta capacidad, los usuarios y desarrolladores pueden combinar las características y funcionalidades de varias aplicaciones DeFi para producir soluciones financieras más sofisticadas.

En cuanto a la privacidad y seguridad, las transacciones en DeFi son transparentes y audibles para cualquier usuario que quiera ver las transacciones realizadas en una blockchain. Aunque los protocolos y aplicaciones también pueden implementar medidas de privacidad y seguridad para proteger la información de los usuarios y poder dar una mayor capa de

seguridad a estos. También es importante destacar que la descentralización también ayuda a reducir los riesgos de ataques ya que aumenta la dificultad de estos y da transparencia a las transacciones.

Al adoptar mecanismos de gobernanza descentralizados que permiten a los usuarios que poseen tokens de gobernanza participar en el progreso y la toma de decisiones del protocolo, DeFi también pretende implicar a la comunidad. Esto apoya una estrategia de desarrollo y gestión más democrática y arraigada en la comunidad.

La apertura y la accesibilidad de DeFi ayudan a crear un entorno de innovación y experimentación en el espacio financiero. Esto ha permitido crear protocolos con numerosos intentos y creaciones de activos financieros muy novedosos, que en el sistema tradicional no serían posibles, ni por la regulación, ni por la dificultad de innovar, otra razón en particular que explica la rápida entrada de capital en el sector. Los emprendedores pueden probar rápidamente nuevos productos y servicios financieros, lo que ayuda a la innovación y la disrupción en la industria. Además, los usuarios pueden explorar y adoptar nuevas soluciones financieras sin las restricciones de los sistemas financieros tradicionales. Que no existan tantas trabas como en el sector tradicional, permite que sea más fácil la entrada tanto de emprendedores como de usuarios.

La flexibilidad y personalización que ofrecen las aplicaciones DeFi también son características clave, ya que los usuarios pueden seleccionar y combinar diferentes protocolos y aplicaciones para crear opciones financieras adaptadas a sus necesidades y preferencias. Esto contrasta enormemente con muchos sistemas financieros tradicionales, que solo llegan a ofrecen productos estandarizados y no se acercan tanto al usuario, dando productos más personalizados.

En la DeFi existen diferentes protocolos, aplicaciones y servicios que forman el ecosistema de las finanzas descentralizadas. Estos componentes pueden clasificarse en varias categorías, según su función. Ahora presentaré algunos de los componentes más importantes en la DeFi:

- Intercambios descentralizados (DEX): son plataformas de intercambio de criptomonedas que operan sin necesidad de la intervención de una autoridad central o intermediario que las controle para que funcionen. Permiten a los usuarios intercambiar tokens de manera directa y segura, utilizando contratos inteligentes y tecnología blockchain para facilitar las transacciones, solo con el cumplimiento de contratos inteligentes funciona el intercambio, no es necesario un intermediario centralizado que configure los intercambios. Algunos ejemplos populares de DEXes son Uniswap, SushiSwap o Balancer.
- Plataformas de préstamos: permiten a los usuarios obtener préstamos o también prestar fondos ganar intereses sobre sus criptoactivos sin la

necesidad de recurrir a intermediarios financieros centralizados. Funcionan utilizando contratos inteligentes que donde se conecta automáticamente a los prestatarios y los prestamistas, estableciendo los términos y condiciones del préstamo previamente. De esta forma, a través de una plataforma que sirve de contacto entre las dos partes se puede o bien ganar una rentabilidad o bien obtener un préstamo. Ejemplos de estas plataformas son Aave, Compound o MakerDAO.

- Protocolos de gestión de activos: estos protocolos permiten a los usuarios invertir y también poder administrar sus activos de manera eficiente dentro de la DeFi. Estos protocolos pueden incluir soluciones de inversión automatizada, que ayudan a los usuarios a diversificar sus inversiones y a poder reducir los riesgos de estas. Ejemplos de este tipo protocolos DeFi son Yearn Finance, Set Protocol y dHEDGE.
- Derivados y productos financieros sintéticos: los derivados y productos financieros sintéticos dan la posibilidad de tener presencia en activos tradicionales y también no tradicionales de una forma descentralizada, haciendo una copia de estos, los cuales tienen el mismo valor en todo momento. Estos productos pueden incluir opciones, futuros, swaps y tokens sintéticos que representan un activo subyacente. Ejemplos de plataformas serian Synthetix, UMA y dYdX.
- Seguros descentralizados: son servicios que permiten a los usuarios protegerse contra riesgos financieros y de seguridad dentro del espacio DeFi, igual que los seguros tradicionales. Esto se consigue mediante el uso de contratos inteligentes y tecnología blockchain, que ofrecen coberturas de seguros de manera descentralizada y sin intermediarios de por medio. Unos ejemplos de plataformas son Nexus Mutual, Cover Protocol y Armor.
- Gobernanza descentralizada y tokens de gobernanza: la gobernanza descentralizada es un aspecto muy importante de la DeFi y también muy utilizado, porque permite a los usuarios participar en la toma de decisiones y en la gestión de los protocolos a través de votaciones según el número de tokens del protocolo que tengan. Los tokens de gobernanza son activos digitales que dan derechos de voto y en algún caso puede llegar a dar otros privilegios a sus titulares siempre en relación con el gobierno de un protocolo DeFi. Estos tokens pueden ser adquiridos, intercambiados y utilizados para influir en las decisiones dentro de un ecosistema DeFi. Algunos ejemplos de tokens de gobernanza son UNI (Uniswap), AAVE (Aave) y COMP (Compound).
- Infraestructuras y herramientas de desarrollo: para poder construir y mejorar las aplicaciones DeFi, los desarrolladores requieren una infraestructuras y herramientas de desarrollo especializadas que les servían para este cometido. Estas infraestructuras y herramientas incluyen marcos de desarrollo, bibliotecas de contratos inteligentes,

interfaces de programación de aplicaciones (API) y servicios de infraestructura de blockchain. Gracias a la aparición de estas herramientas, se ha facilitado enormemente a los desarrolladores la creación dentro de las DeFi y por tanto su crecimiento. Algunos ejemplos son Truffle Suite, Hardhat y The Graph.

- Herramientas de análisis: como el ecosistema DeFi es altamente fragmentado y está en constante evolución, los agregadores y herramientas de análisis juegan un papel muy importante en ayudar a los usuarios a navegar, comparar y evaluar diferentes los componentes y servicios de DeFi. Estos pueden proporcionar información en tiempo real sobre precios, riesgos, rendimientos y potenciales oportunidades en el mundo DeFi. También facilitan la interacción con múltiples protocolos y aplicaciones de una manera uniforme y eficiente. Algún tipo de herramientas pueden ser Zapper, DeBank y DeFi Pulse.

El análisis técnico de la DeFi es un enfoque que tiene en cuenta varios aspectos esenciales para evaluar y comparar protocolos y aplicaciones. El diseño y la arquitectura de los protocolos y aplicaciones de DeFi son importantes factores a tener en cuenta porque tienen un impacto significativo en su funcionalidad, rendimiento y usabilidad. El análisis también debe examinar cómo estos protocolos y aplicaciones interactúan con otros sistemas y redes. Esto es esencial para facilitar la transferencia y el flujo de activos entre varios tipos de plataformas y aplicaciones de finanzas de descentralizadas.

La seguridad es otro elemento crucial en el análisis técnico dentro de las finanzas descentralizadas. Se debe examinar la seguridad de los protocolos y aplicaciones para asegurarse que se protegen los fondos y los datos de los usuarios. Además del análisis de las prácticas de auditoría que se hacen en los contratos inteligentes y también la implementación de soluciones de seguridad confiables y probadas son parte de esto.

El éxito a largo plazo de los protocolos y aplicaciones DeFi depende del rendimiento y la eficiencia. La escalabilidad es la capacidad de un protocolo para manejar un mayor número de usuarios y transacciones sin disminuir su rendimiento y velocidad al que suele operar sin congestión. La capacidad del protocolo para realizar transacciones y operaciones con un uso óptimo de recursos se conoce como eficiencia. Además, es capital investigar cómo los protocolos abordan los problemas de eficiencia y escalabilidad, y como esos intentos de soluciones han traído innovaciones como el sharding de capa 2 y las técnicas de optimización de contratos inteligentes.

Finalmente, un análisis técnico adecuado también debe intentar identificar y evaluar riesgos, y a continuación, tiene que evaluar las medidas de mitigación y protección implementadas por los protocolos y aplicaciones, como seguros, fondos de reserva y prácticas de gestión de riesgos. Además, es

necesario investigar cómo manejan y cumplen con las regulaciones y si cumplen las leyes pertinentes. Esto también incluye el análisis de cómo, cuándo y a partir de qué situación, los protocolos utilizan controles y salvaguardias para mantener un nivel de seguridad alto para la tranquilidad del usuario.

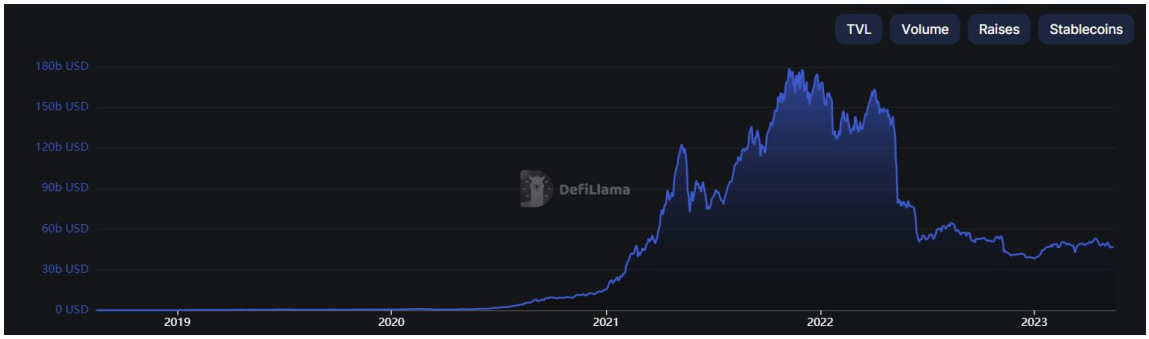

Figura 6. Gráfico de capital bloqueado dentro de todas las blockchains [89]

Como podemos ver en este gráfico, el capital dentro del mundo DeFi es muy alto, llegando a los 60 mil millones de dólares. Es importante recordar que es una aplicación de la blockchain bastante nueva, y que todo lo que hay a su alrededor no tiene mucho recorrido. Por lo que haya tanto capital de usuarios que deciden exponerse a estos riesgos es algo para tener en cuenta. Si es cierto que desde la caída del 2022 no se han recuperado los máximos, si no que se ha estabilizado en los 60 mil millones, pero con la llegada de numerosos protocolos e ideas nuevas, es probable que la DeFi se establezca como alternativa de inversión dentro del mundo blockchain.

Viendo estos datos podemos entender la dimensión de esta aplicación de la blockchain y entender que es importante estudiar tanto los riesgos y limitaciones de las DeFi, como los de las blockchains. Ya que, si la entrada de capital aumenta, tiene que ser un espacio seguro para los usuarios.

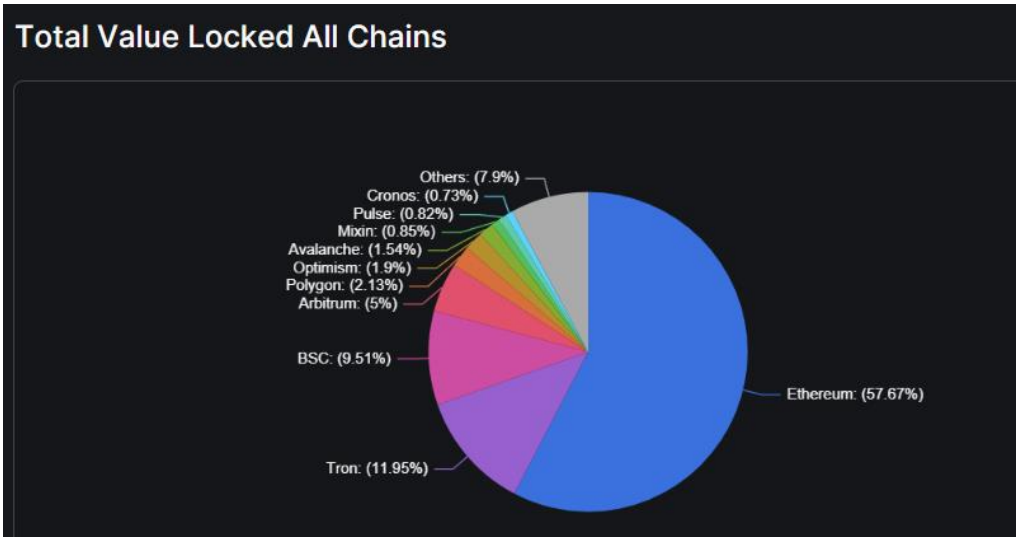

Figura 7. Gráficas de dominancia de blockchains en el sector DeFi [89]

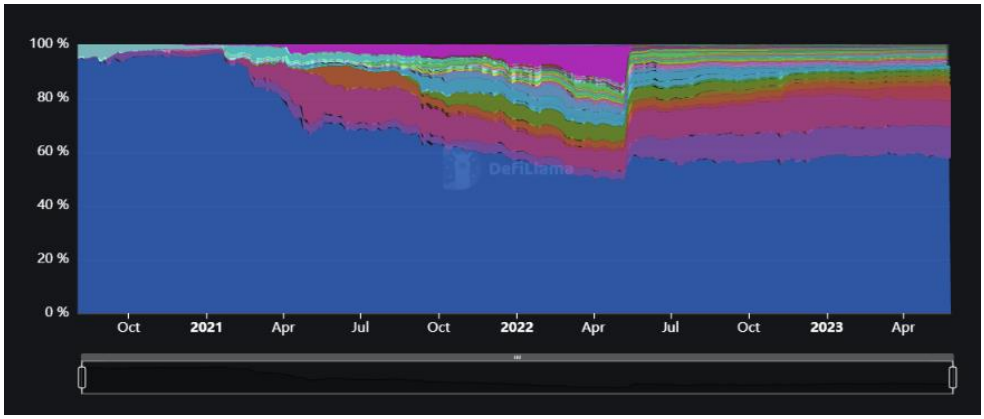

Figura 8. Gráficas de dominancia en el tiempo de blockchains en el sector DeFi [89]

En esta imagen podemos ver la dominancia de las distintas blockchain dentro del sector DeFi. En la tabla superior podemos ver un gráfico de sectores donde la blockchain de Ethereum representa más de la mitad de todo el capital bloqueado (TVL) en DeFi. Luego tenemos BSC y Tron como redes con más TVL, pero muy cerca del 10% cada una. Esto denota la dominancia de Ethereum dentro del sector.

Si nos fijamos en la segunda gráfica, es una tabla de la dominancia histórica. En ella vemos que en el comienzo Ethereum llegó a representar hasta más de un 90% del capital en la DeFi. Pero desde ese punto, y durante la tendencia alcista que hubo en el mundo cripto, hasta mayo del 2022 su peso decreció, debido a la aparición de blockchains nuevas que traían soluciones nuevas al sector. Tras el a debacle volvió a subir y se estabilizo en la franja de entre 50%-60%. Estos datos dejan claro la importancia histórica y actual de Ethereum en las DeFi.

Name	Category	1d Change	7d Change	1m Change	TVL
1 Lido 5 chains	Liquid Staking	-0.62%	-0.24%	-1.22%	$11.7b
2 MakerDAO 1 chain	CDP	-1.02%	-0.67%	-9.91%	$6.85b
3 AAVE 8 chains		-0.85%	+3.40%	-2.69%	$5.15b
4 Curve Finance 12 chains		-0.94%	+0.98%	-7.75%	$4.2b
5 Uniswap 6 chains		-0.66%	+4.11%	-2.47%	$4.08b
6 JustLend 1 chain	Lending	-1.45%	+1.62%	-0.71%	$3.68b
7 Convex Finance 3 chains	Yield	-0.65%	+2.03%	-3.76%	$3.29b
8 Coinbase Wrapped Staked... 1 chain	Liquid Staking	-1.02%	+1.87%	-5.35%	$2.12b
9 PancakeSwap 3 chains		-0.51%	+2.59%	-8.02%	$2.12b
10 Instadapp 1 chain	Services	-1.14%	+2.13%	-1.99%	$2.09b
11 Compound Finance 3 chains		-0.48%	+3.42%	-1.37%	$1.85b

Figura 9. Tabla de los 11 protocolos con mayor capital invertido en ellos [89]

En esta imagen podemos ver los 11 principales proyectos dentro del sector DeFi. Como vemos, la mayoría del capital se encuentra dentro de estos 11 protocolos. Esto permite entender el poder que tienen estos protocolos, y la obligación que tienen sus desarrolladores de saber protegerlos para que no sufran ataques ni el robo de sus fondos.

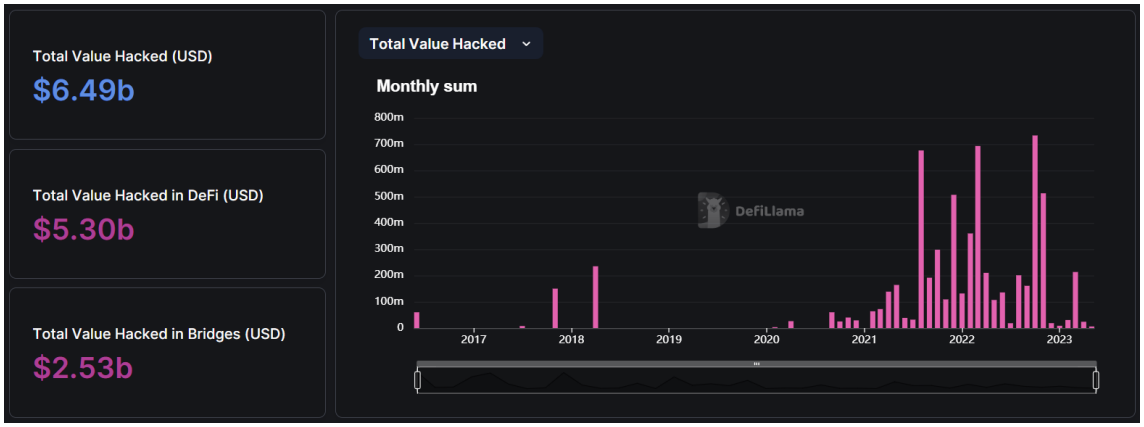

Figura 10. Gráfica con el capital robado en DeFi por meses [89]

Este es un gráfico que recopila la cantidad total de dinero robado por meses, es por esto por lo que antes he comentado la importancia de tener protocolos seguros. Como podemos ver sigue una tendencia bajista, por lo que es posible que los desarrolladores estén intentando realizar entornos más seguros y protegidos. Esta es una pieza clave para lograr una mayor adopción, ya que, si los robos de fondos fueran algo común, no se lograría crear confianza para que los usuarios pusieran sus fondos.

Name	Date	Chains	Classification	Technique	Link	Amount lost
DEUS Finance	5 May, 2023, 00:00		Protocol Logic	Burn Function Mistake		$5m
Level Finance	1 May, 2023, 00:00		Protocol Logic	Referral Claims Logic Exploit		$1m
0vix	28 Apr, 2023, 00:00		Ecosystem	Flashloan Donate Function Logic Exploit		$2m
Merlin	25 Apr, 2023, 00:00		Rugpull	Drained Contracts		$1.82m
Hundred Finance	15 Apr, 2023, 00:00		Protocol Logic	Price Manipulation Attack		$7m
Yearn	13 Apr, 2023, 00:00		Ecosystem	Flashloan Misconfiguration Exploit		$11.539m
Sentiment	4 Apr, 2023, 00:00		Ecosystem	Flashloan Reentrancy Attack		$1m
Allbridge	2 Apr, 2023, 00:00		Ecosystem	Flashloan Price Oracle Attack		$0.57m
Safemoon	28 Mar, 2023, 00:00		Protocol Logic	Access Control Exploit		$8.9m
Paraspace *whitehack	17 Mar, 2023, 00:00		Protocol Logic	Borrow Logic Exploit		$5m
Euler Finance	13 Mar, 2023, 00:00		Protocol Logic	Flashloan Donate Function Logic Exploit		$197m

Figura 11. Últimos hackeos en la DeFi a 28/05/2023 [89]

En esta imagen podemos ver cuando han sido los últimos hackeos de importancia en el sector, y ver la causa de ellos. Es interesante ver que no hay de cuantías muy altas prácticamente, pero se siguen produciendo casi cada semana. Esto una vez más presenta la importancia que tiene mejorar la seguridad en los protocolos para que de esta forma se pueda dar mayor fiabilidad al usuario.

2.1.3 Blockchains más comunes

A lo largo de este punto haré una investigación pormenorizada de las principales blockchains que hay hoy en día. Analizaré tanto sus propuestas como la realidad que ya son hoy, viendo tanto sus virtudes como sus defectos. Están ordenadas por orden de importancia dentro del panorama cripto a día de hoy:

Bitcoin: [10][15][17][33][34][35]

En un white paper publicado en 2008 bajo el pseudónimo de Satoshi Nakamoto, una persona o grupo de personas de las cuales no se conoce aún la identidad, presentarían el Bitcoin que se presentó dinero digital descentralizado. El Bitcoin hacía posibles las transacciones seguras entre pares sin necesidad de que exista una entidad centralizada, como un sería un banco o un gobierno, y utilizando la tecnología blockchain que nacía en ese momento con el Bitcoin.

La blockchain es la tecnología central del funcionamiento de Bitcoin. Una cadena de bloques es un registro descentralizado de acceso público de todas las transacciones realizadas en la red Bitcoin. Los nodos mineros de la red Bitcoin verifican y registran las transacciones mantienen el libro de contabilidad. El primer minero que resuelve con éxito un problema matemático con una dificultad muy alta añade el siguiente bloque de transacciones a la cadena de bloques. Cada nodo minero compite para conseguirlo entre ellos, a través de la inversión de mayores cantidades de potencia computacional. La prueba de trabajo es el procedimiento utilizado para mantener la seguridad y fiabilidad de la red Bitcoin haciendo que sea computacionalmente difícil cambiar transacciones anteriores por la inversión en material informático para conseguirlo.

Uno de los principales avances de Bitcoin es su método para evitar el doble gasto el cual es un problema de las monedas digitales cuando un usuario gasta repetidamente la misma cantidad. Bitcoin hace que cada vez que se produce una transacción, esta se transmita a toda la red y los mineros la añaden al bloque que se está construyendo en ese momento. La transacción se considera confirmada cuando se añade un bloque a la cadena de bloques. La transacción se vuelve más segura cuando se añaden bloques adicionales al bloque que la contiene porque es mucho más difícil deshacerlo, ya que tendría que deshacer los bloques previos y si deshacer uno es difícil varios serian prácticamente imposible.

El Bitcoin se transfiere entre direcciones Bitcoin durante las transacciones. Una dirección está vinculada a dos claves criptográficas: una

clave pública que se pone a disposición del público y se utiliza para recibir los pagos, y una clave privada que se mantiene en privado y se utiliza para firmar las transacciones de la red. Este sistema es un componente clave de la naturaleza de Bitcoin y le permite realizar transacciones irreversibles y poder ofrecer un sólido control de la propiedad a los tenedores.

Bitcoin también ofrece en parte, un cierto grado de anonimato. Aunque todas las transacciones son visibles para todos los usuarios que lo deseen, estas están vinculadas a direcciones y no a personas. Solo si se conociera quien es el propietario de esa dirección, se podría eliminar dicho anonimato.

La oferta regulada de Bitcoin es una de sus características fundamentales y más interesantes. Existe un total de veintiún millones de Bitcoins como máximo. Los mineros reciben nuevos Bitcoins como pago. La recompensa a los mineros se reduce a la mitad cada cuatro años, lo que se conoce como halving. El valor de Bitcoin se ve influido significativamente por esta escasez, haciendo que sea deflacionario.

Bitcoin ofrece gran cantidad de ventajas, pero también tiene serios inconvenientes también. Aunque sea muy necesario para la seguridad, el sistema de prueba de trabajo consume una energía desmesurada y ha llamado la atención por sus efectos negativos sobre el medio ambiente. Otro aspecto que mejorar es la comparación con las redes de pago convencionales para el procesado de pagos. La red Bitcoin puede procesar comparativamente menos transacciones, lo que se traduce en tiempos de confirmación más largos y comisiones más elevadas en momentos de gran demanda, que sería lo opuesto a los procesadores de pagos convencionales.

La descentralización de Bitcoin también tiene inconvenientes. Al no existir una autoridad centralizada, puede resultar difícil alcanzar un consenso entre mineros y usuarios a la hora de realizar cambios en el protocolo que lo puedan llegar a favorecer. Como resultado, se han producido acaloradas discusiones entre los usuarios de Bitcoin e incluso llegando a producirse escisiones en la cadena de bloques que han dado lugar a otras monedas como Bitcoin Cash.

A pesar de estas dificultades, Bitcoin ha demostrado ser increíblemente robusto y seguro. Aunque su valor ha experimentado altibajos extremos, ha perdurado y se ha ganado una amplia aceptación como medio de intercambio y como depósito de valor. Además, su aparición ha permitido la llegada de miles de criptomonedas, muchas de las cuales se basan en la tecnología que sustenta Bitcoin o tratan de mejorarla lo que ha generado una revolución en la moneda digital y la aparición de una tecnología disruptiva.

Figura 12. Tabla de las bifurcaciones que ha habido en Bitcoin [168]

En la imagen anterior podemos ver las 4 bifurcaciones duras que ha tenido Bitcoin y todas las actualizaciones que tuvo a través de bifurcaciones blandas. Como he mencionado antes, estas bifurcaciones son fruto de los

desacuerdos en la comunidad fruto de la alta descentralización y la falta de consenso. Las otras tres criptomonedas resultantes a día de hoy siguen existiendo y algunas con capitalizaciones de mercado altas.

Ethereum: [36][37][38][39]

Con su novedosa capacidad para crear aplicaciones descentralizadas (dApps) en el momento que nació, Ethereum, es la segunda mayor blockchain por valor de mercado a nivel mundial. Esta red ha logrado estar a la vanguardia de la revolución blockchain.

Los desarrolladores de web 3.0 pueden crear e implementar contratos inteligentes, y por tanto aplicaciones descentralizadas utilizando la blockchain y basándose en su descentralización y en el código abierto de Ethereum. Estos contratos inteligentes, tienen las condiciones del contrato escritas directamente en líneas de código. La cadena de bloques de Ethereum se mantiene actualizada gracias a los nodos conectados a la red, donde cada uno de los nodos conserva tanto una copia del historial de transacciones de la red como una de su estado actual.

La capacidad de adaptabilidad y flexibilidad de Ethereum son dos de sus principales ventajas, que gracias a estas ha podido crecer y posicionarse como una red de referencia. Esto es, porque los desarrolladores preferían usar esta red para llevar a cabo sus proyectos fruto de adaptabilidad y flexibilidad que ya mencioné. Su lenguaje de programación nativo es Solidity, que permite a los desarrolladores crear sus propios contratos inteligentes y dApps en la red. Fue creado como un blockchain de uso general. Como resultado de estas características, ya existen muchas más dApps en Ethereum, que abarcan sectores como las DeFi, los juegos y los intercambios descentralizados entre otros muchos sectores.

