UACM

Universidad Autónoma
de la Ciudad de México

NADA HUMANO ME ES AJENO

COLEGIO DE CIENCIA Y TECNOLOGÍA
LICENCIATURA EN INGENIERÍA EN SISTEMAS
ELECTRÓNICOS Y DE TELECOMUNICACIONES

Aula virtual de aprendizaje de Blockchain para los estudiantes de la UACM

T E S I S

QUE PARA OPTAR POR EL TÍTULO DE

LICENCIADO EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

P R E S E N T A

JOEL ALEJANDRO GARCIA ESCOBAR

D I R E C T O R

MTRO. ENRIQUE CRUZ MARTÍNEZ

Ciudad de México, noviembre de 2024.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Índice general

Agradecimientos

Agradezco sinceramente a todas las personas e instituciones que hicieron posible la realización de este trabajo de investigación. Aquellos que siempre estuvieron a mi lado brindándome ánimo y comprensión durante los momentos difíciles y que además me dieron su orientación experta, paciencia y apoyo constante a lo largo de este proceso. Cada uno de ustedes ha dejado una marca indeleble en este trabajo y estaré siempre agradecido por su contribución.

Resumen

En esta tesis se lleva a cabo una investigación exhaustiva sobre los conceptos fundamentales de la tecnología Blockchain. Se introduce al lector en sus principios básicos, explorando sus orígenes y la evolución que ha experimentado a lo largo del tiempo. Además, se ofrece una introducción y definición de los Contratos Inteligentes, así como sus aplicaciones prácticas en diversos sectores. Se establecen las bases para comprender la criptografía aplicada a Blockchain, explicando su funcionamiento en el contexto de las transacciones y la seguridad de los datos.

Asimismo, se investiga el potencial de Blockchain en la intersección con otras tecnologías emergentes, como la Inteligencia Artificial, el Internet de las Cosas y el Big Data. Se examinan sus aplicaciones en áreas específicas como la manufactura y la salud, y se discuten las limitaciones que enfrenta esta tecnología, tanto en el ámbito legal como en el tecnológico. Este análisis proporciona una visión integral de las oportunidades y desafíos que presenta Blockchain en el contexto actual.

Para llevar a cabo esta investigación, se crea un aula virtual que consta de tres módulos diseñados para ofrecer a los estudiantes un curso básico sobre Blockchain. Esta plataforma se fundamenta en los tres primeros capítulos de la investigación, proporcionando un recurso educativo accesible y estructurado. Se implementan rúbricas de evaluación que permiten medir el progreso de los estudiantes de manera efectiva, y la plataforma se diseña utilizando Moodle, conforme al estándar EC 217.01.

Durante el proceso de implementación, surgieron diversas complicaciones; algunas pudieron resolverse, mientras que otras no. Se documentaron meticulosamente cada una de las observaciones encontradas, lo que permitirá mejorar futuras ediciones del curso y optimizar la experiencia de aprendizaje.

Introducción

En la actualidad, los avances tecnológicos se producen a un ritmo vertiginoso, transformando no solo nuestra forma de vivir y comunicarnos, sino también la manera en que nos relacionamos en diversas esferas de la vida cotidiana. Sin embargo, este progreso trae consigo desafíos significativos que deben ser abordados. Entre ellos se destacan la falta de conocimiento sobre tecnologías emergentes, la escasez de talento técnico para desarrollar soluciones efectivas y la resistencia al cambio, que constituye uno de los mayores obstáculos para la adopción de nuevas tecnologías.

El concepto de blockchain tiene sus raíces en ideas que surgieron en 1991, cuando se propuso crear un registro digital de archivos ordenados cronológicamente. Esta idea inicial permitió un registro preciso de información, como la propiedad y la fecha de creación de los archivos. Sin embargo, fue en 2008, con el lanzamiento de Bitcoin (la primera criptomoneda basada en algoritmos avanzados y un poder computacional significativo) que la tecnología blockchain comenzó a captar la atención del público general y a demostrar su potencial.

A lo largo de los últimos años, blockchain ha ganado popularidad no solo como una herramienta destinada a facilitar transacciones digitales, sino también como un sistema capaz de revolucionar diversas industrias. Sin embargo, a pesar de sus múltiples beneficios, enfrenta limitaciones inherentes a las tecnologías emergentes, como la escalabilidad, la eficiencia energética y cuestiones de seguridad que aún necesitan ser resueltas. Además, Blockchain enfrenta desafíos técnicos y sociales significativos que deben ser abordados para su adopción generalizada, incluyendo el problema del doble gasto y el ataque del 51 %.

En esta tesis, se exploran en profundidad los conceptos básicos de Blockchain, abarcando conceptos desde su origen y evolución hasta su estado actual. Se desglosa detalladamente su funcionamiento, así como los principios de la criptografía que garantizan su seguridad y transparencia. Además, se examinan aplicaciones innovadoras, como los contratos inteligentes (Smart Contracts), que permiten la automatización de procesos sin la necesidad de intermediarios. También se exploran otros usos en áreas emergentes como el Internet de las cosas, la inteligencia artificial y el Big Data.

Este proyecto busca expandir el conocimiento académico sobre blockchain mediante la creación de una comunidad virtual para estudiantes de la UACM. A través de un servidor dedicado en Moodle, se pretende facilitar una exploración profunda y comprensiva de esta revolucionaria tecnología en un entorno colaborativo y accesible. Este espacio es un hub de conocimiento, donde se comparte información esencial sobre los fundamentos de blockchain, lo que facilitará un aprendizaje dinámico y participativo.

Dentro de esta comunidad, se abordan conceptos esenciales que comienzan con una introducción a la historia y evolución de blockchain, permitiendo a los estudiantes comprender cómo ha llegado a convertirse en una herramienta clave en la era digital. A medida que avancemos, profundizaremos en los principios de criptografía, proporcionando definiciones clave que ayudarán a los estudiantes a apreciar la importancia y aplicabilidad de esta disciplina en la seguridad de Blockchain.

Además, el curso incluye un análisis detallado de cómo funciona blockchain en la práctica, desglosando su arquitectura y los procesos que permiten su operatividad. Esto garantizará que los estudiantes adquieran un conocimiento básico de sus componentes fundamentales, su arquitectura y su funcionamiento en diversos contextos.

Es importante destacar que el aula virtual estará alineada con el estándar de Competencia Conocer EC 217.01, lo que asegura que los contenidos ofrecidos sean pertinentes, actualizados y de alta calidad. A través de este enfoque, promovemos un aprendizaje significativo y relevante en la era digital, la colaboración y el intercambio de ideas dentro de esta comunidad serán esenciales para enriquecer la experiencia educativa y fomentar un modelo de aprendizaje.

A través de esta tesis, se busca ofrecer una visión integral de la tecnología blockchain, sus beneficios, y las barreras que aún persisten en su camino hacia el futuro, destacando la importancia de un enfoque colaborativo en la educación para enfrentar los desafíos del mundo tecnológico en constante evolución.

Capítulo 1

Introducción a Blockchain

La tecnología de hoy en día ha crecido de manera acelerada a diferencia de años anteriores, trayendo un gran impacto positivo en el desarrollo y la innovación de muchas industrias como la comercialización, la salud, la política y la seguridad de la información, por mencionar algunas. La tecnología Blockchain, otorga diversas aplicaciones que permiten mejorar los procesos que se llevan a cabo en la mayoría de estas industrias. Esto ha permitido que se despierte el interés por su tecnología, su impacto, su efectividad, su seguridad, sus beneficios y su impacto dentro de la tecnología.

Blockchain permite solucionar un gran problema que ha crecido bastante dentro de internet. Este problema es la confianza en las transacciones y los sistemas de intercambio de activos que no requieren de la intervención del mundo real para funcionar. Esto permite llevar más allá cualquier modelo de negocio que se desee implementar dentro del mundo digital.

1.1. Concepto de Blockchain

Blockchain se define como una tecnología que lleva a cabo un registro distribuido donde los usuarios participantes dentro de la red, conocidos como nodos, obtienen su propia copia de este. Esta arquitectura lleva a cabo un sistema de transacciones descentralizadas a nivel de internet, y cada vez que se realiza una transacción nueva esta se añade automáticamente al registro para cada uno de los nodos, es decir, se actualizan todas y cada una de las copias.