Ethereum también introdujo el gas, que es una unidad de medida para cuantificar el trabajo computacional. El gas es un recurso necesario para todas las operaciones realizadas en la plataforma Ethereum, incluidas las transacciones y la ejecución de contratos inteligentes. Además, la utilización de este enfoque reduce el spam en la red y distribuye mejor los recursos de una forma equitativa.

Sin embargo, Ethereum no está exento de problemas. La escalabilidad es uno de los principales puntos a mejorar en la red de Ethereum. Cuando hay una alta utilización de la red Ethereum se puede dar que haya mayor congestión, lo que se traduciría en mayores retrasos en las transacciones y tarifas más caras. Este ha sido un obstáculo importante para la adopción

generalizada de Ethereum, ya que impide un rendimiento deseado si la cantidad de usuarios usándola a la vez es muy alta.

La seguridad también preocupa en la red Ethereum. Los contratos inteligentes establecidos sobre la cadena de bloques son tan seguros como el código que los creó, aunque la propia cadena de bloques sea segura. Por lo que muchas veces los problemas de seguridad que pueden a aparecer son más por la culpa del desarrollador de los contratos inteligente. Pero estas potenciales debilidades pueden dañar la reputación de la red, sin ser su culpa directa. En algunos casos muy sonados, los fallos en el código de los contratos inteligentes permitieron realizar exploits que provocaron grandes pérdidas.

Ethereum 2.0, también está experimentando una mejora considerable con respecto a Ethereum 1.0. Con esta mejora se pretende mejorar la escalabilidad, la seguridad y la sostenibilidad de la red. Sin embargo, este cambio es difícil y está plagado de peligros. Por esta razón están yendo tan lentas las implementaciones y los cambios. Ya que no es fácil los cambios que se quieren implementar, por lo que el desarrollo debe de ser lento para evitar errores que puedan comprometer la red.

En resumen, Ethereum ha sido una fuerza pionera en la industria del blockchain, popularizando las dApps y los contratos inteligentes. Con continuos avances y actualizaciones destinados a mejorar su plataforma, sigue siendo un actor destacado en el ecosistema blockchain a pesar de sus dificultades.

Binance Smart Chain: [40][41][42][43]

La cadena de bloques llamada Binance Smart Chain (BSC) nació para dar cabida a la programabilidad de contratos inteligentes que faltaba en Binance Chain (BC). Hoy en día BSC funciona en paralelo a BC. BSC comenzó a funcionar en septiembre de 2020, casi un año y medio después que apareciera la BC. Nació con la intención de para albergar contratos inteligentes e interoperabilidad con Ethereum, se desarrolló imitando las capacidades de Ethereum y también otras plataformas dApp para albergarlas en su ecosistema.

Los métodos de consenso utilizados por BC y BSC son una de sus principales diferencias. BSC utiliza un proceso de consenso prueba de participación de autoridad (PoSA), mientras que BC utiliza el mecanismo de consenso BFT de Tendermint. Esto permite a otros validadores participar en la gobernanza y la validación de bloques, al tiempo que permite a Binance mantener el control sobre la blockchain de BSC mediante la selección de validadores de bloques. Su funcionalidad es otro aspecto en el que difieren. Mientras que BSC es una blockchain pensada para el uso de smart contracts

que puede alojar cualquier dApp, incluidas las que se ejecutan en Ethereum. Sin embargo, la BC aloja principalmente el DEX de Binance.

A pesar de estos avances, BSC tiene ventajas y desventajas. La centralización de BSC es uno de sus mayores inconvenientes. BSC se diferencia de las cadenas de bloques convencionales en que sólo hay 21 validadores en la red en un momento dado. Debido a esta centralización, el sistema es más susceptible a fallos de funcionamiento, intrusiones, requisitos legales y ciberataques. Además, la obtención del permiso de Binance y el cumplimiento de estrictas normas mínimas hacen que sea difícil y requiera muchos recursos convertirse en operador de nodos o validador en BSC. Además, como Binance suele contratar a desarrolladores de Solidity, que suelen mantener su atención principal en la red Ethereum, la innovación en BSC depende principalmente del desarrollo de Ethereum y pocas veces es tomada como red principal para el desarrollo.

BSC, por otro lado, presenta una serie de ventajas. Los desarrolladores y usuarios que se trasladan desde Ethereum y otras blockchains inteligentes se sienten atraídos por el bajo coste de las transacciones. Una transacción en Ethereum puede costar más de 1.000 veces más que una en BSC en momentos de intensa congestión de la red, y a menudo constantes el gasto de gas por transacción. Debido a la consolidada base de usuarios de Binance, BSC también se beneficia de mayores tasas de adopción, lo que hace que el número de direcciones únicas y las transacciones globales en BSC aumenten exponencialmente. Además, los desarrolladores han construido una serie de puentes entre cadenas que facilitan a los usuarios de BSC la transferencia de tokens entre otras redes de cadenas de bloques. En la actualidad, Binance Bridge admite más de 40 monedas, por estas razones, BSC es la segunda red más grande en términos de capitalización de mercado y se entiende por la gran atracción de usuarios que tiene.

Polkadot y Cosmos: [45][46][47]

La idea de la interoperabilidad de las cadenas de bloques está generando mucho interés en el ámbito de la tecnología de blockchain. Alude a la capacidad de varias redes de cadenas de bloques para interactuar y comunicarse entre sí, permitiendo la transferencia de datos y transacciones entre varios sistemas de cadenas de bloques. Se trata de un desarrollo clave en el avance de la tecnología blockchain porque permite un ecosistema más eficaz e integrado de varias blockchains, cada una con sus propias características y capacidades especiales, y enfocada en unas necesidades particulares.

El problema de la interoperabilidad de las cadenas de bloques está siendo abordado por una amplia gama de iniciativas y soluciones adicionales. Se trata de cadenas laterales adicionales, protocolos entre cadenas y distintos tipos de puentes que permiten la interacción entre distintas cadenas de bloques y logrando la deseada interoperabilidad.

Sin embargo, la verdadera interoperabilidad no está exenta de dificultades. Entre ellas hay problemas técnicos como la gestión de varios sistemas de consenso, la garantía de una comunicación segura y fiable entre varias cadenas de bloques y la gestión de posibles problemas de escalabilidad. Y también se dan otros obstáculos que serían no técnicos como por ejemplo la necesidad de estandarización, problemas de gobernanza y restricciones normativas.

A pesar de estos obstáculos, el objetivo de la interoperabilidad de la blockchain supone un avance significativo en el desarrollo de la tecnología de cadena de bloques. Podría abrir nuevas vías para las aplicaciones blockchain y construir un ecosistema blockchain más cohesionado y eficaz.

Polkadot: [48] [49] [50]

Un marco multi cadena llamado Polkadot promete hacer posible que distintas cadenas de bloques trabajen juntas de forma escalable y segura. Gavin Wood (cofundador de Ethereum), Robert Habermeier y Peter Czaban son sus creadores. En su oferta inicial de monedas, en octubre de 2017, recaudó unos 144 millones de dólares. El DOT sirve como criptodivisa nativa de la blockchain Polkadot.

La red Polkadot se compone de una cadena de bloques principal, conocida como "relay chain", y otras cadenas paralelas creadas por los usuarios, conocidas como "parachains". Mientras que los parachains se subastan para ser accesibles a todos los equipos de desarrollo, lo que permite a los proyectos individuales construir y ejecutar sus propias blockchains dentro de la infraestructura Polkadot, la cadena principal sirve como capa de gobierno de la red. La relay chain se encarga de garantizar que se lleven a cabo las transacciones, alcanzar el consenso y validar los datos, ofrece la seguridad a las parachains. La red puede realizar 1.000 transacciones por segundo según su white paper.

Polkadot utiliza un algoritmo de consenso prueba de participación. El protocolo empleado, se basa en el protocolo Ouroboros. Además, la red cuenta con puentes que enlazan blockchains y permiten la transferencia de datos, lo que hace posible la compatibilidad con otras redes como podrían ser Bitcoin o Cardano. Al igual que las parachains, las parathreads funcionan sobre una base de "pago por uso" y no requieren una conectividad constante a la red Polkadot.

En términos de funcionalidad potencial, los parathreads y los parachains son muy similares, pero difieren en el modelo económico. Son una alternativa para proyectos que no hayan ganado una subasta o no estén interesados en ella.

El modelo de consenso prueba de participación de Polkadot distingue tres tipos de interesados:

1. Nominadores: Seleccionan validadores fiables y protegen las cadenas de principal.
2. Validadores: Participan en el consenso, validan las pruebas de los recopiladores y ponen en juego el DOT.
3. Recopiladores: Estas personas mantienen registros precisos de las transacciones de parachain y los transmiten a los validadores de la cadena de principal.

El token DOT se emplea tanto para la gobernanza como para el staking. El staking promueve el comportamiento ético entre los usuarios de la red al mantener DOT como garantía de "buen" comportamiento, lo que ayuda a garantizar la seguridad de la red. Los usuarios de DOT que realizan staking, tienen derecho a votar en cuestiones de gobernanza utilizando una participación ponderada.

La compatibilidad, escalabilidad y seguridad de Polkadot son sus puntos más fuertes. Permite que una amplia gama de cadenas de bloques de la red Polkadot cooperen permitiendo transferencias entre cadenas de cualquier tipo de datos o activo. Ofrece escalabilidad transaccional al distribuir las transacciones a través de numerosas blockchains paralelas y escalabilidad económica al permitir que un conjunto compartido de validadores asegure múltiples blockchains. Gracias a su enfoque de prueba de participación nominada de nueva generación, también proporciona una eficiencia energética excepcional.

Sin embargo, Polkadot tiene varios inconvenientes. La complejidad de su arquitectura puede plantear problemas a consumidores y desarrolladores. La cadena de principal, que puede ser un único punto de fallo, es crucial para la seguridad de toda la red. Además, puede ser difícil establecer en la práctica el buen funcionamiento y la cooperación de numerosas partes interesadas, incluidos nominadores, validadores y recopiladores, que son cruciales para el éxito de Polkadot, estas razones hacen que aún no hay un gran número de usuarios y desarrolladores usando la red.

En conclusión, Polkadot ofrece un marco que permite la cooperación de varias blockchains, lo que representa un avance significativo en la tecnología blockchain.

Cosmos: [51] [52] [53] [54]

Con la tecnología blockchain y un ecosistema descentralizado, Cosmos pretende crear el Internet del futuro. Debido a que diferentes redes de blockchain utilizan tecnologías diferentes e incompatibles entre sí, Cosmos ha crecido en popularidad buscando una solución para este problema. Cosmos quiere construir una red en la que estas numerosas aplicaciones blockchain puedan cooperar. Las cadenas de bloques del sistema pueden cooperar entre sí, como en Internet. A pesar de que las dos blockchains están separadas entre sí, pueden conectarse y hablar entre ellas dándose información útil para que pueda existir esta relación. Los usuarios pueden incluso intercambiar divisas con Cosmos en una red blockchain diferente. Cosmos utiliza el método de consenso tolerancia a faltas bizantinas (BFT) dentro del PoS.

Cosmos intenta aborda numerosos problemas que ponen en peligro la cadena de bloques que tenemos hasta hoy. La escalabilidad es uno de estos problemas a enfrentarse. Aunque el número de transacciones por segundo se está intentando que aumente y mejorarlo, todavía no es tan rápido como las plataformas tradicionales. Un ejemplo de esto sería Ethereum, que puede manejar hasta 15 transacciones por segundo, pero sin embargo el sistema Visa puede manejar más de 1600. Pero con Cosmos, donde pueden unirse múltiples blockchains, podemos anticiparnos a que podrá ser una plataforma que funcione más rápidamente.

La soberanía es otro gran problema. La ejecución de cualquier aplicación debe estar completamente bajo control de la blockchain. Si hay un problema con la plataforma blockchain tradicional, hay que confiar en que la plataforma blockchain sabrá resolverlo satisfactoriamente. Al ofrecer una plataforma más rápida, fácil de usar y de fácil acceso, Cosmos ayuda a resolver todos estos problemas.

Al ofrecer una solución personalizada para desarrolladores, el kit de desarrollo de software de Cosmos ayuda al creador de blockchain. En lugar de concentrarse en lo que ocurre en segundo plano, deben concentrarse en el desarrollo de aplicaciones blockchain. Utilizando este software, el tiempo de crecimiento de blockchain se reduce de años a semanas. La modularidad y la seguridad basada en la eficiencia son los dos aspectos en los que se centra el SDK. El objetivo del SDK de Cosmos es facilitar a los desarrolladores de blockchain la creación de aplicaciones.

Cosmos es un apasionante proyecto de blockchain que pretende resolver algunos de los problemas básicos que experimenta actualmente el sector. Es un actor clave en el desarrollo de la tecnología blockchain, ya que aporta una solución novedosa a los problemas de interoperabilidad y escalabilidad.

Cardano: [55] [56] [57]

Charles Hoskinson, cofundador de Ethereum, creó y supervisó el desarrollo de Cardano, una plataforma pública de cadena de bloques. Debido a que Cardano se basa en la investigación revisada por pares, todos los cambios sugeridos en la cadena de bloques deben pasar primero una evaluación académica antes de ponerse en práctica. Esto ofrece un marco sólido para el desarrollo de la plataforma y garantiza que las decisiones estén respaldadas por hechos sólidos. Aunque también ha hecho que el desarrollo del proyecto esté siendo extremadamente lento haciendo que sus seguidores pierdan la paciencia.

El algoritmo de consenso Ouroboros de prueba de participación es la que usa la cadena de bloques de Cardano. El token nativo de la blockchain de Cardano se llama ADA. En Ouroboros, el tiempo se divide en epochs y slots, cada una de las cuales tiene una duración determinada. Un epoch se compone de slots. Las partes interesadas con intereses en la red Cardano se eligen líderes de los slots. La cadena de bloques de Cardano se amplía con bloques creados por estos líderes.

El diseño de Cardano también se distingue en que separa la razón por la que ocurre las transacciones moviendo esta información a otro "libro de cuentas". Esta división se lleva a cabo mediante una arquitectura de dos capas formada por una Capa de Computación de Cardano (CCL) y una Capa de Liquidación de Cardano (CSL). Mientras que la CCL contiene la lógica de computación y contratos inteligentes, la CSL sirve como unidad de cuenta. Esta arquitectura en capas facilita las actualizaciones y aumenta la flexibilidad.

La escalabilidad, la interoperabilidad y la sostenibilidad son algunas de las ventajas de Cardano. Cardano tiene un diseño distintivo que permite un mecanismo de consenso rápido y eficaz, lo que permite procesar un gran número de transacciones. Con la intención de tender un puente entre las criptomonedas y las finanzas convencionales, también está diseñado para poder interactuar con otras cadenas de bloques y sistemas financieros tradicionales.

Además, Cardano cuenta con una estructura de tesorería centrada en la sostenibilidad. Cada cargo por transacción incluye un porcentaje que se transfiere a la Tesorería, que proporciona dinero para la expansión y mejora del sistema en el futuro. Este hecho es novedoso y hace que el proyecto tenga capital invertible en mejorar la red.

Sin embargo, Cardano también tiene varios defectos. El retraso en el desarrollo de Cardano es una de sus principales quejas. Las actualizaciones y mejoras pueden tardar en implementarse porque cada cambio debe pasar por un exhaustivo proceso de revisión por pares. Además, la función de contrato inteligente de Cardano se introdujo recientemente lo que supone un retraso con

respecto a otras plataformas como Ethereum y Binance Smart Chain, que ya han creado ecosistemas en torno a sus contratos inteligentes teniendo un ecosistema ya planteado y una base de usuarios en ella.

La naturaleza algo centralizada del desarrollo de la red es otro posible defecto a tener en cuenta. Las tres organizaciones que apoyan a Cardano (la Fundación Cardano, IOHK y Emurgo) son independientes, pero están interconectadas e influyen en el progreso del proyecto.

El proyecto tiene un alto obstáculo de entrada para los desarrolladores y colaboradores que no están acostumbrados a este tipo de metodología rigurosa y académica, y esto es también una desventaja. A pesar de que el enfoque científico de Cardano y su fuerte dependencia de la investigación académica le proporcionan una base sólida. Esto podría impedir el avance y disuadir la participación de la comunidad.

Solana: [58] [59]

Solana es una plataforma blockchain de alto rendimiento, ya que según las capacidades técnicas explicadas en su white paper, está llamada a ser el centro del panorama descentralizado. Fue creada por el antiguo ingeniero de Qualcomm, Anatoly Yakovenko y la Fundación Solana. El principal objetivo de Solana es hacer que la infraestructura blockchain sea rápida, segura, escalable y que esté disponible desde cualquier parte del mundo. Se ha conocido a este proyecto desde su popularización como “Ethereum killer” por sus intenciones de mejorarlo en todos los parámetros.

El distintivo algoritmo de consenso prueba de historia (PoH) de Solana es una de sus características técnicas más importantes y diferenciales. PoH es un reloj descentralizado que aumenta la escalabilidad y seguridad de la red. Al recopilar un historial de todas las transacciones, el sistema puede mantener un seguimiento del flujo cronológico de la red y del paso del tiempo. Los sistemas tradicionales de blockchain, que suelen tener problemas relacionados con el tiempo, cambian significativamente con esta innovación tecnológica.

Solana emplea una técnica de consenso prueba de participación además de prueba de historia. El número de tokens que los validadores tienen y están dispuestos a bloquear como garantía determina qué nodos son elegidos para añadir nuevas transacciones a la blockchain y participar en el funcionamiento de la red a través del método de consenso. Solana puede procesar transacciones fácil y rápidamente gracias a la integración de PoH y PoS.

En la arquitectura de Solana también se utilizan otros elementos de vanguardia. Por ejemplo, utiliza una estructura de datos de función de retardo

verificada, que ayuda a mantener y mejorar la seguridad de la red. Además, aplica un método de procesamiento paralelo del diseño contemporáneo de CPU denominado pipelining para aumentar la velocidad y la eficacia de las transacciones aumentando enormemente las transacciones por segundo gracias a esto.

La velocidad y escalabilidad de Solana son dos de sus ventajas. Es una de las redes blockchain más rápidas del momento y puede procesar miles de transacciones por segundo. Por ello, es una plataforma atractiva para los desarrolladores que desean crear aplicaciones descentralizadas de alto rendimiento frente a otras redes menos rápidas y escalables como es Ethereum.

Sin embargo, Solana no está exenta de defectos. Un problema potencial es que, en contraste con otros procesos más probados como prueba de trabajo o PoS convencional, su modelo de seguridad basado principalmente en el mecanismo de consenso PoH, no ha sido probado antes, ni Solana tiene el suficiente recorrido para tener una respuesta clara. Como resultado, Solana puede ser más susceptible a ataques específicos o cortes de red por el desconocimiento de la innovación.

Otro posible inconveniente es que Solana puede dar prioridad a la velocidad y la escalabilidad frente a la descentralización. Solana exige hardware de gama alta a los validadores para alcanzar su alto rendimiento, lo que puede dar lugar a una concentración de poder entre unos pocos validadores selectos que tengan este hardware. Esto con un gran crecimiento de la red puede ser un problema si solo los equipos con un alto grado de capacidad computacional los tienen una minoría, ya que harían menos diverso y descentralizados a los nodos, y por ende a la blockchain.

Polygon: [60] [61] [62]

Una opción de escalado de capa 2 para Ethereum es Polygon, a veces también conocida como Matic Network, ya que el proyecto nació con ese nombre. El valor que aporta esta cadena es que utiliza sidechains, estas son blockchains que coexisten con la cadena principal de Ethereum, pretendiendo ofrecer transacciones más rápidas y menos costosas en la red Ethereum. Los tokens de Ethereum pueden depositarse en un contrato inteligente de Polygon, utilizarse dentro de Polygon y, a continuación, retirarse de nuevo a la cadena principal de Ethereum sin ningún problema. El marco de Polygon también permite el desarrollo de cadenas independientes que interactúan con Ethereum.

Para su seguridad, Polygon utiliza un método conocido como prueba de participación. Al utilizar menos energía computacional que en usando PoW,

hace que tenga un tiempo de bloque más rápido, y por tanto transacciones más rápidas para Polygon.

La escalabilidad es una de las ventajas diferenciales de Polygon. Esta red puede procesar transacciones de forma más rápida y barata descargándolas de la cadena principal de Ethereum a las cadenas secundarias de capa 2. Esto es especialmente útil para dApps que necesitan un alto rendimiento de transacciones y que en Ethereum no las pueden satisfacer.

Su seguridad es otra gran ventaja. El algoritmo de consenso PoS garantiza que los validadores deshonestos sean penalizados con la retirada de sus tokens inmovilizados. Además, las cadenas laterales de Polygon heredan la seguridad del sistema de consenso de Ethereum porque están protegidas por la cadena principal de Ethereum heredando todas sus ventajas.

Además, Polygon es compatible con Ethereum. Esto indica que las dApps creadas en Ethereum pueden transferirse a Polygon sin requerir ninguna modificación de programación. Esto facilita a los programadores beneficiarse de la escalabilidad de Polygon sin dejar de disfrutar de la seguridad y descentralización de Ethereum. También ayuda al desarrollo de ambas blockchains, ya que como desarrollador, con el mismo esfuerzo tendrías presencia en dos blockchains muy grandes.

La dependencia de la red Ethereum para la seguridad es posiblemente el mayor defecto que tiene la red. La seguridad de las cadenas laterales de Polygon podría verse afectada si la red Ethereum se volviera insegura. Sin embargo, teniendo en cuenta la fortaleza de la seguridad de Ethereum, se trata de un escenario altamente improbable y difícil que ocurra.

Avalanche: [63] [64] [65] [66] [67] [68]

Una innovadora plataforma blockchain es Avalanche, que busca ofrecer un ecosistema altamente escalable, rápido y seguro para aplicaciones descentralizadas y criptoactivos. Fue creada por Ava Labs, una empresa propiedad de la destacada personalidad de blockchain Emin Gün Sirer.

El sistema de consenso utilizado por Avalanche combina los modelos de consenso tradicionales con el modelo de consenso Nakamoto, que es el empleado por Bitcoin, haciendo de este método de consenso algo muy novedoso y disruptivo. El consenso Avalanche es el nombre de este peculiar protocolo. Se trata de un protocolo sin líder, bizantino y tolerante a fallos, por lo que incluso si algunos nodos funcionan mal o se comportan de forma maliciosa, puede seguir funcionando correctamente. El protocolo se basa en la votación por submuestreo recurrente, en la que los nodos preguntan a otros nodos al azar

qué opinan de una transacción concreta. Este procedimiento continúa hasta que un número predeterminado de nodos coincide en que la transacción es auténtica, momento en el que se da por concluida, aceptada y se crea el nuevo bloque.

La escalabilidad es una de las principales ventajas de Avalanche. Promete ser capaz de procesar más de 4.500 transacciones por segundo en su white paper, lo que supone un aumento sustancial respecto a los 15 TPS de Ethereum y los 7 TPS de Bitcoin. Avalanche es una buena opción para crear productos financieros escalables y dApps debido a su alto rendimiento dando velocidades mucho más competitivas.

Su latencia mínima es otra ventaja diferencial. El tiempo de finalización de transacción de Avalanche es sustancialmente más rápido que el blockchains mucho más establecidas, tardando sólo 1-2 segundos. Esto convierte a Avalanche en una plataforma adecuada para casos de uso que requieren una rápida finalización de las transacciones, como los juegos en tiempo real y los intercambios descentralizados (DEX) y haciendo esto que sea más atractiva para usuarios nuevos acostumbrados a transacciones rápidas.

La máquina virtual Ethereum (EVM) es una de las diversas máquinas virtuales que admite Avalanche. Esto hace que sea sencillo para los desarrolladores de Ethereum migrar sus dApps a Avalanche porque los desarrolladores pueden implementar contratos inteligentes con Solidity (que es el mismo lenguaje utilizado para los contratos inteligentes de Ethereum) en Avalanche, este rasgo hace mucho más interesante la blockchain para sus desarrolladores, ya que con menor esfuerzo podrían tener presencia en numerosas redes.

Sin embargo, Avalanche tiene varios defectos potenciales. Uno de ellos es su dependencia del token AVAX para la seguridad. Para participar en el procedimiento de consenso, los nodos de la red Avalanche deben bloquear monedas AVAX. Si el coste de AVAX se reduce drásticamente, será menos costoso atacar la red, lo que podría poner en peligro su seguridad, pero este es un riesgo que tiene todas las redes con consenso de tipo de prueba de participación.

En Avalanche, las subnets, también conocidas como subredes, son un conjunto dinámico de validadores que colaboran para llegar a un consenso sobre el estado de un conjunto de blockchains. Una subnet es necesaria para validar cada blockchain. Una subnet puede validar múltiples blockchains, y un nodo puede ser parte de múltiples subnets. La aparición de las subredes es una gran innovación de este proyecto, ya que ha traído con ella un nuevo paradigma de interoperabilidad y procesamiento de transacciones

La cadena X-Chain, la cadena P-Chain y la cadena C-Chain son las tres blockchains que componen Avalanche. La Red Primaria valida y protege las tres

blockchains. La Red Primaria es una subnet especial y, al bloquear al menos 2,000 AVAX, todos los miembros de todas las subnets personalizadas también deben ser miembros de la Red Primaria. Además, se pueden crear subnets diferentes a estas dentro de Avalanche, creando una blockchain propia que tenga una alta interoperabilidad con el resto de la red. Esto sería algo similar a lo que ocurre con Cosmos.

2.1.4 El trilema de la Blockchain

Las tres características más fundamentales de una cadena de bloques son la descentralización, la seguridad y la escalabilidad. Vitalik Buterin, cofundador de Ethereum, fue el que creo el concepto del trilema de la Blockchain para poder describir las ventajas y desventajas inherentes cuando se intentan conseguir estas características en una red. Lo que defiende el concepto del trilema es que es imposible maximizar simultáneamente las tres cualidades, siempre habrá una que falle en beneficio de las otras dos. [69][70][71][72]

La descentralización es el proceso de distribuir el control a una red de forma que ninguna entidad tenga acceso exclusivo y único a él. La seguridad es la capacidad de la red para resistir intrusiones y seguir funcionando con normalidad, aunque algunos usuarios se comporten mal o intenten atacarlos, la intención principal de una red es que no varie el funcionamiento esperado de esta pese a los intentos de usuario mal intencionados. La escalabilidad es la capacidad de la red para gestionar un volumen creciente de transacciones y usuarios, y su capacidad de crecimiento para adaptarse a ese desarrollo fruto de la actividad que haya en la red.

Estas tres cualidades están naturalmente en oposición entre sí, y es lo que termina conduciendo al trilema. Por ejemplo, la escalabilidad suele resentirse a medida que aumenta la descentralización, ya que cada nodo de una red descentralizada debe procesar cada transacción, lo que puede ralentizar la red a medida que se expande la red. Del mismo modo, el aumento de la escalabilidad a menudo exige sacrificar la seguridad o la descentralización para que se pueda hacer efectiva.