Partiendo de esto, Blockchain se define como un libro programable o base de datos, criptográficamente seguro y disponible para todos los usuarios que lo deseen. Esta manera de mantenerlo compartido es lo que lo hace confiable, no puede ser controlado por un usuario en particular ya que este registro puede ser inspeccionado por cualquiera. Esto último significa que Blockchain utiliza una red descentralizada compartida que no se controla por una autoridad central, su base de datos no se encuentra en un solo lugar sino que reside en varios sitios de internet. Cuando se realiza una nueva transacción, esta se almacena en el registro en orden cronológico de manera pública, actualizando así todas las copias de los nodos. El registro es lo que se conoce como cadena de bloques. Cuando hay nuevos detalles o transacciones estas se codifican y se validan de manera independiente por los nodos, después de esto se actualizan los datos en un bloque y se quedan en el registro de la base de datos de manera permanente.

Blockchain, por lo tanto, es una tecnología que cuenta con una serie de transacciones digitales que se registran dentro del sistema y se agrupan a manera de ”bloques”de información que comparten de manera segura la información entre los diferentes nodos dentro de la misma red. Cuando se genera una nueva transacción, se suma un bloque y una vez validado se encadena a la cadena de bloques general, fortaleciendo y actualizando la información de la red Blockchain de manera segura, transparente e inmutable para todos los nodos de la red. (Network, 2020)

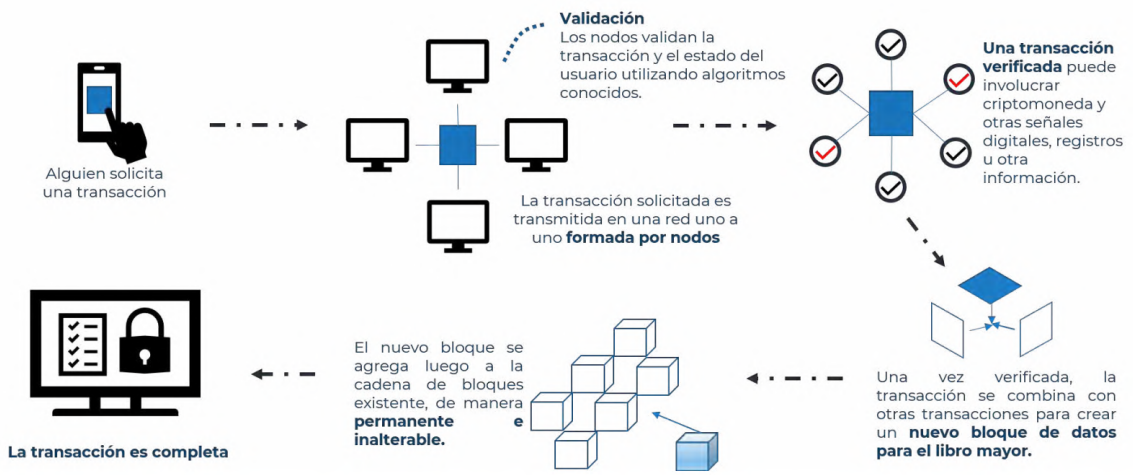


Figura 1.1: Función de Blockchain como registro distribuido (CertiProf, 2021).

1.2. Origen de la tecnología Blockchain

A nivel general, internet facilitó mucho el intercambio de información con la llegada de la web 2.0. Sin embargo, pese a que se tenían grandes y diversos repositorios de información como YouTube, Google y Amazon internet ha carecido de medios de pago, ya que algunas asociaciones y estructuras corporativas no permitían la separación del mundo digital y el mundo real. Internet no tenía una moneda digital propia, ni notarios propios que facilitaran sus transacciones. (Joaquín López Lérida, 2016)

Desde la década de los 90 se propusieron soluciones descentralizadas para realizar pagos electrónicos que no dependieran de la intervención de ninguna entidad central o supervisora. En 1991 apareció el primer trabajo de cadena de bloques que utilizaba la criptografía, Stuart Haber y W. Scott Stornetta presentaron el primer concepto de una cadena de bloques asegurada criptográficamente. Este trabajo sentó las bases para la tecnología de Blockchain al introducir un sistema que permitía proteger la inmutabilidad de los registros digitales (Baggetta, 2022). Posteriormente en 1998 dos grandes criptógrafos desempeñaron cambios importantes dentro de la criptografía. Wei Dai un reconocido criptógrafo y miembro de la comunidad cypherpunk [1] utilizó una solución descentralizada para pagos electrónicos empleando la criptografía de clave pública (Navarro, 2023) mientras que Nick Szabo, un pionero en criptografía, trabajó en ”bit gold”, un precursor de las criptomonedas modernas que utilizaba una cadena de bloques para asegurar las transacciones sin necesidad de una autoridad central. Esta propuesta fue otro paso significativo hacia la creación de sistemas de pago sin intermediarios. Para el año 2000, Stefan Konst publicó un artículo detallando teorías sobre cadenas aseguradas criptográficamente y su implementación, contribuyendo al desarrollo de los sistemas de cadena de bloques y sentando más bases teóricas para esta tecnología emergente (Baggetta, 2022). El verdadero punto de inflexión llegó en 2008, cuando una persona o grupo bajo el pseudónimo de Satoshi Nakamoto publicó el artículo ”Bitcoin: A Peer-to-Peer Electronic Cash System”. Este documento definió el uso del Blockchain para realizar transacciones en una red Peer to peer: (de igual a igual), marcando el inicio de la primera criptomoneda: Bitcoin:.

En 2009, Satoshi Nakamoto minó el primer bloque de Bitcoin, conocido como el bloque génesis, marcando la implementación práctica del Blockchain como un libro mayor público para las transacciones de Bitcoin. Esta innovación permitió la creación de una red de nodos que validaban y registraban transacciones sin la necesidad de una entidad central, lo que con el tiempo popularizó esta red y sentó las bases para el desarrollo de nuevas aplicaciones y criptomonedas basadas en la tecnología Blockchain.

En 2014, se produjo un avance significativo con el lanzamiento de Blockchain 2.0, que separó la

[1] Cypherpunks son una comunidad de activistas que emplea la criptografía de forma no violenta para alcanzar un cambio político y social (Zimmermann, 2013).

tecnología Blockchain de Bitcoin, permitiendo su uso en otras transacciones financieras e interorganizacionales. Este año también marcó el nacimiento del proyecto Ethereum, que amplió las capacidades de la tecnología Blockchain al introducir contratos inteligentes (smart contracts). Estos contratos permitieron la programación de transacciones automáticas y más complejas, expandiendo significativamente las aplicaciones de la tecnología Blockchain (Baggetta, 2022).

1.2.1. Atributos Clave

En esta sección se explicarán algunas de las propiedades clave que conforman a la tecnología Blockchain:

Atributos	**Definición**
Transparencia	El registro completo de transacciones está disponible gracias a las copias mantenidas por cada nodo. Este registro, conocido como libro mayor distribuido, varía en su disponibilidad según sea privado o público, proporcionando transparencia a todos los usuarios al revelar todas las transacciones históricas.
Confianza	Se promete una sólida seguridad sin depender de una autoridad central debido a la inmutabilidad, criptografía y administración de las transacciones realizadas.
Inmutabilidad	Una vez realizadas y registradas, las transacciones dentro de la cadena de bloques no pueden ser alteradas o eliminadas. Para corregir cualquier error, se debe generar un nuevo bloque.
Seudonimato	Los usuarios que formen parte de Blockchain no utilizarán sus datos personales. Ya que al implementar un sistema criptográfico los datos de los usuarios participantes son anónimos.
Verificación	Todas las transacciones generadas son completamente comprobables en tiempo real por los nodos, una vez que se valida su legitimidad se registra en la cadena de bloques.
Seguridad	Los algoritmos criptográficos protegen los datos de las transacciones ante intrusiones con intenciones de destrucción o modificación de los mismos.
Eliminación de intermedios	Dado que no existe una entidad central que deba aprobar las transacciones, el proceso se agiliza bastante gracias a los procesos de la red ditribuida.

Cuadro 1.1: Atributos Blockchain.