El trilema de la blockchain se ha abordado con distintas propuestas para tratar de minimizarlo, si aún no se puede solucionar. Las soluciones de capa 1 y capa 2 son dos categorías principales que se aplican y con las que a día de hoy se está logrando minimizar esta problemática.

Las soluciones de capa 1 requieren modificaciones en el propio protocolo de la red. Un ejemplo es el mecanismo de fragmentación que se utiliza en Ethereum 2.0, el cual divide la cadena de bloques en secciones más pequeñas, o fragmentos, cada uno de los cuales puede procesar transacciones y contratos inteligentes de forma independiente. Esto ayuda a aumentar la escalabilidad al permitir el procesamiento simultáneo de más transacciones, y logra mantener la descentralización y la seguridad.

Por otro lado, las soluciones de capa 2 se construyen sobre la tecnología de cadena de bloques de una red, pero siendo esta capa otra blockchain diferenciada. Pretenden aumentar la escalabilidad eliminando parte del trabajo

computacional de la cadena de bloques principal. Los canales estatales, las cadenas laterales y los rollups son algunos ejemplos de soluciones de capa 2.

Los canales de estado son redes privadas que sólo utilizan la cadena de bloques para abrir y detener los canales. Esto permite que muchas transacciones se realicen fuera de la cadena y no sobre carguen la cadena principal. Las cadenas laterales son cadenas de bloques independientes que funcionan conjuntamente con la cadena principal en paralelo. Cuando los cálculos se realizan fuera de la cadena y sólo se comunican los resultados en la cadena son lo que se conoce como rollups.

Sin embargo, cada uno de estos métodos presenta ventajas y desventajas. La fragmentación, por ejemplo, puede complicar el protocolo y causar problemas con la comunicación entre fragmentaciones. Las soluciones de capa 2, aunque son de las soluciones más prometedoras, también conllevan su propio conjunto de dificultades, como la dificultad de que los usuarios confíen en los administradores del sistema de capa 2 lo suficiente como para usarla.

Para finalizar y a modo de resumen, el trilema de la cadena de bloques es una dificultad crucial en la creación de sistemas de cadena de bloques. Aunque se han propuesto muchas otras soluciones, cada una tiene su propio conjunto de compromisos. Encontrar un equilibrio entre descentralización, seguridad y escalabilidad es el objetivo de la investigación y el desarrollo continuos.

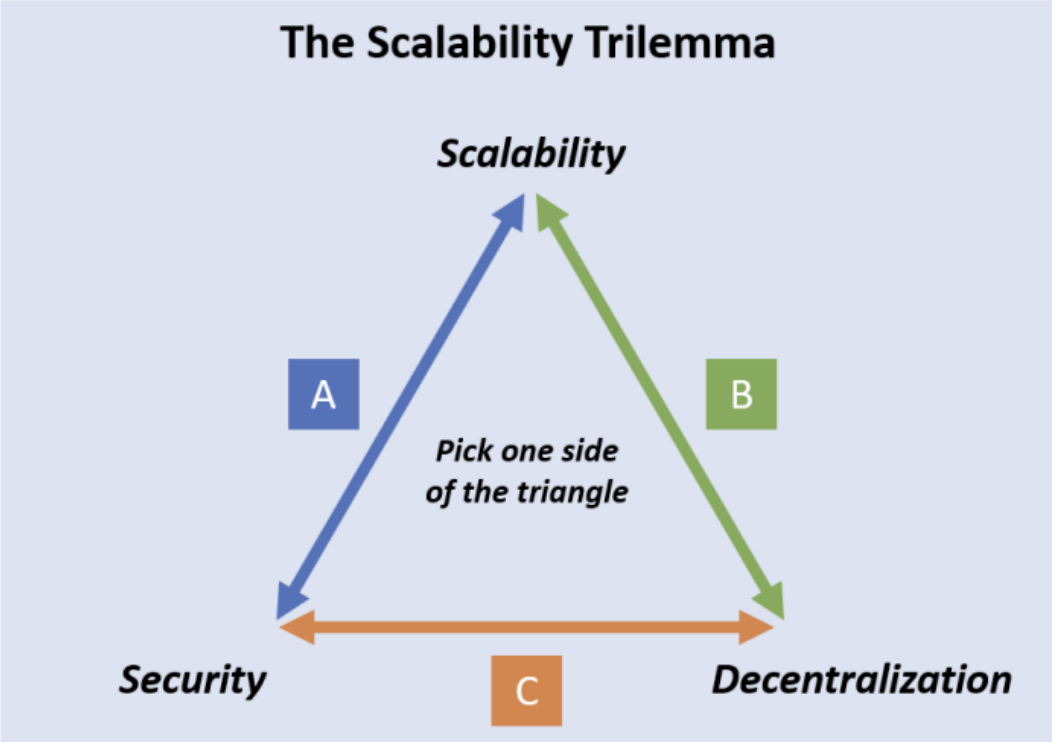

Figura 13. Esquema simplificado del Trilema cripto [169]

Este esquema define perfectamente la limitación. En el podemos ver en cada esquina del triángulo las tres partes del trilema, y el problema viene ya que solo se podría tener un lado en la blockchain, descuidando la esquina opuesta. Y es el trabajo de todos los desarrolladores, lograr encontrar una fórmula para que se cumplan el triángulo entero.

2.1.5 Análisis de descentralización, escalabilidad y seguridad de Blockchains

Un breve resumen a modo de introducción de que significan las tres patas del trilema cripto podría ser:

- La escalabilidad es la capacidad de un sistema para manejar un volumen creciente de trabajo o la capacidad de crecer para manejar esa expansión. En el contexto de blockchain, alude a la capacidad de la red para procesar transacciones con rapidez a medida que la red se expande y crece en número de transacciones y de usuarios.
- La seguridad es la capacidad de un sistema para resistir fallos y ataques y si se perpetraran, a poder recuperarse. En el contexto de la cadena de bloques, alude a la capacidad de la red para evitar intrusiones y mantener la exactitud y accesibilidad de los datos.
- La descentralización describe la división de tareas, autoridades, recursos u otras cosas lejos de autoridad centralizada. En el contexto de blockchain, alude a la uniformidad con la que los individuos tienen acceso a los recursos de la red y quien gobierna sobre ellos.

Escalabilidad [70][72][73][74][75][76][77]

En el contexto de la tecnología blockchain, la escalabilidad se refiere a la capacidad de una cadena de bloques para gestionar un volumen creciente de trabajo o para crecer en tamaño para soportar esa expansión. A medida que aumenta el volumen de transacciones de una red de cadenas de bloques, esto resulta cada vez más crucial. Incluso cuando la red se expande, una cadena de bloques escalable puede ejecutar transacciones con rapidez y eficacia. Y ese es el punto clave de esta parte del trilema, que existan blockchains que, pese a su crecimiento, no baje la velocidad de las transacciones.

Las restricciones inherentes a la arquitectura de muchos sistemas blockchain dan lugar al requisito de escalabilidad en blockchain. El número de transacciones que pueden gestionarse por segundo está limitado por el tamaño de cada bloque en la cadena de bloques de Bitcoin, por ejemplo, que se actualiza aproximadamente cada 10 minutos. Debido a este diseño, la red Bitcoin tiene dificultades para procesar rápidamente un gran número de transacciones, lo que se traduce en tiempos de transacción más largos y comisiones de transacción más elevadas.

La escalabilidad de los sistemas blockchain puede mejorarse de varias maneras. La fragmentación, un método que divide la cadena de bloques en secciones más pequeñas, o fragmentos, cada una capaz de procesar

transacciones por sí misma, es una de las más prometedoras. La capacidad de ampliación de la red puede aumentar considerablemente gracias a la posibilidad de ejecutar transacciones simultáneamente en numerosos fragmentos. Sin embargo, la fragmentación también crea nuevos problemas de seguridad, ya que cada fragmento tiene menos nodos y, por tanto, podría ser más susceptible de sufrir ataques. Como vemos al mejorar una parte se empeora otra sin querer, en este caso mejorando enormemente la escalabilidad, sufre la seguridad.

Otra opción es utilizar transacciones fuera de la cadena, en las que las transacciones se gestionan fuera de la cadena de bloques principal y sólo se registra allí el estado final. Como las transacciones fuera de la cadena pueden gestionarse más rápidamente y con menos recursos que las transacciones en la cadena, esto puede aumentar enormemente la escalabilidad. Las transacciones fuera de la cadena dependen con frecuencia de partes externas fiables, lo que plantea importantes retos de seguridad y descentralización.

Los sistemas de transacciones fuera de la cadena incluyen soluciones de capa 2 como la red Lightning para Bitcoin y la red Arbitrum para Ethereum. Estas soluciones proporcionan una segunda capa sobre la cadena de bloques actual que permite realizar transacciones rápidas y económicas, preservando al mismo tiempo la integridad de la cadena de bloques original.

Un grandísimo ejemplo de escalabilidad es Solana, una cadena de bloques de alto rendimiento que logra una gran escalabilidad utilizando un sistema de marca de tiempo de prueba de historia (PoH) con un método de consenso PoS. Solana, una de las cadenas de bloques más rápidas en uso, promete ser capaz de procesar miles de transacciones por segundo en su white paper y hasta ahora cuando ha tenido más cantidad de usuarios, no se ha congestionado la res.

A pesar de que la escalabilidad sigue siendo un problema importante para la tecnología blockchain, se están creando muchas soluciones para tratar de resolverlo. La decisión entre estas opciones depende de las necesidades únicas de cada red blockchain e implica compromisos en términos de seguridad, descentralización y complejidad, ya que como vemos escapar al trilema es algo casi imposible. Se prevén futuros avances en la escalabilidad de los sistemas blockchain mientras se siga avanzando en este campo de estudio y desarrollo y sigan apareciendo blockchains con propuestas interesantes.

Seguridad [77][78][80][81][82][83]

La integridad de los datos, la estabilidad del sistema y la resistencia a ataques malintencionados son sólo algunas de las muchas partes que tiene la seguridad en la tecnología blockchain. La seguridad de un sistema de cadena de bloques es esencial para mantener la confianza de los usuarios y garantizar

el rendimiento fiable del sistema, sino existe no se podría atraer capital a la red ya que ningún usuario confiaría su capital.

El uso de hashes criptográficos para conectar bloques en una cadena es uno de los principales elementos de seguridad de la tecnología blockchain. Como resultado, modificar transacciones anteriores implicaría cambiar también todos los bloques siguientes, lo que sería computacionalmente imposible y consumiría una cantidad excesiva de recursos de procesamiento lo que hace de escudo protector frente a ataques. La integridad de los datos conservados en la cadena de bloques está garantizada por esta funcionalidad y si se quisiera realizar este ataque habría también que poseer una mayoría suficiente de nodos para poder editar la red. Y este es el principal rasgo que protege la blockchain

Sin embargo, las tecnologías de cadena de bloques no son inmunes a los riesgos de seguridad. El ataque del 51%, en el que una entidad se hace con el control de más de la mitad de la potencia minera de la red y puede alterar el mecanismo de consenso de la blockchain, es uno de los riesgos más conocidos. De este modo, el atacante podría duplicar el gasto de dinero o impedir que otros mineros extraigan nuevos bloques. Aunque con un tamaño significativo lograr acaparar el 51% del poder de voto es algo donde se necesita una inversión de capital muy alta.

Las vulnerabilidades en los contratos inteligentes son otro problema de seguridad. Si el código del contrato inteligente tiene errores o debilidades, estos podrían ser utilizados por los atacantes para robar dinero o causar otros resultados no deseados. Por lo que es importante fijarse también en la calidad del código del contrato inteligente y no solo en el de la blockchain. Porque, aunque una blockchain sea muy segura, si el código tiene vulnerabilidades hará que pueda ser hackeado.

Para aumentar la seguridad de los sistemas blockchain, se han propuesto varias ideas. La utilización de métodos de consenso más sofisticados, como la prueba de participación, puede ayudar a reducir el riesgo de asaltos al 51% al hacerlos más costosos de ejecutar. El uso de técnicas de programación mejoradas, técnicas de verificación formal y auditorías de seguridad automatizadas son otras estrategias para mejorar la seguridad tanto de la blockchain como de los contratos inteligentes.

Otra opción interesante para aumentar la seguridad de la cadena de bloques es la cadena de bloques con seguridad cuántica. Las técnicas criptográficas tradicionales empleadas en la tecnología blockchain pueden volverse inseguras con el auge de la computación cuántica. La distribución cuántica de claves se puede utilizar en la tecnología de cadena de bloques para aumentar la resistencia de la cadena de bloques a los ataques cuánticos.

Es crucial recordar que la seguridad en las cadenas de bloques es una cuestión difícil que requiere una estrategia global. Es importante garantizar la

seguridad de todo el ecosistema, incluidos los contratos inteligentes, los monederos y los intercambios, además del propio protocolo de la cadena de bloques.

Descentralización [76][79][80][84][85]

Uno de los principios rectores de la tecnología blockchain es la descentralización. Alude a la división de funciones, autoridad, personal o recursos lejos de un lugar o autoridad centralizados.

La descentralización de blockchain tiene varias ventajas. Al repartir el libro de cuentas entre varios nodos, mejora la seguridad al hacer más difícil que una entidad modifique los datos, ya que debería tener acceso a todos los nodos. Como todas las transacciones son públicamente verificables e inmutables una vez que se introducen en la cadena de bloques, también fomenta la transparencia y la confianza. La descentralización también puede mejorar la privacidad y la resistencia a la censura porque no hay una única entidad encargada de regular o limitar las transacciones, porque frenarlas o filtrarlas es algo imposible.

La descentralización en blockchain, sin embargo, no está exenta de dificultades. El equilibrio entre escalabilidad y descentralización es uno de los principales problemas, que sobre todo es difícil de corregir a la vez al tener una relación contraria. La escalabilidad de la red se puede ver limitada porque los recursos necesarios para mantenerlo y sincronizarlo crecen igual que la base de usuarios de la red, haciendo que sea mucho más lento la generación de una transacción.

Para mejorar la descentralización de los sistemas blockchain, se han propuesto varias ideas. Utilizar técnicas de consenso como prueba de participación, que fomentan una asignación de poder de una forma más equitativa, es una estrategia que se está usando mucho ahora. La fragmentación es una estrategia diferente que incluye la división de la cadena de bloques en fragmentos más pequeños, con la posibilidad de que cada uno realice transacciones por su cuenta. Esto puede hacer que la red sea mucho más escalable sin afectar a su descentralización, pero si a la seguridad.

Es capital recordar que la descentralización es un continuo y no una cualidad binaria. Dependiendo de cómo se hayan construido e implementado, las distintas cadenas de bloques pueden alcanzar distintos niveles de descentralización. La descentralización es también un medio para alcanzar otros fines, como la seguridad, la transparencia y la resistencia a la censura. No es un fin en sí misma.

La descentralización es un aspecto fundamental de la tecnología blockchain, pero aplicarla en la práctica exige enfrentarse a un número de

difíciles compensaciones y dificultades. La exploración de nuevos enfoques para mejorar la descentralización de los sistemas de cadena de bloques, atendiendo al mismo tiempo a sus requisitos de escalabilidad y seguridad, requiere una labor continua de investigación y desarrollo que a día de hoy se está dando dentro de la comunidad.

2.2 Metodología

Este es uno de los puntos clave del trabajo, ya que es donde explicaré la metodología que voy a usar para realizar las comparaciones y el estudio de las distintas blockchains. La intención de este punto es presentar los parámetros y la forma de estudio que se seguirá en el siguiente tema del proyecto.

2.2.1 Selección de Blockchains a analizar

Mi intención en este punto es seleccionar las redes que se van a estudiar. Es importante señalar que he elegido redes con un volumen de transacciones y un tamaño grande. Ya que es la mejor forma de probar las propuestas hechas en el white paper de cada proyecto. También es importante elegir redes diferentes para poder conocer distintos tipos de consenso, tamaño de bloque… y cómo funcionan realmente y compararlos. [86]

- Avalanche
  Esta red se ha convertido en uno de los proyectos referente. Además de ser una de las redes con mayor capital bloqueado, superando los 700 millones. También el número de protocolos que hay en la red lo colocan en el top de las blockchains.

Figura 14. Gráfica de TVL en Avalanche [89]

Como podemos ver en la figura anterior, el capital bloqueado en la red es muy alto, aunque desde la fuerte caída de mayo del 2022 no logró recuperar esos datos. Se puede ver como se ha mantenido tras la caída en la franja de los 700-800 millones de dólares. El hecho de que llegara hasta los 11 mil millones de dólares permite ver la importancia que tuvo dentro del sector, llegando a ser la segunda red más utilizada por detrás de Ethereum [87]. Viendo estos datos es innegable la importancia que tiene y ha tenido esta red y es un punto a favor para que sea estudiada.

Su propuesta de ser una "plataforma de plataformas" donde avalanche permitiría la aparición de subredes que nacen de ella es una propuesta diferencial, de la que más tarde otras redes se han querido adueñar. Y por último su novedosa propuesta de prueba de participación donde mezcla el consenso de Nakamoto con el consenso clásico, dando lugar a un sistema de consenso único.

Las variables de la red importantes previas al estudio:

- Consenso: Prueba de participación (PoS)
- Tiempo de bloques: < 3 segundos
- Velocidad: 4.500 Transacciones por segundo (TPS)
- Nodos validadores: +500

- Cardano

  Cardano llegó a ser la tercera blockchain por capitalización de mercado, como ya comenté antes, creada por un ex creador de Ethereum, nació para ser la red de contratos inteligentes de referencia. Nació para desbancar a Ethereum siendo su antagonista principalmente en metodología de implementación. Mientras Ethereum implementa actualizaciones "rápido", Cardano procesa, testea y analiza hasta el más mínimo detalle antes de lanzarlo a la mainnet. Esto hace que Cardano se diferencie enormemente y la creadora de avances y tendencias en su sector.

  También es una de las redes principales que más cambios y pruebas recibe en su GitHub, prueba de que hay mucho trabajo detrás de esta blockchain [88].

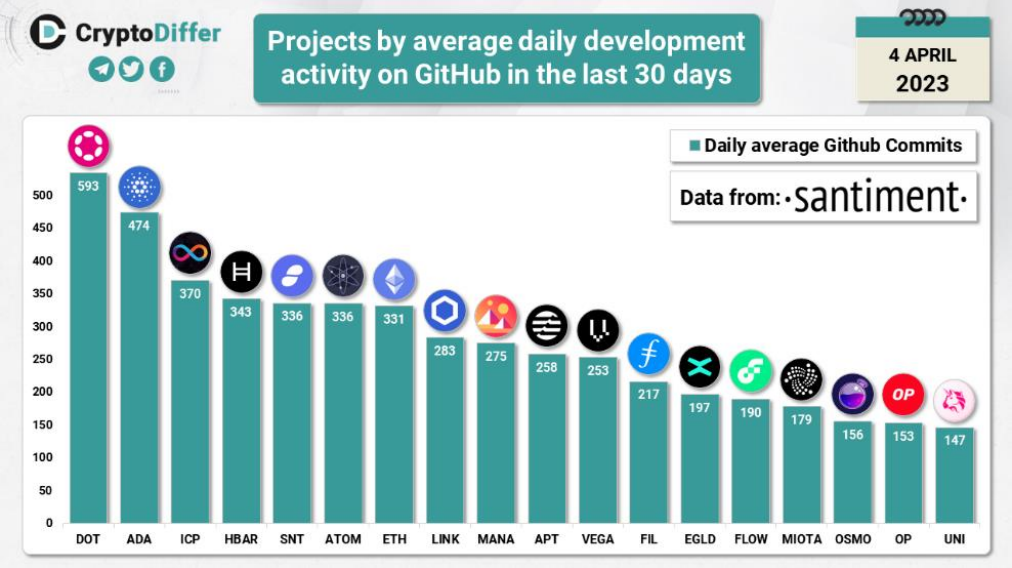

Figura 15. Gráfica con los commit en GitHub de los proyectos Blockchain en el último mes [171]

Esta gráfica es la más reciente, donde se ven el desarrollo diario de las blockchains, si viene este último mes fue la segunda, suele estar en el top tres siendo normalmente la primera. Esto hace que sea interesante estudiar una blockchain que recibe tantísimo desarrollo en el paso del tiempo, porque es lógico pensar que será una de la mejores, y por eso merece la pena compararla con otras.

Figura 16. Gráfica de todo los commit en el último año [170]

Y esta sería la gráfica de todos los cambios en el GitHub a lo largo del año, donde podemos ver que Cardano es la que más actividad tiene, y por ende más desarrollo hay detrás de ella.

Figura 17. Gráfica de TVL de Cardano [89]

Si vemos la gráfica el valor bloqueado subió enormemente, cayó en mayo del 2022 como todo el sector, desde 2023 ha ido recuperándose. Pero aun así los datos de valor bloqueado en la red son muy bajos, en comparación a proyectos tan famosos e importantes. Por lo que estudiarla puede darnos las razones de porque siendo una blockchain con tanto desarrollo detrás, no logra atraer capital de los usuarios.

Esta red fue una de las primeras en usar el PoS como método de consenso, habiendo publicado numerosos paper sobre ello. También es importante remarcar que nace con la intención de ser un producto novedoso, muy enfocado como dije en los contratos inteligentes, lo que lo haría una gran red para la DeFi.

También nace siendo una blockchain de dos capas, lo que deja claro su intención de ser escalable. Por lo que todos estos parámetros la hacen extremadamente interesante para ver si logra solucionar el trilema cripto o al menos se acerca a hacerlo.

Las variables de la red importantes previas al estudio:

- Consenso: (PoS)
- Tiempo de bloques: 20 segundos
- Velocidad: 1000 (TPS)
- Nodos validadores: 2000

- Polkadot

  Polkadot es una de las blockchains con mayor potencial del panorama cripto, su propuesta de ser una blockchain que albergué otras 100 dando ellos la capa de seguridad e interconexión a estas blockchain la hace única. Su creador es el creador de Solidity y cofundador de Ethereum.

  En un resumen, Polkadot es una iniciativa blockchain de vanguardia que enlaza varias blockchains especializadas en una única red. Está protegida mediante un mecanismo de participación por consenso conocido como prueba de participación nominada (NPoS), que permite que la red esté protegida por dos tipos diferentes de actores: validadores y nominadores.

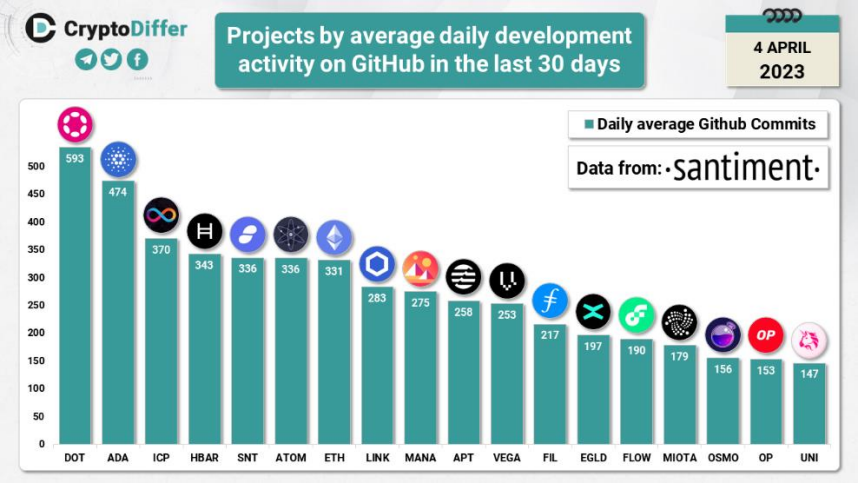

Figura 18. Gráfica con los commit en GitHub de los proyectos Blockchain en el último mes [171]

Recuperando esta imagen de antes, podemos ver que es el primer proyecto con mayor actividad de desarrollo diario en el último mes, y si además se suele mover en el top 3 la mayoría de las veces. Por lo que es un proyecto que no solo destaca por ser novedoso, sino que también lo hace por ser tener un alto grado de desarrollo continuado.

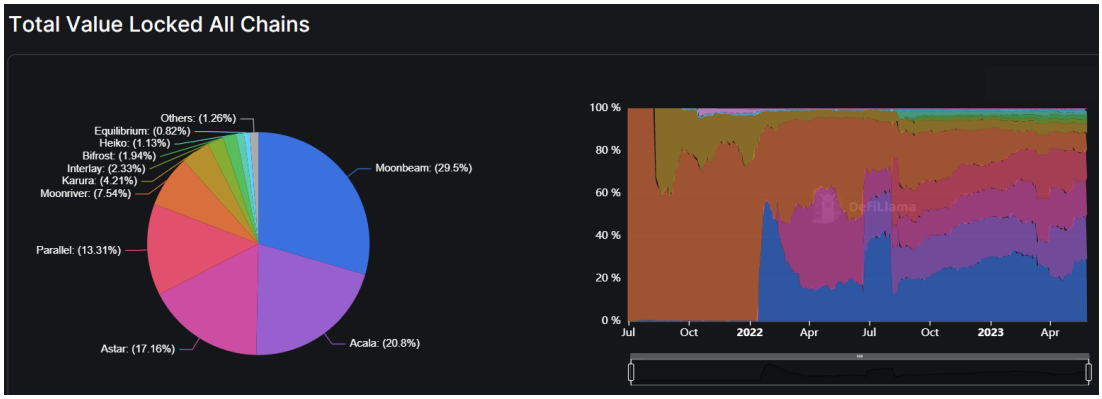

Figura 19. Gráfica de dominancia de las blockchains de Polkadot [89]

Name	Protocols	TVL
1 Moonbeam	49	$46.04m
2 Acala	6	$32.46m
3 Astar	36	$26.78m
4 Parallel	5	$20.77m
5 Moonriver	56	$11.77m
6 Karura	5	$6.564.539
7 Interlay	3	$3.641.292
8 Bifrost	3	$3.035.743
9 Heiko	5	$1.765.838
10 Equilibriun	1	$1.272.815

Figura 20. Tabla de las 14 redes con mayor TVL de Cosmos [89]

A la hora de cuantificar la importancia que tiene esta blockchain según su capital bloqueado (TVL), que es útil para saber su peso en la DeFi, vemos que hay unos datos muy diferentes a las otras blockchains, y esto se debe a que al ser un blockchain que da soporte a otras blockchain, podemos ver el TVL de las blockchains que soporta. Por lo que si sumamos el valor de todas sería un total de más de 154 millones de TVL. Es un dato alto, aunque no estaría entre las blockchains del top 10 de TVL [87]. Esto es algo interesante de estudiar, ya que uno de los proyectos con mayor capitalización de mercado [2], más famosos y mejor

desarrollados, además de ser de los más prometedores, no logra ser una de las blockchains de referencia en cuanto a TVL. También cabe destacar que las subastas de parachains fueron hace relativamente poco por lo que eso ha podido dificultar la entrada de capital.