1.3. Evolución hasta la actualidad

Por cuestiones de organización, los distintos tipos de actividades existentes y potenciales en la revolución industrial de Blockchain se dividen en tres categorías; para empezar Blockchain 1.0 se refiere al despliegue de la criptomoneda, la transferencia de divisas, las remesas y sistemas de pago digital. Blockchain 2.0 se refiere a los contratos, es decir, a las aplicaciones económicas, del mercado y financieras que van más allá de transacciones monetarias tales como; bonos, préstamos, hipotecas, propiedades y contratos inteligentes.

Por último, Blockchain 3.0 va más allá de las transacciones y las finanzas. Ya que tiene aplicaciones en el área gubernamental, de salud, ciencia, literatura, cultura y arte por mencionar algunas. (Swan, 2015) A continuación, se explicarán más a detalle las tres categorías que dieron paso a la evolución de Blockchain.

1.4. Blockchain 1.0: El inicio con Bitcoin

Blockchain se utiliza a menudo de forma incorrecta indistintamente con Bitcoin. Aunque fue el primer uso de Blockchain, es sólo una aplicación de cómo se puede utilizar el libro mayor para almacenar

información. (Network, 2020)

1.4.1. Bitcoin

El término Bitcoin es en esencia dinero o moneda digital denotado como BTC. Fue creado en 2009 en el artículo de una entidad anónima bajo el alias de Satoshi Nakamoto, en donde se proponía un sistema de pagos en línea utilizando técnicas de encriptación tanto en la generación de divisas (BTC) como en la verificación de las transacciones realizadas sin depender de ninguna entidad o banco central. Además, todas las transacciones realizadas serían registradas y publicadas en internet. Estas monedas digitales, además de ser utilizadas para realizar transacciones digitales entre dos usuarios también se puede emplear como recompensa por el trabajo de procesamiento computacional que realizan los mineros, aquellos que ofrecen su potencia computacional para validar y registrar todos los pagos realizados dentro de Blockchain. Los usuarios pueden realizar transacciones con bitcoin mediante una billetera digital desde su computadora personal, teléfono móvil o aplicación web. (Swan, 2015)

De acuerdo con este artículo, Bitcoin se dio a conocer como una transformación fundamental del dinero. Al funcionar de manera descentralizada se administra únicamente por el consenso, empoderando así su valor de modo que el dinero solo pertenece al usuario y nadie más tiene dominio sobre él.

1.4.2. Funcionamiento de bitcoin

Tal y como se mencionó anteriormente, Blockchain es un registro general público de todas las transacciones de Bitcoin que se han ejecutado, aumenta conforme los mineros añaden nuevos bloques en aproximadamente 10 minutos cada transacción. Cada bloque tiene un complemento cronológico y cada cliente cuenta con su propia copia. Los mineros reciben una recompensa que se traduce en Bitcoins. Los componentes de Bitcoin se pueden definir como; desarrolladores de software, mineros, servicios de procesamiento comercial, empresas de monederos web y los usuarios consumidores. (Swan, 2015)

Desde el punto de vista de un usuario, los elementos necesarios para una transacción de Bitcoin son:

- Dirección. Corresponde a la dirección a la que otros enviarán los Bitcoin.
- Clave privada. Es el secreto criptográfico mediante el cual envían Bitcoin a otros usuarios.
- Billetera digital. Es el software de billetera que ejecuta el usuario en su propia computadora o cualquier dispositivo inteligente para administrar su Bitcoin. Además, este software puede conservar una copia de Blockchain, permitiendo obtener el registro en tiempo real de todas las transacciones realizadas con esta moneda, manteniendo el esquema descentralizado de verificación de transacciones.

1.4.3. Aceptación comercial de bitcoin

De acuerdo al director de Cryptocity.press [2] Sergio Morales, en el año 2022 el mercado se vió afectado por varios eventos negativos propios, tales como el colapso de la moneda estable UST [3], la quiebra de FTX [4] a finales de año y el desplome del Bitcoin en un aproximado del 65 % de su valor.