Figura 21. Gráfica en los commit en GitHub de los proyectos blockchain en el último año [170]

Como vemos en la imagen Polkadot ha sido el 5º proyecto con más actividad en GitHub en el último año, esto es lógico pensar que se ha traducido en un mayor desarrollo, y por tanto hace que Polkadot este en el top 5 de blockchains más desarrolladas en el último año. Estos datos hacen que sea muy interesante estudiar una red que tiene un trabajo tan grande detrás, con un concepto tan nuevo y sobre todo que sea un proyecto tan joven.

Figura 22. Gráfica con el número de desarrolladores activos por blockchain [170]

Por último, es interesante ver que Polkadot es la segunda red con más desarrolladores actualmente, además Kusama es la tercera, que sería la red de pruebas de Polkadot. Este dato es interesantísimo y da más fuerza a la intención de estudiar el funcionamiento de esta red, ya que teniendo un equipo tan grande detrás lo más probable es que tenga un gran funcionamiento o al menos un gran potencial.

Las variables a tener en cuenta de la red:

- Consenso: PoS
- Tiempo de bloques: 6 segundos
- Velocidad: 100k a 1.000.000 TPS
- Nodos validadores:1000

- Polygon

  Polygon vuelve a ser una blockchain peculiar, esto es así porque es una solución de capa 2 para Ethereum. Fue de las primeras blockchains de capa dos que vinieron a solucionar los problemas de escalabilidad de la red de Ethereum. Su propuesta ya la vimos antes, y le ha permitido ser una de la blockchains de referencia en el sector DeFi, llegando a tener más de 418 protocolos confirmados en ella lo que le deja en 3 posición [87]. Esto lo hace muy interesante para su estudio.

Figura 23. Gráfica de TVL en la red de Polygon [89]

Como podemos ver en la gráfica, el TVL ha caído en picado desde junio del 2021, y desde entonces no ha logrado recuperar nada del 90% que ha perdido. Si bien es cierto que se ha estabilizado en la zona de los mil millones de dólares, por lo que esa cantidad de dinero bloqueado en DeFi lo pone en el top 5 de más cantidad de TVL.

Figura 24. Gráfica con el número de usuarios activos por blockchain [170]

En esta gráfica podemos ver la comparativa de blockchains con más usuarios, y polygon sería la segunda de que más tiene. Esto hace que su blockchain tenga una cantidad de usuarios altísima que soportar y donde la seguridad y eficiencia son un factor clave.

Estas razones hacen que sea interesante estudiar una de las L2 de Ethereum más famosas y la primera en usuarios, la cual intenta mejora la escalabilidad, por lo que este punto debería ser su fuerte.

Las variables de la red importantes previas al estudio:

- Consenso: (PoS)
- Tiempo de bloques: 2.3 segundos
- Velocidad: 65,000 (TPS)
- Nodos validadores: 100

- Ethereum

  Es imposible hacer un análisis de blockchains sin pasar por la Ethereum, como ya vimos, Ethereum es el padre de los contratos inteligentes, y es donde nació la DeFi. Ethereum es la segunda criptomoneda con mayor capitalización de mercado [2] y la que mayor TVL tiene [87] además comenzó siendo una blockchain con prueba de trabajo y se pasó a prueba de participación como método de consenso. Todas estas razones la hacen muy interesante de estudiar cual es el desempeño de la blockchain de referencia en el mundo DeFi.

Figura 25. Gráfica de TVL en Ethereum [89]

Como podemos ver la red de Ethereum llego a tener un TVL de casi 120 mil millones de dólares, y tras las fuertes caídas del sector cripto, se ha estabilizado en 27 mil millones. Aunque pueda parecer una gran caída de su valor, siguen siendo más de cinco veces el capital bloqueado de la siguiente blockchain. Acemas tiene cerca de 800 protocolos desarrollados en su red, siendo claramente la que más protocolos tiene [87]

Figura 26. Gráfica con el número de usuarios activos por blockchain [170]

Como podemos ver en esta gráfica, Ethereum es la tercera red, muy cerca de la segunda, con mayor cantidad de usuarios. Por lo que vuelve a ser muy relevante en otra variable clave, que ponen en tela de juicio su seguridad y escalabilidad día a día.

Figura 27. Gráfica con los cambios hechos en el último año en los proyectos blockchain [170]

Otro punto en el que también destaca la red de Ethereum es en el número de cambios en su GitHub, lo que se suele traducir también en una mayor cantidad de desarrollo. Por lo que estos datos posicionan a Ethereum como una da los proyectos cripto con mayor desarrollo del sector y da más razones para ser estudiado.

Figura 28. Gráfica con el número de desarrolladores por blockchain [170]

Por último, siguiendo los datos de esta gráfica, podemos ver que Ethereum es la red con mayor cantidad de desarrolladores, que unido a la gráfica anterior permiten entender mejor el éxito de esta blockchain y porque atraen el capital de sus usuarios.

Las variables de la red importantes previas al estudio:

- Consenso: (PoS)
- Tiempo de bloques: 18.12 segundos
- Velocidad: 100000 (TPS)
- Nodos validadores: 250000

- Bitcoin

  Bitcoin está en la lista a analizar por ser la primera blockchain, la que tiene más capitalización de mercado [2] y la que tiene un mayor grado de descentralización. Aunque a día de hoy no tiene nada de DeFi en ella se están construyendo L2 para poder solucionarlo. Es muy interesante su estudio, para compararlo con blockchains de segunda y tercera generación. También para estudiar el trilema en ella, aunque no es un secreto la mala escalabilidad de bitcoin, razón principal de que no tenga un sector DeFi tan importante como su capitalización de mercado.

Figura 29. Gráfico de TVL bloqueado en Bitcoin [89]

Esta es la gráfica del TVL de Bitcoin, como podemos ver tiene una tendencia creciente, que se puede deber a la aperción de L2 para el pago con Bitcoin, aun así, no ha entrado ni en el top 10 de redes con más capital bloqueado [87], lo que deja mucho que desear para el tamaño de Bitcoin.

Las variables de la red importantes previas al estudio:

- Consenso: (PoW)
- Tiempo de bloques: 10 minutes
- Velocidad: 7 (TPS)
- Nodos validadores: +15000

- Solana

  Esta blockchain nació para desbancar a Ethereum y se centró en corregir los problemas que nadie más daba importancia en las blockchains. Para ello intento crear una infraestructura más global y para que se acercara más al público global. Esta blockchain ha hecho esfuerzos en mejorar los problemas de escalabilidad, velocidad, interoperabilidad mientras intentan mejorar el ecosistema de aplicaciones descentralizadas.

Figura 30. Gráfica del TVL en Solana [89]

Si vemos su gráfica de capital bloqueado, llego a tener unos máximos altísimos, que muy pocas blockchains han lo han logrado, llegando a posicionarse en el top de TVL de redes. Pero con la caída del mercado cripto, esta red ha sido una de las mayores afectadas perdiendo el 98% de su capital bloqueado [87]. Por lo que merece la pena estudiarla, para entender por qué una blockchain nacida para destronar a Ethereum y que intenta solucionar tantos problemas de las redes, ha perdido tanta importancia en la DeFi

Las variables de la red importantes previas al estudio:

- Consenso: PoS y Prueba de Historia
- Tiempo de bloques: menos de un segundo
- Velocidad: 50000 TPS
- Nodos validadores: 200

Es importante remarcar que variables que he puesto al final y he marcado como variables importantes previas al estudio, son datos de las blockchain tras hacer una búsqueda rápida o bien en sus white paper o bien en internet. Esto es para saber que datos esperaba tener la blockchain cuando se creó para ponerlos en contraposición con los datos reales que tiene actualmente. Además, estos datos sirven un poco para hacer una comparativa previa al trabajo de análisis de este proyecto [90].

2.2.2 Métricas de descentralización, escalabilidad y seguridad a evaluar

Para comparar la escalabilidad, seguridad y descentralización de una red pueden utilizarse numerosas variables, dependiendo de en qué nos queramos enfocar usaremos unas u otras, en este caso la intención del proyecto es hacer una comparativa de las blockchains previamente seleccionadas, siempre desde una visión de utilidad para las DeFi. Es por esto por lo que las variables seleccionadas, son suficientemente generales para que se puedan comparar entre otras redes, y a la vez son útiles para cuantificar la importancia de estas redes en la DeFi [78][79][80][83][85]:

- Escalabilidad
    - Velocidad de transacción: es el número máximo de transacciones que la red puede gestionar por segundo. Es un elemento clave para determinar el grado de escalabilidad de una red. Una red será más escalable cuanto más rápido se procesan las transacciones que tiene en cola.
    - Capacidad de la red: Sirve para describir la mayor cantidad de datos que pueden se pueden enviar en un tiempo determinado en la red. Las redes con mayor capacidad son más escalables, ya que en un mismo bloque cabría más información.
    - Latencias: Es el periodo de tiempo que transcurre desde que se envía una transferencia hasta que se ejecuta y se añade a la red finalmente. Una mayor escalabilidad se correlaciona con una menor latencia, por lo que es vital tener redes con latencia baja, para poder tener mejores signos de escalabilidad.

- Seguridad:
    - Estándares de encriptación: La seguridad de una red puede medirse por la potencia del cifrado que se ha empleado para proteger los datos de la red. Lo normal es que un cifrado de bits más alto sea más seguro.
    - Historial de fallos de la seguridad: Dirigirse al historial de fallos de seguridad suele ser un buen indicativo. Por lo general se considera que una red es más segura si han dado menos fallos de seguridad. También esto puede ayudar a ver patrones, por si existiera una vulnerabilidad recurrente o redes más vulnerables.
    - Programas de recompensas por fallos: Las redes con programas de recompensas tratan de incentivar a los hackers éticos a encontrar y notificar fallos de seguridad en sus redes o protocolos, lo que

puede dar lugar a redes más seguras y a minimizar riesgos tras haber encontrado estos fallos.

- Descentralización:
    - Número de nodos: Una red descentralizada se puede medir por su cantidad de nodos, por lo que cuantos más nodos tenga esa red, mayor será el grado de descentralización. Esto es porque al tener más nodos significa que el control sobre la red está más disperso, ya que está repartido entre los distintos nodos.
    - Distribución geográfica de los nodos: Una red está más descentralizada si sus nodos están dispersos por varias regiones o naciones distintas, ya que si no lo están se podrían ver afectadas por regulaciones y verse enormemente restringidas.
    - Mecanismo de consenso: La descentralización también puede verse afectada por el modelo de consenso utilizado. Por ejemplo, con el PoS puede ocurrir que el precio para crear un nodo sea demasiado alto dificultando la creación de nodos y por tanto su descentralización.
    - Gobernanza: La descentralización también se medide por la forma en la que se toman las decisiones dentro de la red. Las blockchains están menos descentralizada si la mayoría de los nodos están en un servidor centralizado.

Estos son los factores usaré para examinar, medir y contrastar la escalabilidad, seguridad y descentralización de una red. Dependiendo de los casos de uso de las redes, pueden dar mayor prioridad a características diferentes.

2.2.3 Herramientas y técnicas utilizadas para el análisis

La escalabilidad, seguridad y descentralización de una red blockchain pueden evaluarse y contrastarse principalmente utilizando aplicaciones y sitios web especializados, normalmente son o herramientas de la propia red o portales de datos para el análisis de los usuarios. La mayoría de los datos se encuentran de esta forma, aunque pueda haber datos y análisis de mayor complejidad que se tengan que hacer manualmente o basándose en otros estudios. A continuación, describiré los distintos tipos de herramientas más popular que existen a modo de ejemplo, para que de esta forma las agrupe, estas no serán las únicas herramientas que usare, porque puede que algunos datos sean más complejos de encontrar, pero los grupos que hare para separar las herramientas si serán principalmente en los que me base:

1. **Exploradores de cadenas de bloques:**

Estos son parecidos a motores de búsqueda, pero siendo específicos a las blockchains. Estas herramientas permiten buscar transacciones, direcciones y otros datos de la red, algunas incluso dan datos para analizar de la propia red. Por ejemplo, para Ethereum existen herramientas como Etherscan[91] o Blockchair[92]. O por ejemplo para podría ser Polygon Polygonscan [94] y para Avalanche sería Avascan[93]. Esto se repetiría en todas las blockchains principales respectivamente.

2. Herramientas específicas de la red:

La mayoría de las redes blockchain, además, tienen también su propio conjunto de herramientas y recursos para poder realizar un seguimiento del rendimiento y la salud de la red, además de poder extraer de estas herramientas datos cruciales sobre las propias redes. Un ejemplo para Ethereum podría ser EthGasStation[96], Para Bitcoin podría ser Bitnodes[95] un buen ejemplo. Y así ocurría con las demás redes.

3. GitHub:

Un indicador de la salud de un proyecto y las perspectivas de futuro puede encontrarse en la frecuencia de las actualizaciones y el número de contribuyentes que hay en el repositorio de su GitHub. También es interesante mirarlo para analizar los white paper y el código abierto para entender mejor el funcionamiento y las limitaciones de las distintas redes. Para acceder a esta información, se puede ir directamente desde la página de GitHub del proyecto.

4. Plataformas analíticas de terceros:

Compañías como "CoinMetrics"[97], " In to the block"[98] y "Messari"[90] ofrecen análisis en profundidad y de muy alta calidad, muchas se pueden permitir estos analizas al tener suscripciones bastante altas. Estas herramientas ayudan a analizar y a adquirir perspectivas sobre muchos aspectos de la mayoría de las redes blockchain.

5. Información sobre validadores o nodos:

Se puede obtener información sobre validadores o nodos de una red normalmente en los propios sitios web de los proyectos, pero también pueden existir herramientas o aplicaciones especializados en estos datos, como es el caso de Staking Rewards[99].

6. Mediante estudios académicos, estudios de terceros o búsqueda manual:

Esta es sin duda la forma más tediosa y difícil, ya que encontrar o lograr datos de esta forma puede necesitar una gran inversión de tiempo. Aun así, en muchas situaciones es la única forma de encontrar datos de calidad, para aquellos casos en que los datos que queremos estudiar son menos comunes y por ende más difíciles de encontrar.

2.3 Desarrollo de la Contribución: Análisis de descentralización, escalabilidad y seguridad

A lo largo de este punto hare un análisis de los datos que ofrecen las distintas blockchains con el propósito de analizar la escalabilidad, la seguridad y la descentralización siguiendo los parámetros explicados en los puntos anteriores y las blockchains que previamente he mencionado y analizado.

2.3.1 Análisis de la escalabilidad de las Blockchains

Estas son las variables que mejor pueden definir la escalabilidad de una red y de los que intentaré encontrar información actualizada para poder hacer una comparativa justa. Estas variables son cuantificables en todas las blockchains, es por esto por lo que las elegí, para una mejor comparación.

Como ya se definió, las variables elegidas para la escalabilidad son:

- Velocidad de transacción
- Capacidad de la red
- Latencia

Siguiendo la lista de redes elegida los datos obtenidos son estos:

- Avalanche
    - Velocidad de transacción: 12.35 AVA TPS [93]. Estos datos distan mucho de las 4500 TPS que anunciaron en el white paper, esto se puede deber a que quizás la red no necesita estar al máximo rendimiento porque no hay suficientes transacciones.

    - Capacidad de la red: Su capacidad de generar subredes le permite tener una capacidad de red ilimitada, lo que significa que no hay un límite real de TPS [100]. Esto justifica los datos anteriores de TPS, y porque se diferencian de lo que aparece en el white paper del proyecto. Avalanche nació para ser una solución de escalabilidad, y sobre todo intenta atacar ese problema con las subnets, esta es la prueba de ello.

    - Latencia: La latencia media es de 7 segundos como resultado de las pruebas [101], también podemos ver que tiene una desviación media de 2 segundos tanto a favor como en contra, estos datos se

separan de la latencia menor o cerca al segundo según el white paper que publicaron y siendo peor.

- Cardano
    - Velocidad de transacción: Está teniendo unas 2.4 AVG TPS [102] en la actualidad, una vez más, dista mucho de las 1000 TPS que prometen en el artículo del ecosistema, pero se debe a que no se tiene la necesidad real de llegar a esos números porque la red no esta tan congestionada y no hay tantas transacciones.

    - Capacidad de la red: para Cardano, la capacidad de red no es algo fijo, si no que depende de factores como el tamaño de bloque, de transacciones o el tiempo de bloque, a día de hoy con la actualización que viene en camino se lograría mejorar enormemente esta posibilidad, ya que crecería el tamaño de bloque y el tiempo de bloque se reduciría [103]. Aun así, actualmente solo se está utilizando el 50% de su capacidad total [104], lo que vuelve a ser un indicativo de que le faltarían usuarios para necesitar llegar a su máximo potencial.

    - Latencia: La latencia de la red es de alrededor 20 segundos [105], esto se debe a que aún no han lanzado su L2 para que pueda mejorar la escalabilidad de la red aún más, pero estos datos son buenos ya que, si la red aún le falta una pieza clave y logra tener tiempos bajos, cuando se le añada va a mejorar enormemente. Pero en comparación a otras redes, actualmente, no es un competidor por la latencia.

- Polkadot
    - Velocidad de transacción: Polkadot está procesando una media de 0,43 transacciones por segundo [92]. Comparado con el pico de 100.000 TPS que se alcanzó en 2022, se trata de un descenso sustancial y unos números muy bajos en comparación a las otras blockchains que estamos estudiando. Polkadot aún está en desarrollo, por lo que es vital tener en cuenta que la capacidad de la red probablemente crecerá en el futuro. Además, la cantidad de parachains que operan actualmente en la red está limitando el TPS y es por eso por lo que se prevé que el TPS aumente cuando se añadan más parachains a la red. El TPS máximo teórico para Polkadot es de 1.000.000 del cual dista mucho, pero si subieran los usuarios y las transacciones, teóricamente podría llegar a esas cotas.

- Capacidad de la red: Polkadot tiene una tasa de uso de red del 0,007% [106]. Esto indica que sólo el 0,007% de la capacidad disponible de la red se está utilizando en este momento, por lo que la capacidad restante de la red sería de 99,993%. Esto se puede deber a numerosos factores, los que contribuyen al bajo consumo de red de Polkadot. En primer lugar, tenemos que la red aún se está desarrollando, por lo que todavía no hay muchas dApps u otras aplicaciones que la utilicen. Por otra parte, Polkadot tiene un tiempo de bloque comparativamente largo, lo que se traduce en una menor demanda de transacciones. Aun así, este dato es extremadamente bueno, ya que significa que podría aguantar la entrada de gran cantidad de usuarios y transacciones nuevos, haciendo a la red más escalable.

- Latencia: La latencia media que tiene la red es de 6 segundos [106] [101], unos datos intermedios en comparación a otras redes competidoras, y que dejan ver que Polkadot puede ser una solución escalable.

- Polygon
  - Velocidad de transacción: 30 AVG TPS [94] son los que tiene actualmente la red. Estos números son muy inferiores a los del white paper, pero esta red si tiene mayor número de transacciones [98] en comparación, aunque quizás no suficientes como para necesitar el máximo de TPS teórico.

  - Capacidad de la red: solo está en uso el 50% [94], lo que significa que hay margen de entrada de usuarios, ya que, si solo está el 50% en uso siendo del top5 con más usuarios ya, la cantidad de usuarios que soportaría es enorme, y esta puede ser una razón por la que aún no se ha llegado al máximo de TPS teórico.

  - Latencia:

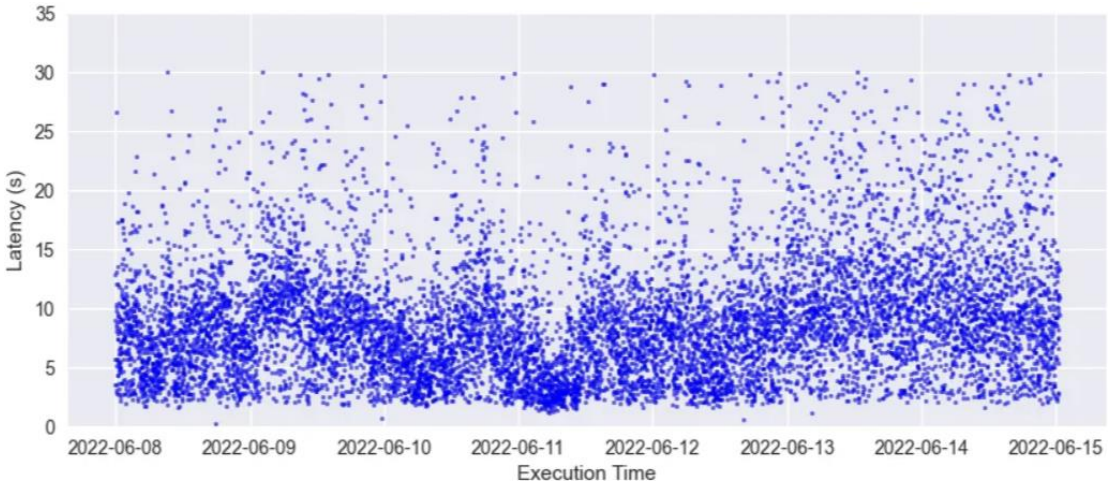

Figura 31. Gráfico con los resultados de tiempo a las pruebas de latencia de la red de Polygon [101]

Como podemos ver en la imagen, la latencia media está cerca de los 10 segundos, una cifra realmente mala en comparación a otras redes, pero llega a tener picos de hasta 30 segundos incluso. Estos datos hacen que la solución de escalabilidad propuesta para Ethereum, aunque le mejora, tiene margen cambio a mejor [101].

- Ethereum
    - Velocidad de transacción: Actualmente tiene un AVG TPS de 30 [107], lo cual es una grandísima mejora de los 10 TPS [107] antes del cambio del método de consenso. Aun así, está lejos de los 100000 TPS que aspira a tener cuando se cumpla el fin de la actualización de ETH 2.0, por lo que debido a la cantidad de usuarios que tiene la red ese 30 se hace un poco bajo y puede servir para explicar porque tardan tanto en ejecutarse las transacciones en la red.

    - Capacidad de la red: A día de hoy se está utilizando un 51% de su capacidad de red [108], por lo que aún queda espacio para que haya más usuarios en ella realizando transacciones. El hecho que tenga estos datos de latencia y de TPS pese a solo estar usando el 51% de su capacidad, no muy favorables. Esto deja claro que Ethereum a día de hoy no es la red más escalable, pese a ser la que tenga más capital retenido en ella.

    - Latencia: La latencia suele estar entre 12 y 24 segundos, este dato es realmente altos en comparación a la nueva generación de blockchain, y por ende algo malo para los usuarios. Esta tardanza

en la confirmación de las transacciones puede justificar que la empresa detrás de Ethereum esté buscando una actualización para así poder ser más competitiva [101][109].

- Bitcoin
    - Velocidad de transacción: Los TPS medios que está teniendo en el momento de redacción son de 4,20 TPS [110], que está por debajo de los 7 TPS que se plantea como la normal de Bitcoin [111]. Por lo que a día de hoy bitcoin está trabajando por debajo de sus TPS esperados y eso que la demanda de la red ha subido recientemente. Además, ya de por sí, 7 TPS es una cifra demasiado baja en comparación a las redes de tercera generación que, si tuvieran esa demanda de la red, según la teoría fácilmente lo superarían.

    - Capacidad de la red: con la llegada de las L2 de Bitcoin lograra mejorar su capacidad de red, actualmente está en 78.16% [112] [110]. Esta se aumenta o disminuye según la cantidad de transacciones que haya en ella. Ver que el 78.16% está siendo utilizado hace pensar que el grado de utilización es alto, y mucho más que otras redes. Esto podría justificar unos números de eficiencia tan bajos, dar a entender las dificultades que pasaría Bitcoin si llegaran más usuarios y por ende la dificultad que tendría para escalar. Pero, aun así, ha tenido números de eficiencia similares con grados de utilización más bajos [113], por lo que no serviría de justificación.

    - Latencia: El tiempo medio para que se ejecute una transacción en Bitcoin es de 10 minutos [114], lo cual es una cifra extremadamente superior al resto de blockchains y deja claro la necesidad tanto de una L2, como que Bitcoin no es muy escalable.

- Solana
    - Velocidad de transacción: Solana actualmente tiene un TPS medio de 4250, que, aunque dista de los 50000 TPS teóricos es la red con mayor cantidad de TPS pese a la bajada de usuarios que sufrió en noviembre del 2021 [89]. Esto deja a Solana como la mejor red en términos de TPS. Lo que significaría que sería la que mejor podría sostener un aumento de los usuarios y de las transacciones en caso de que ocurriera.

- Capacidad de la red: La capacidad de red actual de solana es del 80% [115], esto significa que solo le quedaría el 20% para poder satisfacer una subida en la demanda de transacciones. Si con un nivel tan alto está rindiendo tan bien, esto nos puede dar a entender la alta escalabilidad que tendría Solana.

- Latencia: En cuanto a la latencia si bien se encuentra al medio segundo [116] estas cifras son verdaderamente buenas, ya que la velocidad a la que ejecuta una transacción es altísima en comparación a muchas blockchains.

2.3.2 Análisis de la seguridad de las Blockchains

A lo largo de este punto analizare las variables previamente seleccionadas para el estudio de la seguridad en las blockchains elegidas. Intentaré encontrar los datos de más calidad que puedan dar claridad a la intención del punto, que es estudiar la seguridad de las blockchains elegidas previamente. Tras estudiar esta información podremos entender que blockchains son más o menos seguras y poder elegirlas en función de eso.

Las variables que analizaré y que previamente elegí son estas:

- Estándares de encriptación
- Mecanismo de consenso
- Historial de fallos de la seguridad

Siguiendo la lista de redes elegida anteriormente, a continuación, realizaré el estudio:

- Avalanche
    - Estándares de encriptación: Avalanche utiliza varios estándares de cifrado, entre ellos:
        - Transport Layer Security (TLS): Se trata de un conocido sistema criptográfico que protege las comunicaciones de nodo a nodo contra miradas indiscretas. Usa 128 bits.
        - Secp256k1: Para crear claves públicas y privadas para las direcciones de Avalanche, se emplea este procedimiento de criptografía de curva elíptica. Usa 256 bits.
        - SHA-256: Se trata de un algoritmo criptográfico de hashing que produce hashes de datos de 256 bits.
        - RipeMD-160: Con esta función hash criptográfica se producen hashes de datos de 160 bits. [117]

      Existen 4 tipos de algoritmos para el proceso de encriptado. El número de bits que tiene dicho encriptado en comparación al resto es bastante estándar, siendo el de 128 bits un poco más bajo de lo común, y sobre todo en comparación con sus otros algoritmos de encriptación.

    - Historial de fallos de la seguridad: a lo largo de la existencia de Avalanche, ha habido numerosas vulnerabilidades en la red, pero la mayoría han sido de menor importancia, sin que pudieran poner en tela de juicio para siempre la blockchain. Solo 3 casos han sido realmente graves pudiendo destruir el proyecto [118] pero todas solucionadas por el equipo, y serian estas vulnerabilidades:

        - Febrero del 2021: La vulnerabilidad permitía crear claves privadas para generar validadores, pudo destruir el sistema de consenso de la red.
        - Marzo del 2021: Un fallo en el puente Ethereum-Avalanche que pudo desvirtuar la entrada de capital en la red y robar todos los fondos.
        - Septiembre del 2022: Los contratos precompilados de Avalanche contenían una grave vulnerabilidad que fue descubierta por una empresa de seguridad llamada Statemind. Debido a este fallo, alguien podría haber utilizado aplicaciones DeFi y haber robado dinero.
    - Programas de recompensas por fallos: Si tiene un sistema de recompensas por encontrar bugs en el código [119] lo que habla muy bien de la red.

- Cardano
    - Estándares de encriptación: Cardano utiliza estos estándares de cifrado, entre ellos:
        - Transport Layer Security (TLS): Este es un conocido sistema criptográfico que protege las comunicaciones entre nodo y nodo contra miradas indiscretas. Usa 128 bits.
        - Secp256k1: Se usa para crear claves públicas y privadas para las direcciones de Cardano entre otras redes, se usará este procedimiento de criptografía de curva elíptica. Usa 256 bits.
        - SHA-256: Se trata de un algoritmo criptográfico de hashing que genera hashes de datos de 256 bits.
        - RipeMD-160: Esta función hash criptográfica produce hashes de datos de 160 bits.

      Tenemos 4 tipos de algoritmos principales para el proceso de encriptado. El número de bits que tiene dicho encriptado en comparación al resto es bastante estándar, de hecho, estos algoritmos de encriptado coinciden con otras muchas redes principales de hoy en día, siendo el de 128 bits un poco bajo. [120] [121]

    - Historial de fallos de la seguridad: Como en el caso de todas las redes, en sus comienzos pudo existir más fallos de seguridad graves, pero tras atravesar una madurez en el desarrollo, la mayoría de las vulnerabilidades han sido menores, no comprometían la seguridad de la red. Haré una lista de las vulnerabilidades que si tuvieron una gravedad reseñable.

        - Junio del 2018: La vulnerabilidad de shellcode se encontró a través de las peticiones HTTP, esto podría haber sido explotado mediante ataques al software de los nodos, que podían haber roto el sistema de consenso.
        - Enero del 2019: La vulnerabilidad de maleabilidad de transacciones se encontró en procesado de las transacciones, esto podría haber sido explotado mediante la edición de la cantidad de ADA enviado.
        - Marzo del 2020: La vulnerabilidad de denegación de servicio se descubrió mediante el sistema que usa la red para ejecutar transacciones, un atacante podría haber llenado de transacciones la red para sobre cargarla y acabar con ella.
        - Mayo del 2021: La vulnerabilidad de reentrada se encontró por la forma que controla las llamadas recursivas. Los ataques se podrían haber traducido en el robo de fondos de manera repetida. [122] [123] [124]

    - Programas de recompensas por fallos: Si tiene este tipo de programas, hecho muy reseñable de la red, que hace que esta mejor protegida. [125]

- Polkadot
    - Estándares de encriptación: Polkadot utiliza estos estándares de cifrado, entre ellos:
        - Transport Layer Security (TLS): Este es un conocido sistema criptográfico que se repite en la mayoría de blockchains. Usa 128 bits.
        - Ed25519: Es un algoritmo de 256 bits que se encarga de verificar la firma digital.
        - Blake2b: Se trata de un algoritmo criptográfico de hashing que genera hashes de datos de 256 bits.
        - Curve25519: Este algoritmo de criptografía de curva elíptica, que se usa para crear claves públicas y privadas para las direcciones de Polkadot. Usa 256 bits.

      Hay 4 tipos de algoritmos principales para el proceso de encriptado en la red de Polkadot. Como podemos ver entre los cuatro algoritmos tienen unos bits de encriptado por encima de la media, lo que habla muy bien de su seguridad [126].

    - Historial de fallos de la seguridad:
      Como en todas las redes, a principios puede haber más fallas de seguridad graves, pero después de madurar, la mayoría de las

vulnerabilidades han sido menores y no afectaban la seguridad de la red. Seré capaz de enumerar todas las vulnerabilidades que si tuvieran una gravedad reseñable.

- Junio del 2017: La vulnerabilidad crítica en la base de código de Polkadot se encontró en el software de los nodos que controlaban las peticiones HTTP, este se solucionó con una bifurcación dura y este problema podría haber traducido en la inyección de código malicioso en el software del nodo pudiendo propagarse hasta el ordenador de un usuario.
- Marzo del 2018: La vulnerabilidad de denegación de servicio en la red se descubrió por la forma de realizar las transacciones de Polkadot. El atacante hubiera podido evitar que se procesaran transacciones en la red.
- Enero del 2019: Esta vulnerabilidad de reentrada en la plataforma de contratos inteligentes se explotó robando dinero a los usuarios mediante llamadas al contrato inteligente repetidas veces, este error estaba en la forma que controlaba las llamadas recursivas.
- Octubre del 2020: La vulnerabilidad en el protocolo de mensajería entre cadenas de las parachains de Polkadot se encontró en el método de envío de menajes entre otras parachains, la vulnerabilidad podía haber hecho que las distintas parachains fallarán por el envío de mensajes erróneos.
- Mayo del 2021: El fallo en el sistema de gobernanza venia del método que tenía la cadena de procesar los votos, este fallo podía llevar a usuarios maliciosos a votar propuestas y cambiar el rumbo de la red.
  [127] [128] [129]

- Programas de recompensas por fallos: Esta red también tiene este sistema de encontrar fallos [130], lo que habla muy bien de la protección de la red en este aspecto.

- Polygon
  - Estándares de encriptación: Los principales algoritmos de encriptado para la blockchain de Polygon son estos:
    - Secp256k1: Es un algoritmo de criptografía de curva elíptica, que como ocurre en las demás redes sirve para crear claves públicas y privadas. Usa 256 bits.
    - Blake2b: Es un algoritmo criptográfico de hashing el cual crea hashes de 256 bits.

        - TLS: Este sistema criptográfico es el que se suele usar en muchas redes. Usa 128 bits.

      Polygon en este caso solo tiene tres algoritmos de encriptación, donde el TLS se repite, pero tiene otros dos algoritmos que tienen un nivel alto de encriptación [159] [160][62].

    - Historial de fallos de la seguridad: Como en los demás puntos, solo recopilare fallos que pusieron en problemas la red de manera notable pudiendo acabar con ella:
        - Octubre del 2021: La vulnerabilidad del puente de plasma de Polygon se descubrió que se podía rehacer una transacción varia veces, lo que significa que el atacante logro duplicar su cantidad de tokens cada vez que lo realizaba, en este caso lo hizo 233 veces. Se soluciono en una semana más tarde.
        - Diciembre del 2021: Con el fallo del contrato de prueba de Polygon Genesis se descubrió que se podía editar el número de fondos que tenía un validador, pudiendo darle más fondos a uno o quitarle a otro. Solo duró 24 horas. [161][162][163]

    - Programas de recompensas por fallos: Esta red, como la mayoría de las principales, si tiene bug bounty. Lo cual denota que están preocupados por mantener un nivel de seguridad alto y actualizado [164].

- Ethereum
    - Estándares de encriptación: Existen tres algoritmos principalmente de encriptación en Ethereum:
        - Keccak-256 este algoritmo es el encargado de generar los hashes, es el encargado de verificar la integridad de los datos y crear firmas seguras. Utiliza 256 bits.
        - Secp256k1 es un algoritmo de criptografía de curva elíptica que sirve para crear claves públicas y privadas, como ocurre en otras redes. Se utiliza 256 bits.
        - TLS: Este sistema es usado en muchas redes. Usa 128 bits.

      Tras ver los tres tipos de criptografía, vemos que tienen un nivel de encriptación alto y se colocan en la parte superior de la comparación [131] [132].

    - Historial de fallos de la seguridad: Como siempre, se detallan los fallos que más daño hicieron a la red:

        - Julio 2016: El pirateo del DAO fue un fallo en el contrato inteligente DAO permitió que un atacante accediera a los fondos del contrato.
        - Julio del 2017: Fue el hackeo del monedero Parity multisig donde un fallo en el contrato inteligente del monedero Parity multisig permitió a un delincuente hacerse con 513.774 ETH.
        - Noviembre del 2017: El ataque del 51% de Geth se logró al reunir más de la mitad del hashrate de la red estaba bajo el control de un grupo de atacantes, lo que les dio la capacidad de revertir transacciones y gastar dinero por partida doble.
        - Enero del 2020: El fallo de reentrada en el contrato Keep fue un ataque que pudo robar 11,5 millones de USDC gracias a una debilidad en el contrato Keep.
        - Agosto del 2020: El fallo de reentrada en el contrato Harvest Finance permitió un robo de 34 millones de USDC, que fue posible gracias a una vulnerabilidad en el contrato Harvest Finance.
        - Octubre del 2020: Un error en el contrato Value DeFi permitió a un delincuente robar 15 millones de USDC.
        - Octubre del 2020: La vulnerabilidad de reentrada en el protocolo bZx donde el atacante pudo robar 50 millones de USDC.
        - Febrero del 2021: Bug en la reentrada del contrato Harvest Finance, en este robo se pudo sustraer 2,5 millones de USDC aprovechando un fallo de seguridad en el contrato Harvest Finance.

      Como podemos ver Ethereum tuvo muchos más ataques y con grandes cantidades, pero esto también se debe a que es una de las primeras blockchains del estudio en crearse. Pero si miramos la isma franja horaria con otros proyectos los datos son parecidos. [133] [134]
    - Programas de recompensas por fallos: Como todos los proyectos grandes tiene bug bounties, por lo que desde la organización se pretende tener al día la protección de muchas maneras. [135].

- Bitcoin
    - Estándares de encriptación: Los principales algoritmos de encriptación son 3:
        - Criptografía de curva elíptica (ECC): Usa 256 bits para generar claves públicas y privadas con algoritmos de curvas elípticas

        - Algoritmo Hash Seguro 256 (SHA-256): Es algoritmo de funciones hash, es el que chequea la identidad de las firmas.

    Bitcoin solo tiene dos algoritmos de encriptación, pero todos ellos con un numero alto de bitas, lo que le coloca entre las redes más seguras según la encriptación. [3]

- Historial de fallos de la seguridad: Los principales fallos de seguridad en Bitcoin han sido:
    - Enero del 2010: El fallo de inflación permitió a un usuario la capacidad de imprimir un suministro infinito de bitcoins. El mismo Satoshi corrigió este bug de la red.
    - Marzo de 2012: El bug de la maleabilidad de las transacciones fue aquel donde el usuario malicioso podía modificar el destinatario de una transacción después de haber sido enviada. Una bifurcación dura lo corregiría.
    - Agosto del 2013: El bug de la tasa de transacción consistía en que después de haber enviado una transacción, el ataque era capaz de duplicar los fondos. Fue corregido con una bifurcación blanda.
    - Abril del 2014: El problema Heartbleed permitió a un usuario el acceso a la memoria de un nodo Bitcoin.

    Como podemos ver, Bitcoin ha sufrido muy pocos ataques y sobre todo han sido en su fase más joven y donde existía una mayor inexperiencia sobre esta tecnología. Tras esto no ha tenido ningún fallo en de seguridad. [136] [137] [138]

- Programas de recompensas por fallos: Esta red, al no tener una empresa detrás que se encargue de actualizarla y mejorarla, no tiene ningún tipo de recompensa por encontrar debilidades.

- Solana
    - Estándares de encriptación: Los algoritmos de encriptación que usa solana principalmente son tres, estos son todos de 256 bits por lo que se colocan en el top de mejor criptografía. Los algoritmos son estos:
        - Ed25519: Las transacciones pueden firmarse con la técnica de firma digital de Ed25519, que también genera pares de claves públicas y privadas. El algoritmo de firma es de 256 bits y se considera bastante seguro.
        - Secp256k1: Las claves públicas y privadas se crean mediante la técnica de criptografía de curva elíptica

Secp256k1. El algoritmo ECC de 256 bits que utiliza se considera excepcionalmente seguro.
    - SHA-256: Para comprobar la exactitud de los datos se emplea una función hash criptográfica denominada SHA-256. Utiliza una función hash de 256 bits, que se considera bastante segura. [139] [140]

- Historial de fallos de la seguridad: Como en el resto de las entradas, en este apartado solo se pondrán fallos de seguridad graves.
    - Febrero de 2022: El problema con Wormhole fue un exploit que permitió crear 120000 WETH en Solana, esto ocurrió por la falta de autoría en la verificación de autorizaciones.
    - Marzo de 2022: El problema Optifi vino una condición de carrera en el protocolo que hizo que se robaran más de 1 millón de euros.
    - Junio de 2022: El problema de Solend fue que un exploit logro tener el control de una ballena de Solana. El fallo se dio en el protocolo de solend cambiando los sistemas de liquidación del sistema.

  Solo ha habido 3 caso lo cual es una buena señal, los únicos problemas estos datos es que son muy recientes y son también de Dapp de la parte DeFi. [141] [142]

- Programas de recompensas por fallos: Si tiene programa de recompensas. [143]

2.3.3 Análisis de la descentralización de las Blockchains

A lo largo de este capítulo, examinaremos las variables que se eligieron previamente para investigar la descentralización en las blockchains seleccionadas antes. Buscaré los datos de mayor calidad que puedan aclarar el propósito del tema, que es investigar la descentralización de las blockchains seleccionadas. Después de leer esta información, podremos comprender que blockchains son más o menos descentralizadas y elegir las que queremos. Las variables que analizaré y que previamente elegí son estas:

- Número de nodos
- Distribución geográfica de los nodos
- Mecanismo de consenso Gobernanza
- Gobernanza

A continuación, analizaré las redes seleccionadas:

- Avalanche
    - Número de nodos: La red actualmente tiene un total de 1377 nodos. [93]

    - Distribución geográfica de los nodos:

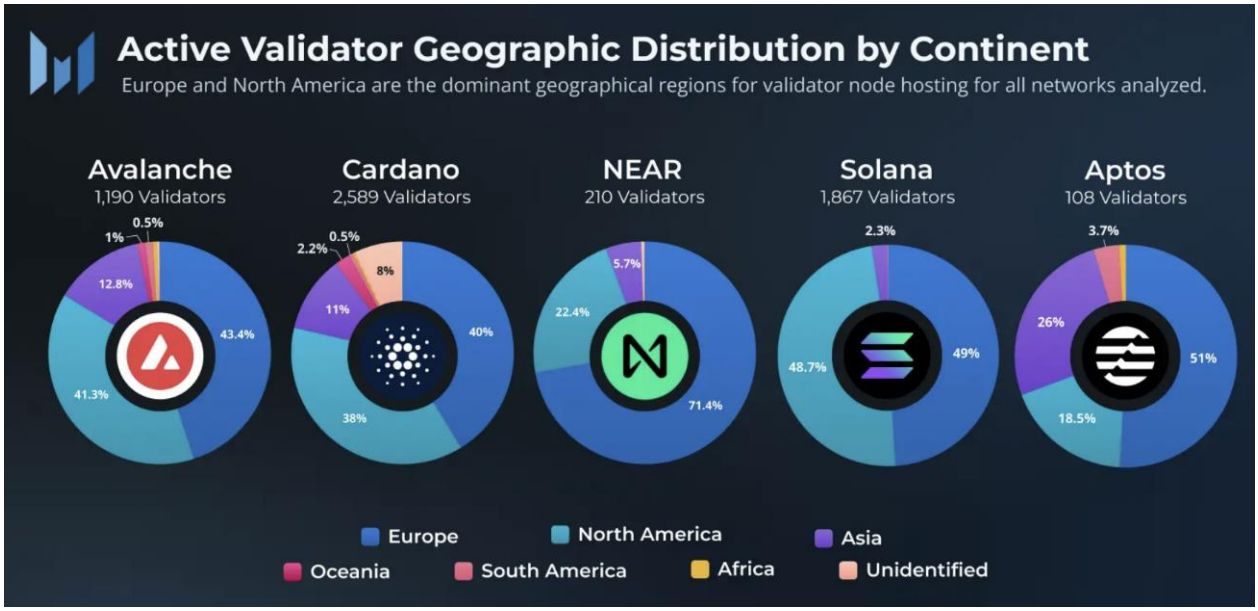

Figura 32. Gráficas de la distribución de validadores por continentes [90]

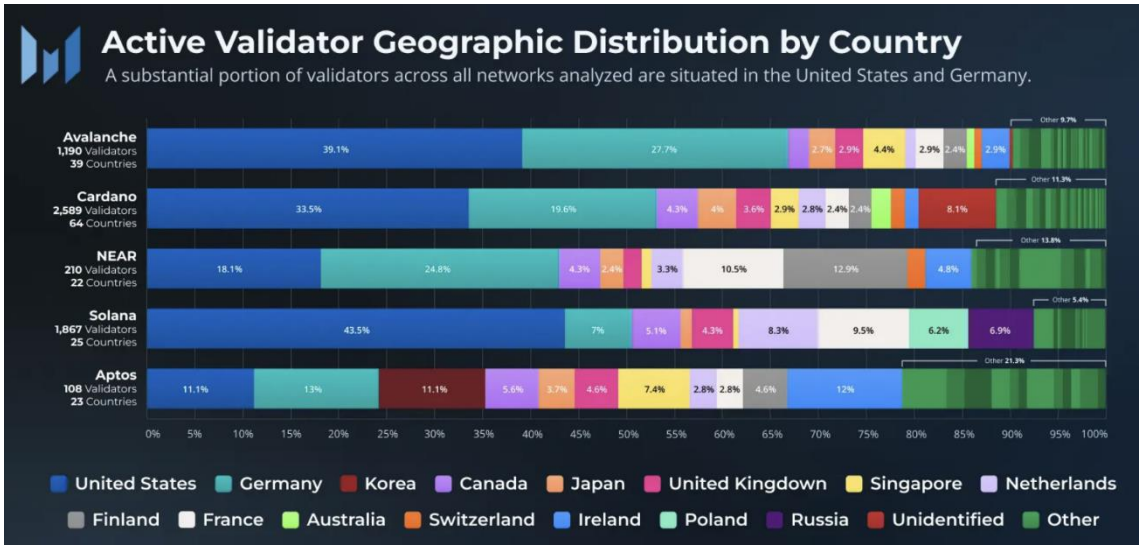

Figura 33. Gráficas de la distribución de validadores por países [90]

Tras ver las dos gráficas de Avalanche, podemos ver que el 80% de los nodos se encuentran entre norte América y Europa. Y más del 60% se encuentran en solo dos países. Estos datos no son favorables de cara a la descentralización. Ya que un cambio en las regulaciones de estos países podría dañar el desempeño de la red. [90]

- Mecanismo de consenso: 2000 Avax [144] son necesarios para crear un nodo, lo que es cerca de $26000 actualmente. [2]

- Gobernanza:

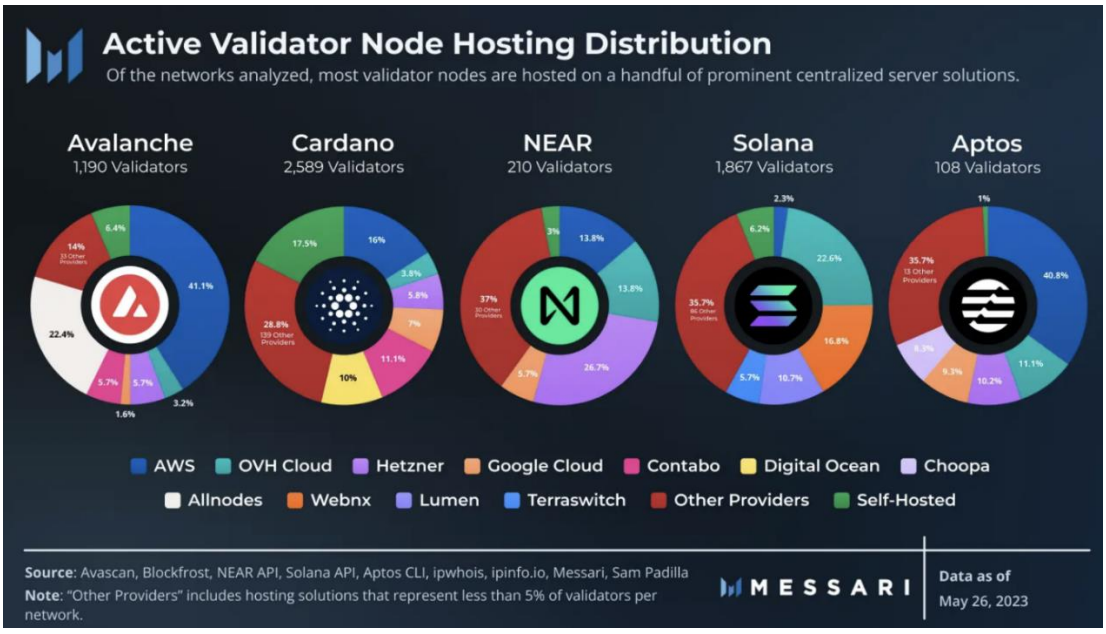

Figura 34. Gráficas de la distribución del hosteo de los validadores por empresas [90]

Como podemos ver en el gráfico de Avalanche, solo dos proveedores de servicios tienen el 60% de los nodos de la red ejecutándose en sus servidores. No es un dato muy alentador para la descentralización de la red [90].

- Cardano
  - Número de nodos: Son 3171 nodos validadores actualmente [145]

  - Distribución geográfica de los nodos:

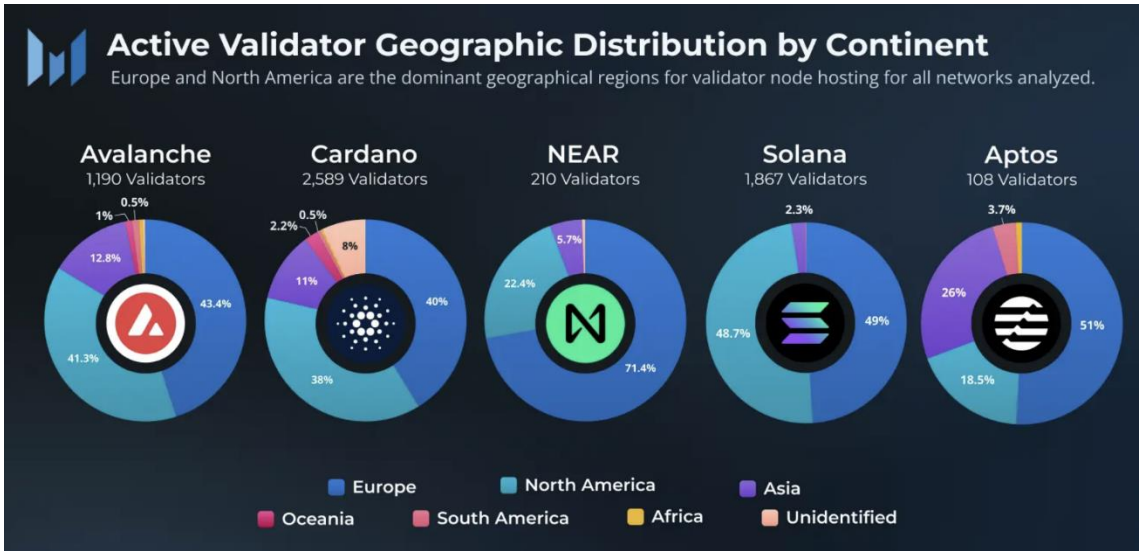

Figura 35. Gráficas de la distribución de validadores por continentes [90]

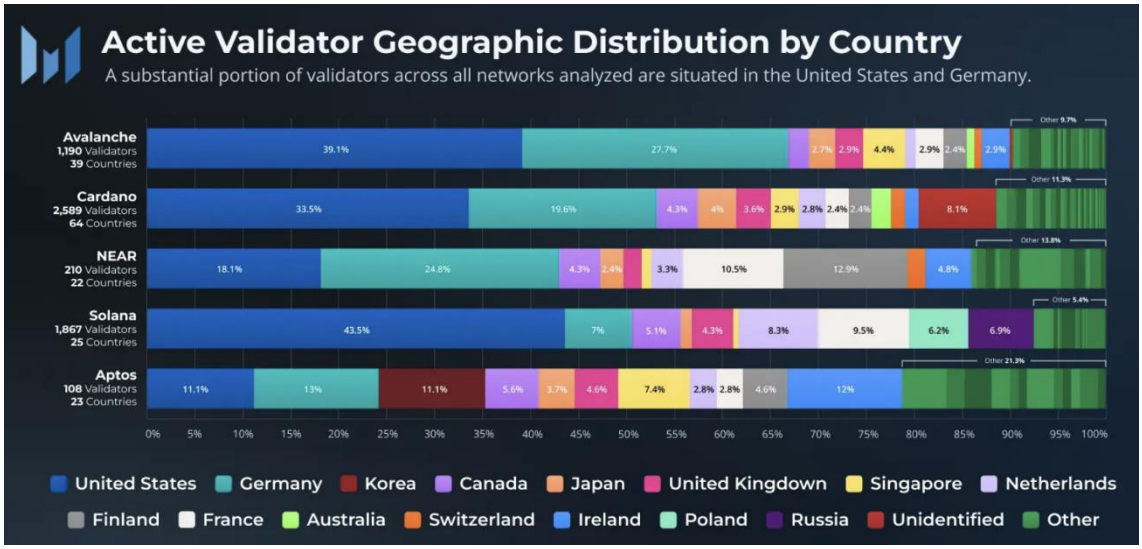

Figura 36. Gráficas de la distribución de validadores por países [90]

Si vemos los gráficos de distribución geográfica, podemos ver que más del 75% de los nodos se encuentran en norte América y

Europa. Además, Alemania y USA tiene más del 50% de la red individualmente. Estos datos no son buenos de cara a tener una red descentralizada [90].

- Mecanismo de consenso: 500,000 ADA [146] son necesarios para crear un nodo, dificultando enormemente la creación nodos por el alto precio que sería sobre $150000 [2].