Para el año 2023 Morales mencionó que se esperaba una fuerte solidificación monetaria en los bancos centrales en distintos países dependiendo de la inflación. Además, aseguró que la previsión de reglas claras para los años posteriores ocasionaría que más empresas e instituciones se interesen por la tecnología Blockchain, lo que estimula el crecimiento general del ecosistema y, considerando el piso desde donde parten los criptomercados, pueden resultar unas condiciones muy atractivas para los inversores que quieran posicionarse a largo plazo, en precios muy por debajo respecto del año pasado. (Rial, 2023)

[2] Cryptocity.press es un agregador de noticias algorítmico que identifica las tendencias del mercado criptográfico

[3] UST es una criptomoneda estable diseñada con el fin de operar en diferentes Blockchain (López, 2022b)

[4] FTX es un exchange en donde varias instituciones compran o venden criptoactivos, tokens, NFTs etc (Contreros, 2022).

De acuerdo al comunicado No. 039 párrafo 3 del Banco de México publicado en 2021; *"Las instituciones financieras del país no están autorizadas a realizar y ofrecer al público operaciones con activos virtuales, tales como Bitcoin, Ether, XRP y otros con el fin de mantener una sana distancia entre estos y el sistema financiero."* ("Comunicado No. 039 Banco de México, SHCP y CNBV advierten sobre riesgos de utilizar activos virtuales.", 2021)

Sin embargo, pese a que aún no se ha reconocido a las criptomonedas como divisa de circulación legal en nuestro país no significa que no se puedan realizar transacciones con estas y mucho menos que su uso sea ilegal. Ya que en México en lo que llevamos de este año existen alrededor de 100 establecimientos y empresas que aceptan el bitcoin y otras criptomonedas como método de pago, entre estas destacan Elektra y Rappi. Los usos que normalmente se dan son el holding, que se basa en comprar Bitcoin cuando esta baja de precio y venderlo cuando su valor aumenta, y el otro está en compras cotidianas. (Insider, 2023)

1.5. Blockchain 2.0: Más allá de las criptomonedas

Anteriormente se mencionó una aplicación importante para Blockchain, sin embargo, Bitcoin sólo fue la primera parte de lo que se vendría. Ya que esto dió paso a que se den otras aplicaciones con ayuda de esta tecnología. Transacciones de depósito en garantía, contratos en garantía, arbitraje de terceros, firma de múltiples partes, etc. La llegada de Blockchain 2.0 brindó un enfoque más allá que sólo criptomonedas, al tener un espacio más amplio en desarrollo se amplió el número de categorías, distinciones, estándares y clasificaciones de su uso. De hecho, parte de su terminología hace referencia a los protocolos de Bitcoin 2.0, los cuales están conformados por contratos inteligentes, propiedades inteligentes, Aplicaciones Descentralizadas (Dapps), Organizaciones Autónomas Descentralizadas (DAO) y las Corporaciones Autónomas Descentralizadas (DAC).

Blockchain 2.0 permite una descentralización de los mercados en general, es decir, que brinda la oportunidad de que se pueda utilizar en mercados que no sólo se limiten a dinero y activos. Tales como registrar, confirmar y transferir todo tipo de contratos y hasta propiedades. Las transacciones financieras podrían transformarse o reinventarse con ayuda de Blockchain, como las acciones, capital privado, instrumentos de crowdfunding [5], fondos y bonos, pensiones, anualidades y muchos derivados más.

Otros elementos que pueden migrar a la tecnología Blockchain son los registros públicos, tales como; títulos de propiedad, títulos de terrenos, registros de automóviles, actas de matrimonio y defunción, y licencias comerciales. La identidad digital se puede confirmar más fácilmente con ayuda de licencias de conducir, tarjetas de identidad y pasaportes. Se pueden almacenar registros privados como préstamos, contratos, firmas, pagarés, depósitos de garantía y testamentos.

Además, Blockchain también facilita los trámites de testimonios y constancias, como pruebas de seguros, de propiedades y documentos notariales (Swan, 2015).

1.5.1. Mercados de predicción de Bitcoin

Estos ofrecen la posibilidad de brindar resultados en base a esta herramienta en el mundo real, es decir, nos permiten saber lo que piensan los expertos sobre el camino actual y futuro de Bitcoin, sus precios, su demanda y también los problemas de la industria como el desarrollo técnico de Bitcoin, posibles bifurcaciones, cambios y aumentos de dificultad en el algoritmo de minería etc. También funcionan como una fuente confiable de información sobre la industria Blockchain en desarrollo actual y futuro.