- Gobernanza:

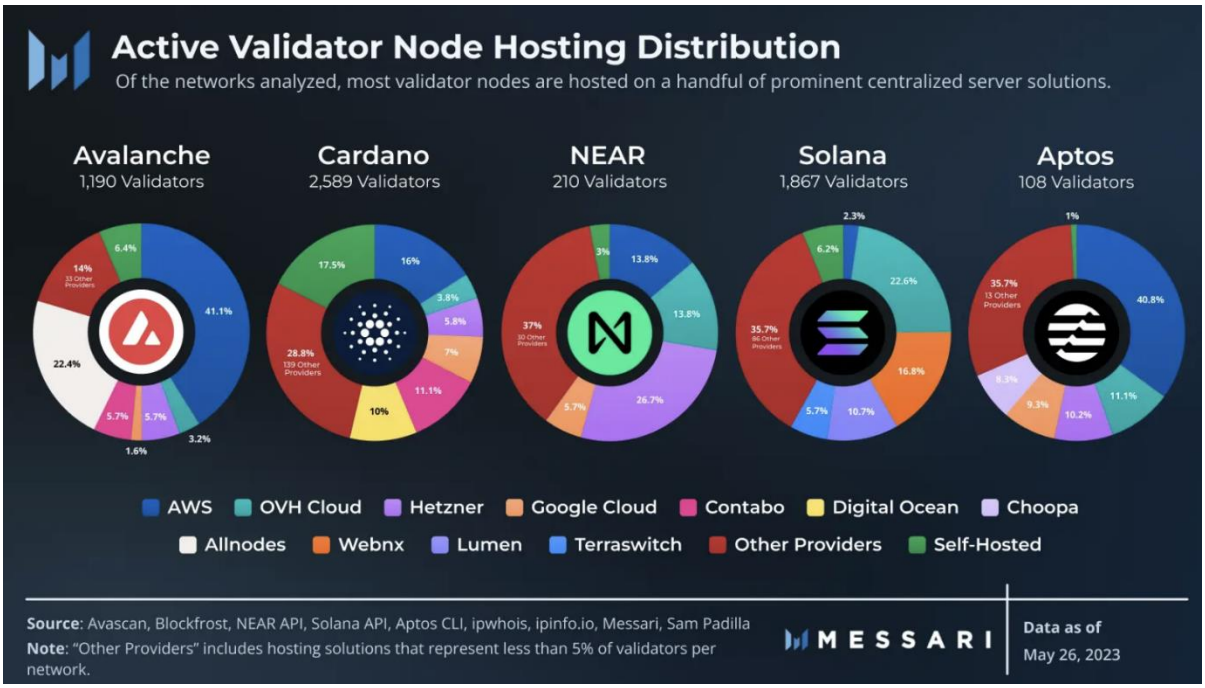

Figura 37. Gráficas de la distribución del hosteo de los validadores por empresas [90]

En el caso de Cardano, si están los proveedores de servicios mejor repartidos, y en comparación a los otros gráficos sería el que mejor repartido lo tiene. Por lo que no sería un mal dato sobre descentralización en este punto [90].

- Polkadot
  - Número de nodos: Son 297 nodos validadores [147]. Una cantidad que se hace bastante baja en comparación a otras redes.

  - Distribución geográfica de los nodos: Siguiendo el reporte de Staking Rewards [99] la distribución geográfica por continentes sería:
    - Asia: 57%

        - Norte América: 25%
        - Europa: 12%
        - Otros: 6%

      Y por países sería:

        1. China: 27%
        2. Estados Unidos: 23%
        3. Corea del Sur: 10%
        4. Japón: 7%
        5. Alemania: 6%

      Como podemos ver más de la mitad de los nodos validadores se encuentran en Asia, pero sin embargo se necesitan tres países para superar el 50% de validadores. Que, sin ser datos de descentralización excelentes, están mejor que los anteriores.

    - Mecanismo de consenso: Se necesitarán 120 DOTs para poder crear un nodo validador [148] lo que es a precio de mercado $620 [2]. Un precio demasiado accesible, pudiendo llegar a ser peligroso poder crear nodos tan baratos.

    - Gobernanza: Los proveedores de servicios de servidores son el 60% de los nodos validadores. De estos Google Cloud Platform representa el 30% y Amazon Web Services el 25% [149] entre dos proveedores ya superan el 50% dato un poco perjudicial para su descentralización.

- Polygon
    - Número de nodos: Son 100 validadores únicamente [150]. Una vez es un dato algo corto en comparación a otras redes.

    - Distribución geográfica de los nodos: Según un informe de Staking Rewards [99], la distribución geográfica de los validadores de Polygon es la siguiente:
        - Asia: 48%
        - América del Norte: 28%
        - Europa: 16%.
        - Otros 8%

      El informe también revela que los 5 países con más validadores de Polygon son:

        - China: 22%
        - Estados Unidos: 17%
        - Corea del Sur: 10%.

- Japón: 7%.
- Singapur: 5%.

Como podemos ver entre dos continentes casi estarían el 80% de los validadores, pero se necesitarían los 4 primeros países para llegar al 50% lo que da una mejor imagen de descentralización que muchas redes que estoy estudiando.

- Mecanismo de consenso: Actualmente no se puede ser validador, lo que da una mala imagen de Polygon para ser descentralizada [150].

- Gobernanza: Solo el 40% de los nodos están en proveedores de servicios cloud, donde ni sumando los 4 primeros se logra llegar al 50%. Estos datos son muy positivos, porque la mayoría de los nodos no están en un proveedor centralizado. [90]

- Ethereum
  - Número de nodos: Son 798081 nodos validadores [151]. Un número muy superior al resto de blockchains.

  - Distribución geográfica de los nodos:

Figura 38. Mapa con la distribución geográfica de los nodos de Ethereum [152]

Como podemos ver la gran mayoría están en Europa y Estados Unidos. En cuanto a países solo estados unidos cubre el 44% y unido a Alemania ya superarían el 50%. Por lo que en

descentralización geográfica Ethereum no es tan bueno como en otras variables de descentralización [151].

- Mecanismo de consenso: 32 ETH son los que se necesitan para poder crear tu propio nodo validador [153] que tiene un precio de mercado de $60000 [2], si lo comparamos con otras blockchains es un precio intermedio alto.

- Gobernanza: Según lo publicado por ethernodes [152]
  Solo el 34% de los nodos se encuentran en servicios cloud y sumando los 5 proveedores más usados no llegarían al 50%. Esto son buenos datos de descentralización, ya que no se depende excesivamente de empresas centralizadas.

- Bitcoin
  - Número de nodos: Bitcoin tiene 16894 nodos [95]. Este dato es muy superior a la mayoría de las redes.

  - Distribución geográfica de los nodos:

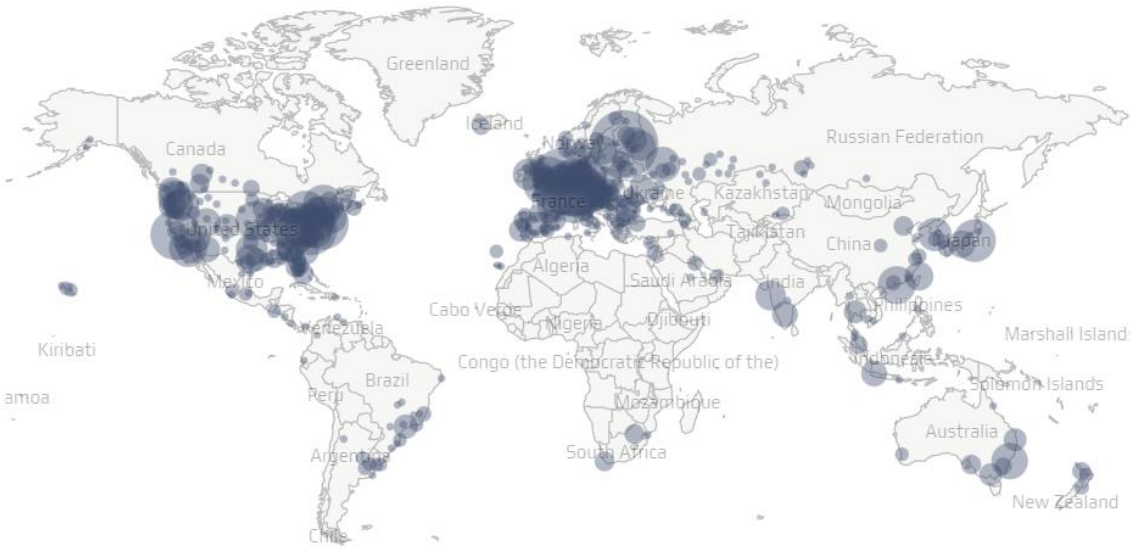

Figura 39. Mapa con la distribución geográfica de los nodos de Bitcoin [95]

Si vemos el mapa podemos ver que Bitcoin tiene presencia prácticamente en todo el mundo. Si bien es cierto que Estados Unido y Europa son las zonas donde quizás haya más cantidad de nodos. Aun así, tiene una presencia mundial y eso es muy beneficioso a ojos de la descentralización [95].

- Gobernanza: Solo el 34% de los nodos formaran parte de un servicio externo de cloud. Y entre los 4 más usados no se llega al 50% de los nodos. Por lo que Bitcoin también está muy descentralizado y este aspecto. [95]

- Solana
  - Número de nodos: El número de validadores actualmente es de 1843 [154], que como hemos visto a lo largo de la comparación no es una mala cantidad de nodos.

  - Distribución geográfica de los nodos:

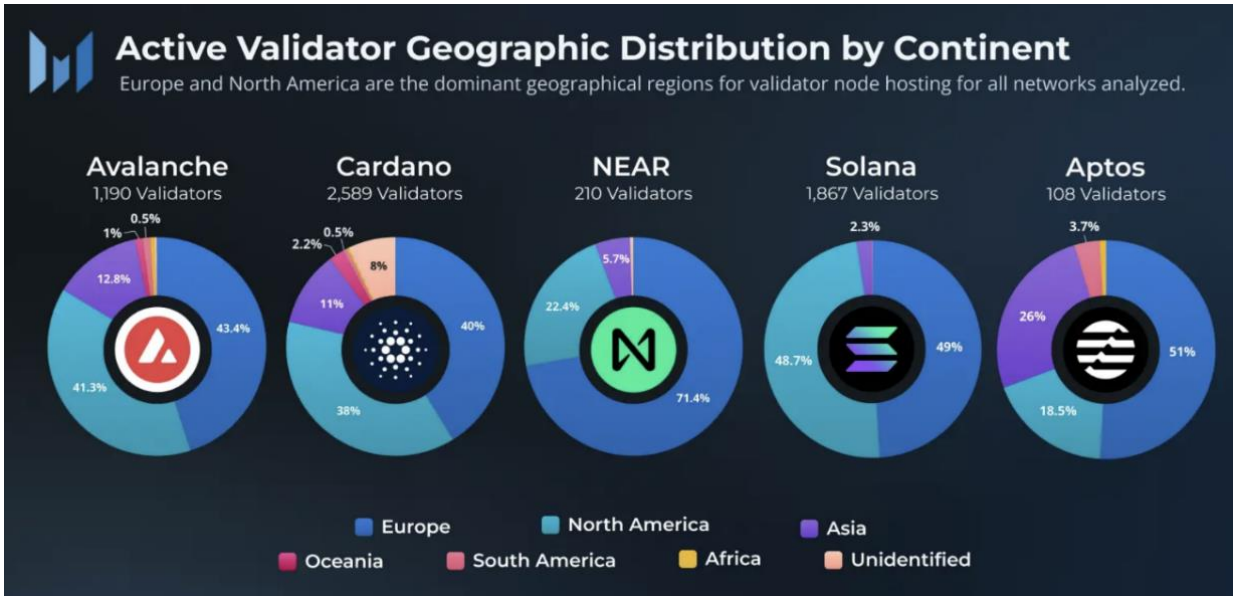

Figura 40. Gráficas de la distribución de validadores por continentes [90]

Figura 41. Mapa con la distribución geográfica de los nodos de Solana [154]

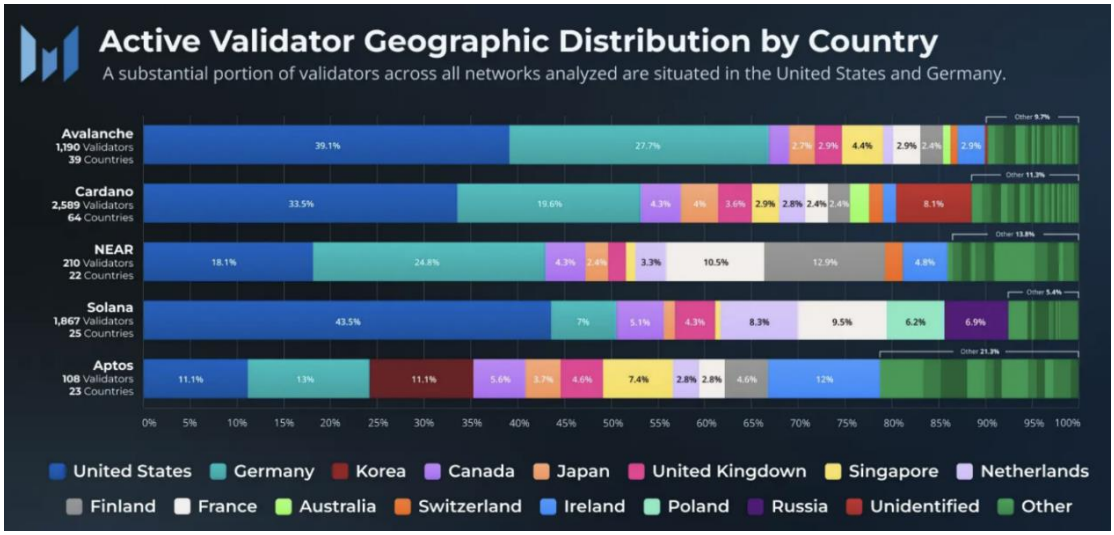

Figura 42. Gráficas de la distribución de validadores por países [90]

Según las gráficas, casi el 100% de los nodos están entre Norte América y Europa. Aunque lo reducimos a países, Estados unidos tiene casi el 50% de los validadoras. Este hecho puede ser un poco peligros si se intenta conseguir la mayor descentralización posible [90].

- Mecanismo de consenso: Se necesitan 0.02685864 SOL para poder formar un nodo validador [155]. Esto son $0,5 [2] lo que es un precio muy bajo pudiendo dejar entrar a muchos nodos maliciosos.

- Gobernanza:

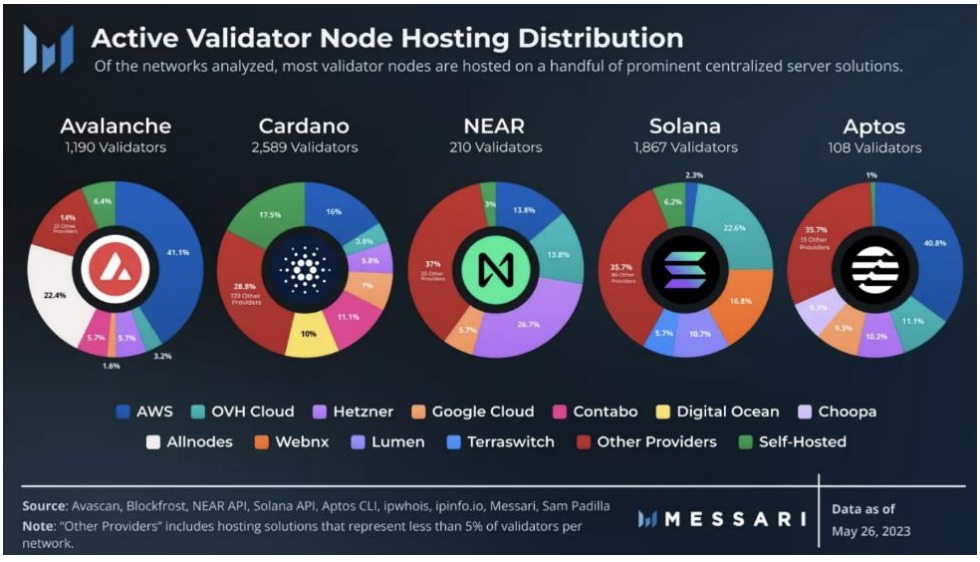

Figura 43. Gráficas de la distribución del hosteo de los validadores por empresas [90]

Como podemos ver en el gráfico, Solana no tiene ningún proveedor de cloud que supere el 25% individualmente y si sumas los 3 más grande no llegan al 50%. Esto es una buena señal para una red que aspira ser lo más descentralizada posible [90].

2.3.4 Comparación entre las diferentes Blockchains analizados

Pese a ser un resultado resumido, ya que la extensión es corta, es importante destacar la dificultad para encontrar datos fiables y actuales, además de la importancia de la selección de las redes a estudiar. Ya que al elegir redes importantes con propuestas diferentes descartamos blockchains que solo prometen resultados o blockchains repetitivas. Esto hace que el resultado alcanzado sea relevante pese a la extensión de la explicación.

En los puntos anteriores tenemos el producto de la investigación de las tres variables que forman parte el trilema; seguridad, escalabilidad y descentralización. Si bien he analizado estas variables por separado, también es importante recalcar que uniendo dos variables pueden mejorarse entre sí. Un ejemplo de esto sería una red que es muy descentralizada, que será más segura ya que es más difícil ser controlada.

Si entramos a analizar los resultados, en el apartado de escalabilidad, tenemos sobre todo claros perdedores, más que claros ganadores. Esto es así porque las dos blockchains más antiguas de la lista se han descolgado rápidamente. No es un secreto la poca escalabilidad que tienen las redes de Ethereum y de Bitcoin. Es por esto por lo que están apareciendo distintas redes de capa dos para poder hacer estas blockchains más escalables. Las principales razones de la baja estabilidad que tenían eran las transacciones por segundo (TPS) tan altas que tenían la latencia. Estos tiempos tan altos hacen al usuario estándar desencantarse por el producto, porque: ¿Quién pagaría con una tarjeta que tarda 10 minutos en verificar la transacción?

Las otras redes que han ido naciendo, sobre todo para intentar solucionar esas problemáticas, tienen tiempos mucho más lógicos que desde luego un usuario estaría contento en asumir, llegando el caso de Solana, que sería el que mejores resultados ha tenido en las pruebas realizas para medir la escalabilidad. Solana es una red que nació para mejorar la escalabilidad y superar a Ethereum. Y desde luego en el apartado de la escalabilidad le ha ganado. También es cierto que cuando Ethereum logre acabar su actualización lo más probable es que sea mucho más escalable también.

Si nos vamos al apartado de seguridad, todas las redes tienen unas bases mínimas de calidad. En el mercado tan competitivo que es el de las criptomonedas, una buena seguridad es primordial, y es esta la razón por la que los desarrolladores de blockchain centran sus esfuerzos en no faltar en esta pata del trilema. Si vemos el historial de fallos en la seguridad, Ethereum y Bitcoin pueden ser los que más tengan, pero son las redes más longevas y llevan muchos años sin ningún tipo de fallo. Además, tienen los encriptados de nivel

más alto, lo que hace al algoritmo de encriptación mucho más seguro. Es por esto por lo que es difícil elegir unas redes en concreto como más seguras, pero estando todas muy cercas unas de otras, Ethereum, Bitcoin y Polygon posiblemente sean las más seguras, y de manera muy holgada sobre el resto.

Por último, posiblemente la variable más representativa de la tecnología blockchain dentro del trilema. La descentralización es el camino que intentan seguir todas las blockchain y al que aspiran todos los proyectos, por esta razón, la descentralización era una parte clave a analizar.

Como se puede ver en los datos recogido, hay dos claras blockchains descentralizadas, principalmente por el número de validadores, Ethereum y Bitcoin. Una vez más, no era un secreto que estas blockchains serían las más descentralizadas. Con este punto se puede ver muy bien lo que es el trilema, tanto Ethereum como Bitcoin tienen su extremo débil en el trilema por la escalabilidad, pero en las otras dos variables tienen de los mejores resultados de redes reconocidas.

Cabe destacar que en un escalón más abajo estarían tanto Cardano como Solana en cuanto a redes descentralizadas, aunque el caso de Solana es muy interesante, ya que viendo sus datos puede estar en un segundo escalón de redes descentralizas, pero sin embargo cuando ha tenido errores la red, los desarrolladores han sido capaces de pararla [156], este hecho es impensable en una red realmente descentralizada, ya que para frenarla se debería tener el 51% de los nodos al menos.

Tras haber realizado este estudio es difícil quedarse con una red solo que domine las tres variables; no solo porque esa es la gracia del trilema cripto, sino porque aún no hay ninguna red que llegue a poder hacerlo y porque como hemos probado, siempre se flaquea por algún lado, o no se destaca en ninguna, como ha podido ser el caso de Avalanche, que ha tenido buenos resultados, pero no notables en ninguno de los ámbitos.

Si tuviera que escoger una red como la mejor entre las mejores, posiblemente seria Ethereum, ya que en cuanto a tecnología de los smart contract está mucho más desarrollada, aunque tiene una escalabilidad baja no es tan baja como la de Bitcoin. Y la seguridad y descentralización de Ethereum son muy destacables. Además, con la aparición de tantas layer para Ethereum, permitirá tener una red escalable, pero con las facultades de Ethereum, por lo que en el corto plazo esta problemática estaría controlada.

También Solana podría ser una red interesante, que ha logrado buenos datos en todas las variables, pero como comenté antes, tiene una falsa realidad en cuanto descentralización y se ha visto envuelto en caídas de su precio por problemas del mundo cripto que hace sospechar en la red [157].

3 Resultados y conclusiones

Se ha observado que la contribución actual y potencial de la Blockchain es amplia y diversa. Muchas de las ramas están en pleno desarrollo, mientras que otras están en una etapa mucho más temprana. La tecnología disruptiva de Blockchain ha asentado las bases para un futuro tecnológico mucho más eficiente, democrático y seguro, aunque no se puede precisar quién gobernará en el futuro.

A lo largo de este extenso trabajo se ha logrado establecer una base de conocimiento clave sobre una tecnología que pese a estar en boca de todos es una gran desconocida. En este trabajo he partido desde un punto inicial, presentando directamente nombre de blockchain hasta explicar una de las mayores limitaciones que tienen las blockchains a día de hoy; que es el trilema cripto. Y no solo eso, he terminado el proyecto realizando un análisis en profundidad de la escalabilidad, seguridad y descentralización, de las blockchains más destacadas o con más potencial actualmente en el sector DeFi.

El trabajo se divide en dos partes, una parte más teórica, donde se intenta pasar de un conocimiento bajo o nulo a un conocimiento más avanzado de la blockchain y los smart contracts. La intención con esta primera parte no es ser un maestro en la materia, pero si tener las nociones básicas para entender esta tecnología. Y es por esa razón, por la que he hecho tanto hincapié en la primera parte y he querido que fuera tan extensa. La segunda parte, y donde se ha hecho el mayor trabajo de investigación con diferencia, intenta hacerlo de las principales variables que cuantifican la seguridad, escalabilidad y descentralización de un proyecto. Con esta investigación se intenta buscar, en primer lugar, la fiabilidad de las redes más famosas y utilizadas para el sector DeFi, sector que tiene un peso clave en el proyecto también por ser uno de los casos de uso más grandes de los contratos inteligentes. En segundo lugar, se trata de buscar si alguna de las blockchains actuales no cumple el trilema cripto y si todas lo cumplen intentar elegir una o varias que sean interesantes para poder trabajar con la DeFi en ellas.

Como he mencionado, la primera parte del trabajo comienza con un punto introductorio de la blockchain, donde intento presentar los conceptos más básicos de ésta, y tratar de dibujar en la mente del lector el funcionamiento de esta tecnología. Primero presentando la tecnología de una forma simple pero profunda, más tarde entro ya a hablar sobre la criptografía que tienen las blockchains, este punto es muy importante.

Al principio hablo en profundidad de la criptografía de la blockchain, presento una de las piedras angulares de esta tecnología, que prácticamente le da nombre “criptomonedas”. Como vemos en el punto, la criptografía es muy

importante, porque es lo que permite enviar información de manera segura conociendo a los usuarios y la autenticidad del mensaje gracias a la firma electrónica. Además, se usan unos métodos de compactación de la información que cuando nació la tecnología no eran tan comunes, que permiten hacer al mensaje inmutable, seguro y con información del emisor y receptor. Del mismo modo, habla de la importancia de las claves públicas y privadas y de la vital importancia de función hash y los árboles de Merkle. También se mencionarán algoritmos de encriptación que a día de hoy se usan y cuales se han quedado obsoletos.

El siguiente punto, dentro de la introducción, intenta hablar de un tema muy útil dentro de la blockchain, que son las distintas formas que se tienen de agrupar las blockchains, se presentan los dos tipos principales y se explican que grupos hay dentro de ellos. Este punto es interesante, porque al final solo un tipo es el que tiene la fama, y aunque de ese tipo vaya el proyecto, está bien ser conocedor de todos los demás que hay y más con el propósito que tiene el proyecto de ser una introducción de calidad al sector.

Se acaba este punto introductorio hablando de la importancia y los beneficios que ha traído o ha creado la blockchain, ya que, aunque algunos sean constantemente repetidos, como es la descentralización, esas cinco claves no son tan comunes, pero sin duda son las razones del progreso de la tecnología.

El siguiente punto es la historia de la blockchain. Esta parte es importantísima, para entender el desarrollo que ha habido y el papel clave que tiene Bitcoin en él. Este apartado le abro hablando de lo que ocurrió antes del Bitcoin, antes de que existiera la blockchain como tal. Hablo de los distintos eventos que permitieron en 2008 la aparición del Bitcoin. Tras esto me refiero en profundidad a la aparición de la tecnología blockchain de la mano del Bitcoin, como la mezcla de criptografía con tecnología P2P, que permitía un sistema de pagos descentralizado que era nuevo en el mundo. Del mismo modo, hago una especie de separación cronológica de las fases que ha vivido Bitcoin hasta el día de hoy. Por último, cierro este punto dividiendo por orden cronológico las fases que ha vivido la tecnología blockchain desde su creación, hasta hoy y mirando al futuro. Este punto es muy interesante, porque presenta la evolución que ha habido en la blockchain y que algunas veces es menos conocida.

Una vez se ha hecho una introducción de la blockchains y se ha explicado la historia hasta hoy, entro más en detalle en el funcionamiento de la blockchain. Primero, explicando los distintos sistemas de consenso que existen, y yendo más en profundidad de los clásicos dos que todo el mundo conoce, que, aunque no sean tan utilizados es necesario conocerlos para tener un mayor dominio del sector. Como es lógico tanto la prueba de trabajo como la prueba de participación, al ser los dos sistemas de consenso más utilizados, me hablo de ellos con mucho más detalle.

Seguidamente, entro a hablar de los nodos, apartado muy necesario, ya que los nodos son pieza clave dentro de la blockchain y es preciso su estudio para entender mejor el funcionamiento de estos. En este punto intento explicar de manera sencilla, pero sin olvidar todo lo referido a los nodos y lo relacionado con ellos.

Para cerrar el último punto sobre blockchain, hablo de tres de los problemas que tienen las blockchains a día de hoy, estos son bifurcaciones, ataques del 51% y la escalabilidad. Intento hablar en profundidad de estos temas, sobre todo lo hago con las bifurcaciones, ya que son algo bastante común que derivan de un fallo que de primeras parece difícil pero no lo es tanto. Solo habría que mirar la cantidad de bifurcaciones que ha tenido Bitcoin.

Tras acabar con el apartado de la blockchain, comienzo hablando de los contratos inteligente. Ya que a día de hoy no se pueden entender unos sin los otros prácticamente. En este punto comienzo explicando que son y para qué sirven, primero con una pequeña historia y contexto. Para posteriormente explicar la tecnología de manera más pormenorizada. Luego hablo de todas las industrias donde los contratos inteligentes son útiles y han afectado positivamente su aparición; por último, cierro el punto de los contratos inteligentes estudiando los beneficios de estos y también sus debilidades, para que el lector entienda qué partes quedan por mejorar y en qué puntos ya tiene una buena fortaleza. También comento los principales lenguajes de programación que se usan a modo de curiosidad informática.

El último punto de la primera sección trata de las 5 aplicaciones que ya se están dando para la unión de la blockchain con los contratos inteligentes, esto permite ver el potencial que tiene a futuro y todas las posibilidades que ya se están dando. Los principales sectores donde han entrado e innovado son; las finanzas de la mano de las DeFi, en la logística, en la propiedad y en los sistemas de gobierno. Es importante destacar que estos avances están en una fase de nacimiento por lo que tienen aún mucho margen de mejora.

El siguiente capítulo es uno de los que le da nombre al proyecto, y es el estudio del concepto DeFi, aquí estudio qué es, como nace y qué particularidades tiene. También hablo de las ventajas y desventajas y de la parte más técnica de la DeFi. Más tarde entro a comentar que componentes tiene que lo hacen tan disruptivo y útil, y sobre todo que justifican el crecimiento tan grande que está teniendo. Al final del capítulo, intento ver con datos, la realidad del crecimiento y del peso que tiene este sector en el mucho cripto, analizando el capital que hay, los protocolos y como han ido cambiando y también la seguridad de esta tecnología para ver si es de confianza para el usuario medio.

El capítulo con el que sigue es uno de los más interesantes, ya que escojo las que para mí son las blockchains más interesantes, por temas de capital, capitalización de mercado, innovación, propuesta a futuro, DeFi… Y las analizo

en profundidad para entender mejor de que se trata y cuáles son las tendencias tecnológicas a día de hoy, bien sean los sistemas de consenso, las propuestas de valor como las L0 o las L2. Primero comienzo con Bitcoin, terminando de hablar de él, ya que es la blockchain más importante, no solo por ser el padre de las demás, sino también por la capitalización de mercado que acumula. Tras esto, hago un análisis de Ethereum, el padre de los contratos inteligentes y la segunda blockchain con más capitalización. Luego vendrá la Binance Smart Chain, la tercera red más grande, pero la que primero logró abaratar los costes de transacción y hacerlos más rápidos, además es muy interesante estudiar la blockchain de CEX más grande del mundo.

A continuación, investigo sobre Polkadot y Cosmos, y su propuesta de las layer 0 y la interoperabilidad entre redes, los avances que pueden traer y la propuesta tan ambiciosa que están haciendo.

Después viene Cardano, blockchain creada por uno de los padres de Ethereum la cual se la conoce como la blockchain más perfeccionista, sus desarrolladoras tardan mucho en sacar actualizaciones y mejoras fruto del perfeccionismo que persiguen, esta blockchain es muy interesante no solo por ser de las que más capitalización tienen, sino también porque fueron las primeras en algunas propuestas novedosas y sobre todo por el perfeccionismo detrás de Hoskinson. Solana nació como la blockchain que destronaría a Ethereum, gracias a la escalabilidad que promete ofrecer, también trae consigo innovaciones como la prueba de historia o los altísimo TPS que promete tener. También hago un estudio de Polygon, ya que fue una de las primeras soluciones de capa 2 de Ethereum y posiblemente sea la más asentada y con más historia por lo que es interesante de estudiar. Por último, estudio la red de Avalanche, ya que su propuesta de las subnets y el poco gasto energético que promete tener la red es algo que merecía ser estudiado.

El penúltimo capítulo, habla en profundidad del problema que dio nombre Vitalik Buterin, y que el mismo está intentando solucionar. En este punto se explica que es el trilema cripto y que tres patas tiene que nunca se pueden cumplir las tres y porque todos los desarrolladores de blockchain están intentando lograr superar.

Finalmente termino mi parte teórica con el estudio de pormenorizado de las tres variables del trilema cripto, escalabilidad, seguridad y descentralización.

Una vez entendida la primera parte del trabajo, paso hablar de la parte más práctica y compleja, que es la de estudiar datos y variables para poder medir y comparar la escalabilidad, seguridad y descentralización. La selección de redes que hice fue mezclando las que había estudiado previamente añadiéndole las que más peso tuvieran en el sector DeFi, es interesante ver la cantidad de desarrollo que tienen algunas redes, y luego no logran cumplir, aun,

las propuestas de su white paper. También es interesante ver qué redes son peores a nivel de rendimiento, que tengan mucho más capital bloqueado que otras.

Una vez seleccionadas las blockchains a estudiar, realicé un estudio de herramientas y variable que pudieran servir para medir las tres patas del trilema. En este punto es interesante ver la cantidad de herramientas que hay para informarse, pero sin embargo la gran dificultad que existe muchas veces cuando no buscas los tres parámetros típicos como realizan en la mayoría de los estudios.

Ya entrando con el último punto del proyecto, como se ha podido ver ni siquiera eligiendo las blockchain con mejores propuestas se ha logrado encontrar una que logre ser escalable, segura y descentralizada. La blockchains que más dominaban en un factor perdía en otro o incluso otros, lo que prueba que el trilema sigue siendo algo actual, y que, pese a que se intenta, aún no exista una blockchain que lo solucione.

Los resultados del análisis han sido muy interesantes no solo por lo mencionado en el párrafo anterior, sino porque han probado lo que se ve en otras fuentes de información y otros análisis más populares, como puede ser la falta de descentralización de los nuevos proyectos y la falta de escalabilidad de los veteranos. Esto es así en términos de escalabilidad, los claros perdedores han sido Ethereum y Bitcoin, como se presuponía, y demuestra que las nuevas corrientes que están creando soluciones de capa 2 para estas blockchains están totalmente justificadas, ya que la escalabilidad es el punto débil y el cual necesita ser mejorado, en este caso con un L2. Pero es lógico que tengan que aparecer estas mejoras, porque si no es difícil que las criptomonedas lleguen al público general, o al menos con Ethereum y Bitcoin a la cabeza. Porque el usuario medio acostumbrado a transacciones en milésimas no aceptaría pasar a tardar minutos en que se confirme. También es interesante ver la gran escalabilidad de proyectos como Solana, que desde su nacimiento se propuso como una red pensada con esa finalidad, por eso tiene datos como el de TPS tan superiores al resto.

Si nos referimos a los resultados arrojados por el estudio de la seguridad, es lógico ver que ningún proyecto flaquee, porque sería imposible atraer capital si tus fondos no estuvieran seguros, es por eso por lo que las blockchains establecidas, ya sean nuevas o viejas, no olvidan esta característica en absoluto. Aun así, hemos podido ver diferencias no muy grandes entre las distintas blockchains, ya sea por la calidad de los algoritmos de encriptado o por el número de hackeos recientes que han tenido, siendo la razón por la que Polygon, Ethereum y Bitcoin se posicionarían como las mejores.

Por último, en el apartado de la descentralización, Ethereum y Bitcoin han ganado con la misma soltura que perdieron el apartado de escalabilidad, la

diferencia en la cantidad de nodos validadores es abismal, y también el reparto de estos por el mundo, lo que les hace ser las dos blockchains menos centralizadas. Cabe destacar que una red más descentralizada, también es más segura, ya que será más difícil lograr unir nodos para llevar a cabo actos maliciosos o será necesario atacar a más nodos para generar daños en la red.

Es por esto, que el análisis de los datos recabados ha sido muy interesante y ha sido un claro espejo de opinión publica en las criptomonedas, tanto por identificar con datos que blockchains flaquean en que y ver que aún hay que esperar la llegada a una solución del trilema cripto.

En conclusión, la tecnología blockchain es una tecnología disruptiva y que puede traer grandes avances junto con la aparición de los contratos inteligentes que han hecho de catalizador para la aparición de mejoras reales del sector. Lograr tener una base para entenderlo puede ayudar a posicionarse primero en la tendencia tecnológica, y más en uno de los campos donde son mayores las aplicaciones aparecidas, la DeFi. De esta forma, se puede lograr eliminar intermediarios y abaratar costes, mientras se gana seguridad y transparencia. Además, el estudio de la escalabilidad, seguridad y descentralización puede arrojar datos muy interesantes, para poder seleccionar la blockchain que es más interesante a la hora de entrar en el sector DeFi. Por lo que, tras el estudio realizado en este proyecto, se podría obtener una red candidata para el usuario de DeFi.

3.1 Líneas futuras de investigación

Se proponen las siguientes líneas de investigación futuras basándose en la investigación que se hizo en este trabajo de fin de grado, así como en los desafíos pendientes en el campo de las finanzas descentralizadas y la tecnología blockchain:

- Análisis más profundo de las soluciones de escalabilidad: Aunque este estudio ya ha proporcionado un estudio inicial de la escalabilidad. También podría ser beneficioso llevar a cabo investigaciones más detalladas con las soluciones específicas de escalabilidad, como podrían ser las cadenas laterales, los canales estatales o incluso las soluciones de fragmentación.

- Evaluación del impacto de las mejoras tecnológicas futuras: Es crucial seguir evaluando el impacto de las mejoras tecnológicas futuras debido al rápido ritmo de innovación que está habiendo en el espacio blockchain.

Un muy buen ejemplo podría ser la transición de Ethereum al Ethereum 2.0, y el impacto que podría tener en la descentralización, la escalabilidad y la seguridad de la plataforma.

- Investigación sobre la adopción y la usabilidad de DeFi: Aunque la mayor parte de este estudio se ha centrado en los aspectos técnicos de la cadena de bloques y DeFi, sería útil examinar además las oportunidades y problemas asociados a la adopción y usabilidad de DeFi.

- Estudio del impacto socioeconómico de DeFi: Se podría investigar más a fondo el potencial de la DeFi para promover la inclusión financiera y la reducción de la desigualdad sólo se ha mencionado brevemente.

- Investigación sobre las implicaciones medioambientales de la blockchain: Por la creciente preocupación en el impacto medioambiental de la tecnología blockchain, sería interesante investigar este tema. Esto se podría hacer comparando la eficiencia energética de varios algoritmos de consenso o estudiar soluciones para disminuir el impacto medioambiental de la tecnología blockchain.

4 Análisis de Impacto

El impacto que se espera de este Trabajo Fin de Grado y la tecnología disruptiva tratada en el proyecto se analizarán en este último apartado del trabajo. También mencionaré algunos de los Objetivos de Desarrollo Sostenible que se incluyen en la Agenda 2030 y que la blockchain puede ayudar a mejorar [158], y por tanto se consideran importantes para el tema del proyecto.

Impacto Personal:

A nivel personal, el desarrollo de este TFG ha tenido un impacto significativo. Este proyecto me ha permitido ampliar mis conocimientos en áreas como blockchain, sistemas distribuidos, finanzas descentralizadas y ciberseguridad gracias a la investigación y el análisis exhaustivos realizados. Además, ha establecido una base sólida para comprender esta tecnología innovadora y cómo se puede aplicar a las finanzas contemporáneas. Dado que me brinda una ventaja competitiva en una industria emergente, este conocimiento me será esencial para mi desarrollo profesional.

Impacto Empresarial:

Este trabajo podría tener un impacto empresarial muy significativo por la importancia de la tecnología que se estudia en él. Este estudio puede ayudar a las empresas que buscan innovar en el sector financiero o poderse informar y aprender nuevas estrategias logrando una adopción de blockchain e incluso de la DeFi. Las empresas pueden tomar decisiones más informadas sobre qué tecnologías adoptar para sus necesidades específicas al poder comprender las ventajas y desventajas de cada blockchain en términos de escalabilidad, seguridad y descentralización. Esto podría ahorrar mucho tiempo y recursos, así como también mejorar la seguridad y la eficiencia de estas empresas al adoptar estas nuevas tecnologías.

Impacto Social:

La adopción de finanzas descentralizadas tiene el potencial de hacer que el acceso a los servicios financieros sea más accesible, especialmente en regiones del mundo que no tienen muchos bancos. Este estudio podría mejorar la comprensión de cómo hacer que estas tecnologías sean más seguras y accesibles para todos. Sin embargo, es importante señalar los posibles efectos negativos, como la posibilidad de que estas tecnologías sean utilizadas para actividades ilegales debido a su naturaleza descentralizada. También podría servir como base de aprendizaje para entrar con la tecnología blockchain. El análisis de escalabilidad, seguridad y descentralización podría usarse para entender que variables son importantes si nos queremos fijar en alguno de esos rasgos en una blockchain.

Impacto Económico:

A medida que más empresas adopten finanzas descentralizadas, es probable que veamos un cambio importante en la economía global. La comprensión de las características y limitaciones de cada blockchain puede informar este cambio, asegurando que se adopten las tecnologías más seguras y eficientes. Sin embargo, es importante tener en cuenta los efectos negativos potenciales en las industrias actuales y en la estabilidad económica en general.

Impacto Medioambiental:

El impacto de la tecnología blockchain y las criptomonedas en el medio ambiente ha sido un tema de gran controversia. Aunque algunas blockchains requieren una gran cantidad de energía, otras están desarrollando soluciones energéticamente más eficientes. Un aspecto importante de este estudio es la evaluación de las diferentes blockchains desde esta perspectiva, pudiendo diferenciar entre las blockchain de prueba de trabajo y prueba de participación, donde las segundas son las que más respetan el medio ambiente.

Impacto Cultural:

La adopción de finanzas descentralizadas y blockchain puede cambiar la forma en que las personas interactúan con el dinero y las instituciones financieras, incluso con la totalidad del sistema, nuevas formas de votar, de registrar la propiedad… Por lo que este estudio también puede tener un impacto cultural. El conocimiento de los beneficios y desventajas potenciales de estas tecnologías puede ayudar a moldear este cambio de manera justa y positiva para toda la población.

Este estudio contribuye a múltiples objetivos relacionados con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030. Se enfoca principalmente en el Objetivo 9: Industria, Innovación e Infraestructura porque busca mejorar la comprensión de la tecnología blockchain, una innovación importante en la industria tecnológica. Además, es relevante para el Objetivo 8 de Trabajo Decente y Crecimiento Económico porque fomenta una mayor comprensión tanto de las finanzas descentralizadas como de la tecnología en sí, que podría ofrecer nuevas oportunidades de crecimiento económico y empleo.

Además, este estudio puede ayudar al Objetivo 10: Reducción de las Desigualdades porque las finanzas descentralizadas pueden hacer que los servicios financieros sean más accesibles para las personas en regiones menos bancarizadas del mundo, lo que ayuda a reducir las desigualdades en el acceso a estos servicios, también la tecnología al ser sin intermediarios, descentralizada y trasparente, ayudaría facilitar la entrada a todos por tener barreras de entrada más bajas.

También está relacionado con el Objetivo 13: Acción por el Clima en términos de impacto ambiental. Este estudio puede contribuir a las discusiones sobre cómo hacer que la adopción de blockchain y finanzas descentralizadas sea más sostenible desde un punto de vista ambiental al evaluar las diferentes blockchains en términos de su eficiencia y consumo de energía.

Se han tomado decisiones en este TFG teniendo en cuenta los efectos de cada uno de estos aspectos. Por ejemplo, se consideró la relevancia y el potencial impacto de las blockchains en términos personales, empresariales, sociales, económicos, ambientales y culturales. Además, las métricas de descentralización, escalabilidad y seguridad para evaluar estas blockchains se eligieron en función de su relevancia para cada uno de los diferentes contextos de impacto, siempre en pro del bien común.

5 Bibliografía

[1] Google (2023) *Google trends*. Available at: https://trends.google.com/trends/explore?date=all (Accessed: 02 July 2023).

[2] CoinMarketCap (2023) *Precios, Gráficos y Capitalizaciones de Mercado de Criptomonedas, CoinMarketCap*. Available at: https://coinmarketcap.com/es/ (Accessed: 02 July 2023).

[3] Guardeño, A.D., Vico, D.J. and Encinas, H.L. (2019) *Que sabemos de Blockchain, climberstrading.com*. Madrid, Spain: CSIC. Available at: https://climberstrading.com/wp-content/uploads/2022/09/Que-sabemos-de-Blockchain.pdf (Accessed: 02 July 2023).

[4] Blockchain, S.B.S. (2022) *Los 3 Principales tipos de redes blockchain – Observatorio Blockchain, Noticias Blockchain | Observatorio Blockchain*. Available at: https://observatorioblockchain.com/hypernifty/redes-blockchain-tipos/ (Accessed: 02 July 2023).

[5] Kumar, M.S. (2019) *The disruptive blockchain: Types, platforms and applications, Scribd*. Available at: https://www.scribd.com/document/492021012/DisruptiveBlockchainTypesPlatformsandApplications (Accessed: 02 July 2023).

[6] Kim, H.M. *et al.* (2020) *Permissionless and Permissioned, Technology-Focused and Business Needs-Driven: Understanding the Hybrid Opportunity in Blockchain Through a Case Study of Insolar, https://ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7169508 (Accessed: 02 July 2023).

[7] Khettry, A.R., Patil, K.R. and Basavaraju, A.C. (2021) *A detailed review on blockchain and its Applications, SpringerLink*. Available at: https://link.springer.com/article/10.1007/s42979-020-00366-x (Accessed: 02 July 2023).

[8] IBM, I. (2021) Beneficios de blockchain - IBM Blockchain, IBM. Available at: https://www.ibm.com/es-es/topics/benefits-of-blockchain (Accessed: 02 July 2023).

[9] Liu, Q. et al. (2019) Education-industry cooperative system based on Blockchain, ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/abstract/document/8606036 (Accessed: 02 July 2023).

[10] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system, Bitcoin. Available at: https://bitcoin.org/en/bitcoin-paper (Accessed: 02 July 2023).

[11] Martin, P.P. (2021) Blockchain ¿Por qué y cómo surge? , Visualeo. Available at: https://visualeo.com/blockchian-por-que-y-como-surge/#:~:text=Blockchain%20surge%20en%202008%2C%20dentro,P2P)%20con%20t%C3%A9cnicas%20criptogr%C3%A1ficas%20avanzadas (Accessed: 02 July 2023).

[12] Sancho, C. (2020) *Historia y Evolución de la Tecnología blockchain de bitcoin, campus blockchain*. Available at: https://www.campusblockchain.es/historia-y-evolucion-de-la-tecnologia-blockchain-de-bitcoin/ (Accessed: 02 July 2023).

[13] Cointelegraph, O. (2018) *Últimas Noticias sobre BitPesa*, *Cointelegraph*. Available at: https://es.cointelegraph.com/tags/bitpesa (Accessed: 02 July 2023).

[14] Gómez, I. (2018) *Banco Central de Kenia advierte sobre bitcoin mientras Bitpesa Continúa Su Contienda Legal*, *CriptoNoticias*. Available at: https://www.criptonoticias.com/regulacion/banco-central-de-kenia-advierte-sobre-bitcoin-mientras-bitpesa-continua-su-contienda-legal/ (Accessed: 02 July 2023).

[15] Jiménez Mesa, Á. (2022) *Blockchain y Contratos Inteligentes. Oráculo de Precios Para Automated Market Makers, Orvium*. Available at: https://dapp.orvium.io/deposits/62d839c7928981fa754e1f24/view (Accessed: 02 July 2023).

[16] Mingxiao, D. *et al.* (2017) *A review on consensus algorithm of Blockchain, ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/8123011 (Accessed: 02 July 2023).

[17] de Vries , A. (2018) *Bitcoin's growing energy problem*, *Joule*. Available at: https://www.sciencedirect.com/science/article/pii/S2542435118301776 (Accessed: 02 July 2023).

[18] Smith, O. (2022) *Tipos de blockchain: Pública, Privada, híbrida Y federada, Metaverso Orange*. Available at: https://www.orange.es/metaverso/noticias/curiosidades/tipos-de-blockchain-publica-privada-hibrida-y-federada (Accessed: 02 July 2023).

[19] Yiu, N.C.K. (2021) *An overview of forks and coordination in Blockchain Development, arXiv.org*. Available at: https://arxiv.org/abs/2102.10006 (Accessed: 02 July 2023).

[20] Banafa, A. and IoT, Prof.A.Banafa. (2020) *Soft Fork and hard fork in Blockchain, OpenMind*. Available at: https://www.bbvaopenmind.com/en/technology/digital-world/soft-fork-hard-fork-in-blockchain/ (Accessed: 02 July 2023).

[21] Vokerla, R.R. *et al.* (2019) *An overview of blockchain applications and attacks, ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/8899450/ (Accessed: 02 July 2023).

[22] Team, xcoins. com (2022) *¿Cuál es la diferencia entre un hard fork y un soft fork?, Xcoins*. Available at: https://xcoins.com/es/blog/cual-es-la-diferencia-entre-un-hard-fork-y-un-soft-fork/ (Accessed: 02 July 2023).

[23] Bermejo, O. (2022) *▷ ataque del 51%: Definición, Quién está en Riesgo, ejemplo y Costo, invatatiafaceri.ro*. Available at: https://invatatiafaceri.ro/es/diccionario-financiero/ataque-del-51-definicion-quien-esta-en-riesgo-ejemplo-y-costo/ (Accessed: 02 July 2023).

[24] DiarioBitcoin, D. (2023) *Las Principales 4 Soluciones de Escalabilidad Capa 2 Para Ethereum, DiarioBitcoin*. Available at: https://www.diariobitcoin.com/ethereum/las-principales-4-soluciones-de-escalabilidad-capa-2-para-ethereum/ (Accessed: 02 July 2023).

[25] Basic, R. (2023) *¿Quién es David Chaum?, Bit2Me Academy*. Available at: https://academy.bit2me.com/quien-es-david-chaum/ (Accessed: 02 July 2023).

[26] Crypto, D. (2022) *¿Qué es bitgold? El precursor de Bitcoin*, *Crypto4Dummy*. Available at: https://crypto4dummy.com/que-es-bitgold/ (Accessed: 02 July 2023).

[27] Bastardo, J. (2019) *Bitcoin Antes de Nakamoto: El Intento de B-Money*, *CriptoNoticias*. Available at: https://www.criptonoticias.com/educacion/bitcoin-antes-nakamoto-intento-bmoney/ (Accessed: 02 July 2023).

[28] Qin, K. *et al.* (2021) *Cefi vs. defi -- comparing centralized to Decentralized Finance*, *arXiv.org*. Available at: https://arxiv.org/abs/2106.08157v2 (Accessed: 02 July 2023).

[29] Jiménez Mesa, Á. (2022) *Finanzas descentralizadas en blockchain: Automated market makers, swaps ..., dapp.orvium.io*. Available at: https://dapp.orvium.io/deposits/62d83b0658e50f1564f7bdda/view (Accessed: 02 July 2023).

[30] Amler, H. *et al.* (2021) *Defi-Ning Defi: Challenges & Pathway*, *arXiv.org*. Available at: https://arxiv.org/abs/2101.05589v1 (Accessed: 02 July 2023).

[31] Li, W. *et al.* (2022) *Security Analysis of DEFI: Vulnerabilities, attacks and advances*, *arXiv.org*. Available at: https://arxiv.org/abs/2205.09524v1 (Accessed: 02 July 2023).

[32] Li, W. *et al.* (2022) *Security Analysis of DEFI: Vulnerabilities, attacks and advances*, *arXiv.org*. Available at: https://arxiv.org/abs/2205.09524v1 (Accessed: 02 July 2023).

[33] Sambana, B. (2021) *Blockchain technology: Bitcoins, cryptocurrency and applications*, *arXiv.org*. Available at: https://arxiv.org/abs/2107.07964v2 (Accessed: 03 July 2023).

[34] Tapsell, J., Akram, R.N. and Markantonakis, K. (2018) *An evaluation of the security of the bitcoin peer-to- peer network*, *arXiv.org*. Available at: https://arxiv.org/abs/1805.10259v2 (Accessed: 03 July 2023).

[35] Rao, S.P. (2014) *Turning bitcoins into the best-coins*, *arXiv.org*. Available at: https://arxiv.org/abs/1412.7424v1 (Accessed: 03 July 2023).

[36] Ethereum , F. (2015) *Ethereum whitepaper*, *ethereum.org*. Available at: https://ethereum.org/en/whitepaper/ (Accessed: 03 July 2023).

[37] Hertig, A. (2023) *What is Ethereum?*, *CoinDesk Latest Headlines RSS*. Available at: https://www.coindesk.com/learn/what-is-ethereum/ (Accessed: 03 July 2023).

[38] Reiff, N. (2023) *Bitcoin vs. Ethereum: What's the difference?*, *Investopedia*. Available at: https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp (Accessed: 03 July 2023).

[39] Wackerow, P. (2022) *Ethereum Development Documentation*, *ethereum.org*. Available at: https://ethereum.org/en/developers/docs/ (Accessed: 03 July 2023).

[40] Cernera, F. *et al.* (2022) *Token spammers, rug pulls, and SniperBots: An analysis of the ecosystem of tokens in Ethereum and the Binance Smart Chain (BNB)*, *arXiv.org*. Available at: https://arxiv.org/abs/2206.08202v1 (Accessed: 03 July 2023).

[41] Compare, P. (2021) *What is Binance Smart Chain? the Pros and cons of the binance smart chain blockchain platform*, *CoinCodex*. Available at: https://coincodex.com/article/10884/what-is-binance-smart-chain-the-pros-and-cons-of-the-binance-smart-chain-blockchain-platform/ (Accessed: 03 July 2023).

[42] Dolor, R.J. (2023) *Binance Smart Chain (BSC) explained: A beginner's guide*, *Finbold*. Available at: https://finbold.com/guide/binance-smart-chain/ (Accessed: 03 July 2023).

[43] Wang, Qin *et al.* (2022) *Exploring unfairness on proof of authority: Order manipulation attacks and remedies*, *arXiv.org*. Available at: https://arxiv.org/abs/2203.03008v2 (Accessed: 03 July 2023).

[44] Hao, M., Qian, K. and Chau, S.C.-K. (2023) *Blockchain-enabled parametric solar energy insurance via ... - arxiv.org, https://arxiv.org/*. Available at: https://arxiv.org/pdf/2305.09961v2 (Accessed: 03 July 2023).

[45] Clarke, A. (2022) *Why interoperability is the key to blockchain technology's mass adoption, Cointelegraph*. Available at: https://cointelegraph.com/news/why-interoperability-is-the-key-to-blockchain-technology-s-mass-adoption (Accessed: 03 July 2023).

[46] Cryptopedia , S. (2021) *Why is interoperability important for blockchain?, Gemini*. Available at: https://www.gemini.com/cryptopedia/why-is-interoperability-important-for-blockchain (Accessed: 03 July 2023).

[47] Reegu, F.A. *et al.* (2022) *Interoperability requirements for blockchain-enabled Electronic Health Records in Healthcare: A systematic review and open research challenges, Security and Communication Networks*. Available at: https://www.hindawi.com/journals/scn/2022/9227343/ (Accessed: 03 July 2023).

[48] CryptoEQ , T.F. (2023) *Use Case Polkadot, Cryptocurrency Market Research and Insights*. Available at: https://www.cryptoeq.io/corereports/polkadot-abridged (Accessed: 03 July 2023).

[49] Platts, J. (2019) *Polkadot: The foundation of a new internet, Medium*. Available at: https://medium.com/polkadot-network/polkadot-the-foundation-of-a-new-internet-e8800ec81c7 (Accessed: 03 July 2023).

[50] Polkadot, F. (2017) *Whitepaper: Polkadot, Polkadot Network*. Available at: https://polkadot.network/whitepaper/ (Accessed: 03 July 2023).

[51] Chauhan, G. (2020) *What are cosmos benefits and advantages?, LinkedIn*. Available at: https://www.linkedin.com/pulse/what-cosmos-benefits-advantages-gurmeet-chauhan (Accessed: 03 July 2023).