[5] Crowdfunding es una fuente de financiación para empresas pequeñas en proyectos musicales, artísticos, películas, y campañas políticas o empresariales (Sevilla, 2020).

1.5.2. Propiedades inteligentes

Se define como propiedad inteligente a aquella transacción cuyas propiedades se basen en todos los modelos basados en Blockchain. Esta propiedad puede estar conformada por activos tangibles del mundo físico, tales como un automóvil, un equipo de cómputo, una bicicleta o hasta una casa. Los activos intangibles como las patentes, las marcas registradas, derechos de autor o nombres de dominio también se pueden adaptar a esta tecnología. Esto último, por ejemplo, se puede lograr codificando una idea en un bloque de la cadena, una vez almacenada la información esta será registrada con un sello de fecha y hora de forma permanente.

El objetivo de la propiedad inteligente está en tener control sobre sus activos una vez que se hayan registrado como activo digital dentro de Blockchain. Cualquier activo puede registrarse, y el propietario de esta será el que cuente con la clave privada. Si se desea vender el activo, el antiguo propietario deberá transferir la clave privada a otra parte. Por ejemplo, en la compra de un vehículo un contrato inteligente preestablecido sería capaz de transferir la propiedad de este desde la compañía financiera al propietario cuando se hayan concluido todos los pagos del préstamo. Esto permite que se tenga la confianza suficiente por parte del usuario, ya que, como se mencionó anteriormente si se han cumplido la totalidad de los pagos esto será comprobable ya que no se puede eliminar ningún registro una vez dentro de la cadena. La propiedad inteligente, por tanto, es aquella cuyo mandato o titularidad se controla a través de Blockchain, mediante contratos sujetos a la legislación vigente. Esto será llevado a cabo con los contratos inteligentes, aquellos contratos cuyas propiedades van más allá de simples transacciones basadas en Blockchain, tema que se mencionará más a detalle en el capítulo 4.

1.5.3. Proyectos de protocolo Blockchain 2.0

Hay una gran variedad de proyectos en desarrollo que bien podrían aprovechar esta tecnología, sin embargo, en este capítulo vamos a centrarnos únicamente en dos de ellos:

- Desarrollo de billetera. Las billeteras son un elemento fundamental para el empleo de criptomonedas como Bitcoin, ya que estas permiten la tenencia y transferencia segura de la criptomoneda o cualquier activo que requiera la criptografía.

- Plataformas de desarrollo y API:s. Actualmente existe gran variedad de empresas de plataformas que ofrecen herramientas que facilitan a los desarrolladores la elaboración de aplicaciones mediante APIs. Por ejemplo; Blockchain.info utiliza un software de billetera electrónica para realizar transacciones digitales, Stellar es una plataforma de registro público semidescentralizada (no es mantenida por mineros) vinculada a la red de pago Stripe [6], una plataforma de procesamiento de pagos por internet.

1.5.4. Dapps

Las aplicaciones descentralizadas (Dapps) forman una parte importante dentro de Blockchain. Algunas de sus características más destacables son; están escritos en código abierto, no requieren de ninguna entidad que las controle, cuando se realiza una acción que aporte valor a la Dapp por parte de algún desarrollador se recompensará con tokens provenientes de la misma aplicación. Un ejemplo muy claro de estas aplicaciones es Bitcoin, la primera Dapp creada por Satoshi Nakamoto. Como se ha mencionado anteriormente, Bitcoin no requiere de ninguna entidad central que permita su funcionamiento o aprobación, se puede definir como el Token: que utiliza la Dapp. Y este puede utilizarse dentro de esta mediante Blockchain.

Por lo tanto, una Dapp se define como una aplicación de código abierto cuyo funcionamiento se basa en generar y emplear tokens que se almacenan dentro de Blockchain. Si un usuario quiere utilizar una Dapp, tendrá que adquirir tokens de la misma para utilizarla. Si la demanda de tokens aumenta, su valor

[6] Stripe es una plataforma de pagos en línea que facilita y protege la gestión de pagos minoristas a través de internet (Dobaño, 2023).

también lo hará trayendo más beneficios para sus usuarios ya que estos podrán vender sus tokens cuando tengan más valor a comparación de su adquisición. (Joaquín López Lérida, 2016)

El funcionamiento de las Dapps se basa en dos elementos importantes que llevan a cabo sus propios usuarios; la prueba de trabajo (Proof Of Work - POW) y la prueba de participación (Proof Of Stake - POS). En el capítulo 3 se definirán más a detalle estos elementos.