[52] Cosmos , F. (2016) *Internet of blockchains, Cosmos Network*. Available at: https://v1.cosmos.network/intro (Accessed: 03 July 2023).

[53] Cosmos, C. (2021) *Deep Dive: HOW WILL IBC create value for the cosmos hub?, Medium*. Available at: https://blog.cosmos.network/deep-dive-how-will-ibc-create-value-for-the-cosmos-hub-eedefb83c7a0 (Accessed: 03 July 2023).

[54] Cosmos, F. (2016) *The internet of Blockchains, Cosmos*. Available at: https://cosmos.network/ (Accessed: 03 July 2023).

[55] Anderson, B. (2023) *A tick-by-tick level measurement of the lead-lag duration between cryptocurrencies: The case of bitcoin versus cardano, Investment Management and Financial Innovations*. Available at: https://www.businessperspectives.org/index.php/journals/investment-management-and-financial-innovations/issue-421/a-tick-by-tick-level-

measurement-of-the-lead-lag-duration-between-cryptocurrencies-the-case-of-bitcoin-versus-cardano (Accessed: 03 July 2023).

[56] Conway, L. (2023) *Cardano (ADA): What it is, how it differs from bitcoin*, *Investopedia*. Available at: https://www.investopedia.com/cardano-definition-4683961 (Accessed: 03 July 2023).

[57] Edinburgh, C.O.U. of *et al.* (2022) *Decentralization analysis of pooling behavior in cardano proof of stake: Proceedings of the third ACM International Conference on AI in Finance, ACM Other conferences*. Available at: https://dl.acm.org/doi/10.1145/3533271.3561787 (Accessed: 03 July 2023).

[58] Li, X. *et al.* (2022) *From bitcoin to Solana -- innovating blockchain towards enterprise applications*, *arXiv.org*. Available at: https://arxiv.org/abs/2207.05240 (Accessed: 03 July 2023).

[59] Solana, F. (2017) *Web3 infrastructure for everyone*, *Solana*. Available at: https://solana.com/es (Accessed: 03 July 2023).

[60] B, Mr.P. (2022) *What is Polygon (Matic)?*, *Medium*. Available at: https://medium.com/coinmonks/what-is-polygon-matic-4dd6b2e9cb8d (Accessed: 03 July 2023).

[61] Binance Academy, T. (2023) *What is Polygon (Matic)?*, *Binance Academy*. Available at: https://academy.binance.com/en/articles/what-is-polygon-matic (Accessed: 03 July 2023).

[62] Polygon, T. (2017) *Blockchains for mass adoption*. Available at: https://polygon.technology/ (Accessed: 03 July 2023).

[63] Aaron (2020) *Why Avax?*, *Why AVA*. Available at: https://web.archive.org/web/20200430143613/https:/www.avalabs.org/documents/why-ava (Accessed: 03 July 2023).

[64] Avalanche (2020) *Homepage: Avalanche dev docs*, *Homepage | Avalanche Dev Docs*. Available at: https://docs.avax.network/ (Accessed: 03 July 2023).

[65] Avax, F. (2020a) *Avalanche consensus*, *Avalanche Dev Docs*. Available at: https://docs.avax.network/learn/avalanche/avalanche-consensus (Accessed: 03 July 2023).

[66] Avax, F. (2020b) *What is a subnet?*, *Avalanche Support*. Available at: https://support.avax.network/en/articles/4064861-what-is-a-subnet (Accessed: 03 July 2023).

[67] Reiff, N. (2023) *What is Avalanche (AVAX), its pros, cons, and risks?*, *Investopedia*. Available at: https://www.investopedia.com/avalanche-avax-definition-5217374 (Accessed: 03 July 2023).

[68] Seq (2021) *Avalanche, a revolutionary consensus engine and platform. A game changer for Blockchain*, *Medium*. Available at: https://medium.com/avalanche-hub/avalanche-a-revolutionary-consensus-engine-and-platform-a-game-changer-for-blockchain-fdac008edc35 (Accessed: 03 July 2023).

[69] Binance Academy (2023) *What is the blockchain trilemma?*, *Binance Academy*. Available at: https://academy.binance.com/en/articles/what-is-the-blockchain-trilemma (Accessed: 03 July 2023).

[70] Cryptopedia , S. (2022) *Blockchain technology: Layer-1 and layer-2 networks*, *Gemini*. Available at: https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network (Accessed: 03 July 2023).

[71] Lapuschin, M. (2023) *What Is The Blockchain Trilemma?*, *What is the blockchain trilemma?* Available at: https://sensoriumxr.com/articles/what-is-the-blockchain-trilemma (Accessed: 03 July 2023).

[72] Qin, K., Zhou, L. and Gervais, A. (2021) *Quantifying blockchain extractable value: How dark is the forest?*, *arXiv.org*. Available at: https://arxiv.org/abs/2101.05511 (Accessed: 03 July 2023).

[73] *Blockchain scalability approaches: Chainlink* (2020) *Blockchain Scalability Approaches | Chainlink*. Available at: https://chain.link/education-hub/blockchain-scalability#:~:text=Blockchain%20scalability%20is%20the%20ability,are%20added%20to%20the%20network (Accessed: 03 July 2023).

[74] Kessler, S. (2023) *How the hunt for yet-to-exist tokens is Shaping Ethereum's layer 2 landscape*, *CoinDesk Latest Headlines RSS*. Available at: https://www.coindesk.com/tech/2023/04/26/how-the-hunt-for-yet-to-exist-tokens-is-shaping-ethereums-layer-2-landscape/ (Accessed: 03 July 2023).

[75] Malwa, S. (2023) *Ethereum Layer 2 network zksync ERA jumps to nearly $250m in locked value*, *CoinDesk Latest Headlines RSS*. Available at: https://www.coindesk.com/tech/2023/04/14/ethereum-layer-2-network-zksync-era-jumps-to-nearly-250m-in-locked-value/ (Accessed: 03 July 2023).

[76] Qiheng , Z. *et al.* (2020) *Solutions to scalability of Blockchain: A survey*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/8962150/ (Accessed: 03 July 2023).

[77] Takyar, A. (2023) *All about blockchain scalability solutions, LeewayHertz*. Available at: https://www.leewayhertz.com/blockchain-scalability-solutions/ (Accessed: 03 July 2023).

[78] Daley, S. (2022) *Blockchain, BuiltIn*. Available at: https://builtin.com/blockchain (Accessed: 03 July 2023).

[79] Hayes, A. (2023) *Blockchain facts: What is it, how it works, and how it can be used, Investopedia*. Available at: https://www.investopedia.com/terms/b/blockchain.asp (Accessed: 03 July 2023).

[80] Sultania, R. (2022) *What are the major limitations of blockchain technology, What Are The Major Limitations Of Blockchain Technology*. Available at: https://www.tutorialspoint.com/what-are-the-major-limitations-of-blockchain-technology#:~:text=A%20blockchain%20network%20is%20vulnerable,entitled%20to%20their%20personal%20space (Accessed: 03 July 2023).

[81] Yang, D. *et al.* (2020) *A review on scalability of Blockchain: Proceedings of the 2020 the 2nd International Conference on blockchain technology, ACM Other conferences*. Available at: https://dl.acm.org/doi/abs/10.1145/3390566.3391665 (Accessed: 03 July 2023).

[82] Group, T. (2022) *Soluciones de Seguridad de Blockchain, Thales*. Available at: https://cpl.thalesgroup.com/es/encryption/blockchain (Accessed: 03 July 2023).

[83] Santander, B. (2023) *'blockchain': El Baile Entre La Eficiencia y la seguridad, Web Corporativa Santander*. Available at: https://www.santander.com/es/stories/blockchain-eficiencia-vs-seguridad (Accessed: 03 July 2023).

[84] Adhikari, N. and Ramkumar, M. (2023) *IOT and Blockchain Integration: Applications, opportunities, and challenges, MDPI*. Available at: https://www.mdpi.com/2673-8732/3/1/6 (Accessed: 03 July 2023).

[85] Tanwar, S. *et al.* (2022) *Next Generation IoT and Blockchain Integration, hindawi*. Available at: https://downloads.hindawi.com/journals/js/2022/9077348.pdf (Accessed: 03 July 2023).

[86] iProUP (2022) *Estas Blockchain Quieren Destronar a ethereum: Cuáles son y qué hacen para lograrlo, Lo último*. Available at: https://www.iproup.com/economia-digital/20740-diez-blockchain-de-nueva-generacion-quieren-destronar-a-ethereum.amp (Accessed: 03 July 2023).

[87] DefiLlama (2023) *Total value locked all chains, DefiLlama*. Available at: https://defillama.com/chains (Accessed: 03 July 2023).

[88] Sun, Z. (2022) *Cardano se convirtió en la Criptomoneda Más desarrollada en github en 2021, Según Santiment, Cointelegraph*. Available at: https://es.cointelegraph.com/news/cardano-became-the-most-developed-crypto-on-github-in-2021-santiment (Accessed: 03 July 2023).

[89] DefiLlama (2023) *Total value locked in Solana, DefiLlama*. Available at: https://defillama.com/chains (Accessed: 03 July 2023).

[90] Messari (2023) *Crypto research, data, and Tools, Messari Crypto News*. Available at: https://messari.io/ (Accessed: 03 July 2023).

[91] etherscan (2023) *Ethereum (ETH) Blockchain Explorer - Etherscan, etherscan*. Available at: https://etherscan.io/ (Accessed: 03 July 2023).

[92] Blockchair (2023) *Universal blockchain explorer and search engine, Blockchair*. Available at: https://blockchair.com/ (Accessed: 03 July 2023).

[93] avascan (2023) *Avax explorer: Avascan, Avalanche Blockchain Explorer*. Available at: https://avascan.info/ (Accessed: 03 July 2023).

[94] Polygonscan.com (2023) *Polygon (Matic) Blockchain Explorer, Polygon (MATIC) Blockchain Explorer*. Available at: https://polygonscan.com/ (Accessed: 03 July 2023).

[95] Bitnodes (2023) *Bitnodes*. Available at: https://bitnodes.io/ (Accessed: 03 July 2023).

[96] Gas Station, E. (2023) *Eth Gas Station, ethgasstation.info*. Available at: https://ethgasstation.info/ (Accessed: 03 July 2023).

[97] Coin Metrics (2023) *Coin Metrics*. Available at: https://coinmetrics.io/ (Accessed: 03 July 2023).

[98] IntoTheBlock (2023) *On-chain crypto, Defi & NFT Analytics, IntoTheBlock*. Available at: https://app.intotheblock.com/ (Accessed: 03 July 2023).

[99] Staking Rewards (2023) *Crypto staking explorer, Staking Rewards*. Available at: https://www.stakingrewards.com/ (Accessed: 03 July 2023).

[100] Shrimpy , A. (2023) *What is Avalanche (AVAX)? the next defi blockchain explained, Shrimpy Academy: Stay Ahead of the Future*. Available at: https://academy.shrimpy.io/post/what-is-avalanche-avax-the-next-defi-blockchain-explained (Accessed: 03 July 2023).

[101] Klaytn (2022) *A comparison of Blockchain Network latencies, Medium*. Available at: https://medium.com/klaytn/a-comparison-of-blockchain-network-latencies-7508509b8460 (Accessed: 03 July 2023).

[102] cexplorer (2023b) *Cardano transactions per seconds (TPS) | cexplorer.io, cexplorer.io*. Available at: https://cexplorer.io/tps (Accessed: 03 July 2023).

[103] Today, U. (2023) *Cardano nears Max Capacity: What it means for investors, TradingView*. Available at: https://www.tradingview.com/news/u_today:fc19c1756094b:0-cardano-nears-max-capacity-what-it-means-for-investors/ (Accessed: 03 July 2023).

[104] cexplorer (2023a) *Cardano network usage | cardano explorer, cexplorer.io*. Available at: https://cexplorer.io/usage (Accessed: 03 July 2023).

[105] Barsby, O. (2023) *Cardano Hydra release date: When does cardano's layer-2 solution launch?, Cardano Hydra Release Date: When Does The Cardano Layer-2 Solution Launch?* Available at: https://www.gfinityesports.com/cryptocurrency/cardano-hydra-release-date-ada-layer-2-solution-launch-update-latest-news/ (Accessed: 03 July 2023).

[106] Subscan (2023) *Aggregate network high-precision Web3 Explorer, Subscan*. Available at: https://polkadot.subscan.io/block (Accessed: 03 July 2023).

[107] ethtps (2023) *ETHTPS, Live Ethereum TPS data*. Available at: https://ethtps.info/ (Accessed: 03 July 2023).

[108] ycharts (2023) *Ethereum network utilization, Ethereum Network Utilization*. Available at: https://ycharts.com/indicators/ethereum_network_utilization (Accessed: 03 July 2023).

[109] QuickNode (2023) *Comparison of latency across node providers in Ethereum, QuickNode Blog*. Available at: https://blog.quicknode.com/comparisons-of-latency-across-node-service-providers-in-ethereum/ (Accessed: 03 July 2023).

[110] Ycharts (2023) *Ycharts indicators BTC, Economic indicators*. Available at: https://ycharts.com/indicators (Accessed: 03 July 2023).

[111] miamiherald (2023) *Unleashing the power of cryptocurrency: Exploring ... , miamiherald*. Available at: https://www.miamiherald.com/software-business/article274817896.html (Accessed: 03 July 2023).

[112] Blockchain (2023) *Be early to the future of Finance, Blockchain.com*. Available at: https://www.blockchain.com/ (Accessed: 03 July 2023).

[113] PHEMEX (2023) *How many transaction per second can bitcoin process? Scalability Problem, Phemex*. Available at: https://phemex.com/blogs/what-is-transactions-per-second-tps (Accessed: 03 July 2023).

[114] CoinMarketCap (2021) *How long does a bitcoin transaction take?: CoinMarketCap, CoinMarketCap Alexandria*. Available at: https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take (Accessed: 03 July 2023).

[115] Solana Beach (2023) *Solana Beach, Dashboard*. Available at: https://solanabeach.io/supply (Accessed: 03 July 2023).

[116] Explorer solana (2023) *Explorer solana, Explorer.solana.com*. Available at: https://explorer.solana.com/ (Accessed: 03 July 2023).

[117] Dev Docs, A. (2020) *Cryptographic primitives, Avalanche Dev Docs*. Available at: https://docs.avax.network/specs/cryptographic-primitives (Accessed: 03 July 2023).

[118] Certik, S. (2023) *Blog - web3 security leaderboard, Blog - Web3 Security Leaderboard*. Available at: https://www.certik.com/resources (Accessed: 03 July 2023).

[119] HackenProof (2023) *Avalanche protocol: Program info, HackenProof*. Available at: https://hackenproof.com/avalanche/avalanche-protocol (Accessed: 03 July 2023).

[120] Santos, F. (2023) *What is SECP and how it drives cross-chain development on Cardano - IOHK, iohk.io*. Available at: https://iohk.io/en/blog/posts/2022/11/03/what-is-secp-and-how-it-drives-cross-chain-development-on-cardano/ (Accessed: 03 July 2023).

[121] Community (2023) *Cardano improvement proposals, CIP Cardano Improvement Proposals*. Available at: https://cips.cardano.org/cips/cip83/ (Accessed: 03 July 2023).

[122] Zimwara, T. (2022) *Cardano Foundation doubles reward offered to hackers for uncovering bugs on its blockchain – security bitcoin news, Bitcoin News*. Available at: https://news.bitcoin.com/cardano-foundation-doubles-reward-offered-to-hackers-for-uncovering-bugs-on-its-blockchain/ (Accessed: 03 July 2023).

[123] Candia, A. de (2020) *Cardano: The Blockchain had 11 vulnerabilities, The Cryptonomist*. Available at: https://en.cryptonomist.ch/2020/04/24/cardano-blockchain-vulnerabilities/ (Accessed: 03 July 2023).

[124] Cardanians. io (CRDNS (2021) *Cardano has undergone an independent source code audit*, *Medium*. Available at: https://cardanians-io.medium.com/cardano-has-undergone-an-independent-source-code-audit-a8941dc0e60b (Accessed: 03 July 2023).

[125] HackerOne (2023) *Cardano Foundation - Bug Bounty program*, *HackerOne*. Available at: https://hackerone.com/cardano-foundation?type=team (Accessed: 03 July 2023).

[126] Polkadot Wiki (2023) *Cryptography on polkadot*, *Polkadot Wiki*. Available at: https://wiki.polkadot.network/docs/learn-cryptography (Accessed: 03 July 2023).

[127] Admin (2023) *Polkadot escaped a significant loss: $200 million catastrophic bug*, *CoinUnited.io* . Available at: https://coinunited.io/news/en/2023-01-09/crypto/polkadot-escaped-a-significant-loss-200-million-catastrophic-bug/ (Accessed: 03 July 2023).

[128] Immunefi (2023) *Moonbeam, Astar, and Acala Library Truncation Bugfix Review - $1M payout*, *Medium*. Available at: https://medium.com/immunefi/moonbeam-astar-and-acala-library-truncation-bugfix-review-1m-payout-41a862877a5b (Accessed: 03 July 2023).

[129] Certik (2023) *Certik Web3 security, Web3 Security Leaderboard*. Available at: https://www.certik.com/ (Accessed: 03 July 2023).

[130] Bug Bounty (2023) *Bug Bounty Programme · Polkadot Wiki*, *Polkadot Wiki*. Available at: https://wiki.polkadot.network/docs/bug-bounty#:~:text=The%20bug%20bounty%20program%20does,%2C%20XCM%2C%20GRANDPA%2C%20etc. (Accessed: 03 July 2023).

[131] Gitbook (2023) *Elliptic curve cryptography (ECC), Elliptic Curve Cryptography (ECC) - Practical Cryptography for Developers*. Available at: https://cryptobook.nakov.com/asymmetric-key-ciphers/elliptic-curve-cryptography-ecc (Accessed: 03 July 2023).

[132] Gluhovsky, V. (2017) *EIP-627: Whisper specification, Ethereum Improvement Proposals*. Available at: https://eips.ethereum.org/EIPS/eip-627 (Accessed: 03 July 2023).

[133] Ethereum, F. (2023) *History and Forks of ethereum, ethereum.org*. Available at: https://ethereum.org/en/history/ (Accessed: 03 July 2023).

[134] H. and Rare Earth Magnets And Electronics Says: (2019) *History of ethereum security vulnerabilities, hacks, and their fixes, Applicature*. Available at: https://applicature.com/blog/blockchain-technology/history-of-ethereum-security-vulnerabilities-hacks-and-their-fixes (Accessed: 03 July 2023).

[135] ethereum, bug bounty (2023) *Ethereum Bug Bounty program, ethereum.org*. Available at: https://ethereum.org/en/bug-bounty/ (Accessed: 03 July 2023).

[136] Bitcoin wiki (2023) *Common vulnerabilities and exposures, Common Vulnerabilities and Exposures - Bitcoin Wiki*. Available at: https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures (Accessed: 03 July 2023).

[137] Kennedy, T. (2022) *Bitcoin hacked? it happened (twice), Medium*. Available at: https://medium.datadriveninvestor.com/itcoin-unhackable-it-happened-twice-not-blowing-smoke-9e16bcddd5ab (Accessed: 03 July 2023).

[138] Miller Danika and Ullman (2023) *Crypto Hacks & Historical Cryptocurrency exploits, Milk Road*. Available at: https://milkroad.com/hacks (Accessed: 03 July 2023).

[139] Solana Program (2023) *Encryption, Solana Program Library Docs*. Available at: https://spl.solana.com/confidential-token/deep-dive/encryption (Accessed: 03 July 2023).

[140] Certik (2023b) *What is Solana? , What is Solana? - Blog - Web3 Security Leaderboard*. Available at: https://www.certik.com/resources/blog/6FXjQJLF2kQoAOnwIedhDX-what-is-solana (Accessed: 03 July 2023).

[141] Certik (2023a) *2022 Solana Exploits Overview , 2022 Solana Exploits Overview - Blog - Web3 Security Leaderboard*. Available at: https://www.certik.com/resources/blog/v2PsJKL9GBWhfD05rrAZ1-2022-solana-exploits-overview (Accessed: 03 July 2023).

[142] Vincent, J. (2022) *Solana ecosystem hit by Hack draining millions in crypto from 8,000 hot wallets, The Verge*. Available at: https://www.theverge.com/2022/8/3/23290149/solana-ecosystem-blockchain-attack-hack-wallets-phantom-slope-supply-chain (Accessed: 03 July 2023).

[143] HackenProof (2023) *Hackenproof, HackenProof*. Available at: https://hackenproof.com/public-bug-bounty-list/solana-bug-bounty-program (Accessed: 03 July 2023).

[144] Avalanche (2023) *Whitepapers, Ava Labs*. Available at: https://www.avalabs.org/whitepapers (Accessed: 03 July 2023).

[145] Cexplorer (2023) *Cardano explorer | stake pools, cexplorer.io*. Available at: https://cexplorer.io/ (Accessed: 03 July 2023).

[146] whitepapers, C. (2017) *Cardano Ada, Cardano ADA whitepapers*. Available at: https://whitepaper.io/coin/cardano (Accessed: 03 July 2023).

[147] Subscan, P. (2023) *Aggregate network high-precision Web3 Explorer, Subscan*. Available at: https://polkadot.subscan.io/validator (Accessed: 03 July 2023).

[148] Polkadot Network (2017) *Whitepaper: Polkadot, Polkadot Network*. Available at: https://polkadot.network/whitepaper/ (Accessed: 03 July 2023).

[149] Polkadot Wiki (2023) *Validator on polkadot, Polkadot Wiki*. Available at: https://wiki.polkadot.network/docs/learn-validator (Accessed: 03 July 2023).

[150] Polygon Staking (2023) *Polygon staking, Polygon Staking*. Available at: https://staking.polygon.technology/ (Accessed: 03 July 2023).

[151] Beaconscan (2023) *Mainnet chain explorer, beaconscan.com*. Available at: https://beaconscan.com/ (Accessed: 03 July 2023).

[152] Ethernodes (2023) *Ethereum Mainnet statistics, The Ethereum Network & Node Explorer*. Available at: https://www.ethernodes.org/countries (Accessed: 03 July 2023).

[153] Clementín, F. (2022) *¿Por qué se necesitan 32 eth para ser validador en ethereum 2.0?, CriptoNoticias*. Available at: https://www.criptonoticias.com/tecnologia/por-que-necesitan-32-eth-ser-validador-ethereum-20/#:~:text=A%20d%C3%ADa%20de%20hoy%2C%20los,aumento%20desde%20hace%20un%20a%C3%B1o. (Accessed: 03 July 2023).

[154] Solana Beach (2023) *Solana Beach, Validators Dashboard*. Available at: https://solanabeach.io/validators (Accessed: 03 July 2023).

[155] Solana , F. (2023) *Validator requirements, Solana Docs*. Available at: https://docs.solana.com/es/running-validator/validator-reqs#:~:text=Minimum%20SOL%20requirements%E2%80%8B,exempt%20reserve%20of%200.02685864%20SOL. (Accessed: 03 July 2023).

[156] Quarmby, B. (2022) *Los Desarrolladores de Solana Corrigen los bugs de la red con la esperanza de evitar nuevas interrupciones, Cointelegraph*. Available at: https://es.cointelegraph.com/news/solana-developers-tackle-bugs-hoping-to-prevent-further-outages (Accessed: 03 July 2023).

[157] Yang, J. (2022) *Solana Falls and speculation centers on links to Sam Bankman-Fried's FTX, Alameda, CoinDesk Latest Headlines RSS*. Available at: https://www.coindesk.com/markets/2022/11/07/solana-falls-and-speculation-centers-on-links-to-sam-bankman-frieds-ftx-alameda/ (Accessed: 03 July 2023).

[158] United Nations (2000) *Objetivos y Metas de Desarrollo Sostenible - Desarrollo Sostenible*, *United Nations*. Available at: https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/ (Accessed: 03 July 2023).

[159] G, A. (2023) *Polygon (Matic) crypto: Everything you need to know*, *Geekflare*. Available at: https://geekflare.com/polygon-matic-crypto/ (Accessed: 03 July 2023).

[160] Polygon Wiki (2023) *Polygon Wiki*. Available at: https://wiki.polygon.technology/docs/develop/wallets/portis/ (Accessed: 03 July 2023).

[161] Quarmby, B. (2021) *Polygon upgrade quietly fixes bug that put $24b of Matic at risk*, *Cointelegraph*. Available at: https://cointelegraph.com/news/polygon-upgrade-quietly-fixes-bug-that-put-24b-of-matic-at-risk (Accessed: 03 July 2023).

[162] Nair, P. and Ross, R. (2021) *Polygon bug put $23 billion in cryptocurrency at risk*, *Bank Information Security*. Available at: https://www.bankinfosecurity.com/polygon-bug-put-23-billion-in-cryptocurrency-at-risk-a-18224 (Accessed: 03 July 2023).

[163] Immunefi (2023) *Polygon double-spend bug fix postmortem - $2M Bounty*, *Medium*. Available at: https://medium.com/immunefi/polygon-double-spend-bug-fix-postmortem-2m-bounty-5a1db09db7f1 (Accessed: 03 July 2023).

[164] Polygon Bug Bounty (2023) *Bug Bounty program*, *Polygon Wiki*. Available at: https://wiki.polygon.technology/docs/contribute/bug-bountry-program/#:~:text=The%20bounty%20program%20is%20to,to%20%245%2C000%20for%20critical%20issues (Accessed: 03 July 2023).

[165] Kibo, B. (2021) *Introducción a blockchain: Crea Tus propios Bloques con javascript*, *BBVA Next Technologies*. Available at: https://www.bbvanexttechnologies.com/blogs/introduccion-a-blockchain-crea-tus-propios-bloques-con-javascript/ (Accessed: 05 July 2023).

[166] N., J.L.M. and Herrera, E.J.C. (2019) *Tecnologías Blockchain y sus aplicaciones*, *Visión Antataura*. Available at: http://portal.amelica.org/ameli/jatsRepo/225/225971010/html/index.html (Accessed: 05 July 2023).

[167] Finance , M.S. (2022) *Soft Fork vs hard fork: What are the differences?*, *Financial and Business News | Finance Magnates*. Available at: https://www.financemagnates.com/cryptocurrency/education-centre/soft-fork-vs-hard-fork-what-are-the-differences/ (Accessed: 05 July 2023).

[168] btc (2019) *Dive into anything*, *Reddit*. Available at: https://www.reddit.com/r/CryptoCurrency/comments/e1sjue/a_map_of_the_major_bitcoin_forks/ (Accessed: 05 July 2023).

[169] Okx (2023) *Entendiendo el trilema de la blockchain: Guía Para Principiantes*, *OKX*. Available at: https://www.okx.com/es-es/learn/blockchain-trilemma-guide (Accessed: 05 July 2023).

[170] Token Terminal (2023) *Token Terminal*. Available at: https://tokenterminal.com/terminal (Accessed: 05 July 2023).

[171] CryptoDiffer (2023) *CryptoDiffer*. Available at: https://cryptodiffer.com/ (Accessed: 05 July 2023).