1.5.5. DAC/DAO

Las Corporaciones / Organizaciones Autónomas Descentralizadas (DAC/DAO) son el resultado de un conjunto de distintas Dapps, y su funcionamiento se basa en mantener una gobernanza definida dentro de Blockchain, además estos financian, administran y estructuran sus operaciones mediante mecanismos propios sin depender de una entidad central. Permiten a una organización funcionar de manera adecuada gracias a sus redes descentralizadas las cuales están compuestas por agentes autónomos que ejercen trabajos automatizados (Joaquín López Lérida, 2016).

Partiendo de esto, se puede decir que las DAC son un concepto derivado de la inteligencia artificial. Ya que no se requiere de la intervención humana para su funcionamiento, tan solo un conjunto de reglas comerciales que permitan el control de estos agentes automatizados. A diferencia de las DAO que sí requieren de la intervención humana para su implementación. Tanto en las DAC/DAO hay contratos inteligentes que operan dentro de Blockchain que ejecutan tareas preaprobadas una vez que se haya cumplido una tarea o condición establecida. Un ejemplo de esto último está en la asignación de Bitcoin al minero ganador. Y a medida que las transacciones en esta criptomoneda se reinventan aumentando la eficiencia del mercado de remesas, es muy probable que en el futuro se haga lo mismo por las empresas cuyas actividades se basen en el cumplimiento de la jurisdicción local, licencias comerciales, seguros, impuestos etc. (Swan, 2015)

1.5.6. DAS

Por último, las Sociedades Autónomas Descentralizadas (DAS) no son más que el resultado de unir las Dapps y las DAC/DAO. Convirtiendo así las entidades organizacionales en sociedades virtuales que no dependen de ningún gobierno, nación o estado específico. Esta es una nueva idea de negocio que surge en Blockchain o incluso una persona. (Swan, 2015)

El propósito de DAS está enfocado en crear sociedades que puedan autogobernarse por uno o más contratos que sean capaces de; pagar dividendos a sus accionistas, mantener una estructura socioeconómica y política que permita la gobernanza de su funcionamiento de forma automática. (Joaquín López Lérida, 2016)

1.6. Blockchain 3.0: La visión futurista

Como resumen, se ha mencionado que Blockchain 1.0 es un sistema eficaz y revolucionario para el intercambio financiero sin intermediarios, tal y como sucede con el Bitcoin. Blockchain 2.0 como un sistema que desarrolla un concepto completamente nuevo como los contratos inteligentes y un avance importante en los mercados digitales que utlizan la tecnología Blockchain.

En la versión 3.0 se tiene como objetivo llegar más allá. Expandiendo sus aplicaciones a nuevas tecnologías basadas en la identidad, la libertad, la democracia y la contabilidad de activos de cualquier tipo generando nuevos modelos de contabilidad y trazabilidad. Pese a que Blockchain todavía está en una etapa temprana, no se descarta que será una revolución tecnológica en los próximos años. Sus elementos aún están evolucionando, las empresas TIC que se encargarán de su desarrollo todavía no

están completamente preparadas y los inversores u organizaciones que sacarán beneficio de su aplicación todavía están identificando sus estrategias para ponerlo en práctica.

Complementando lo anterior mencionado, Blockchain 3.0 está enfocado en la regulación y el cambio en las bases del mundo actual con ayuda de las DAS. Logrando así un mundo con entidades autónomas que tengan la capacidad de autogestionarse, generar sus propios ingresos, mantener un funcionamiento distribuido estable, neutral y autónomo. (Joaquín López Lérida, 2016).

Debido a la extensión de este tema, se hablará más a detalle de toda su composición y elementos en los siguientes capítulos mencionando algunas de sus aplicaciones y beneficios de emplear Blockchain tanto en la actualidad como en los próximos años.

Capítulo 2

Criptografía en Blockchain

El área de la seguridad informática se ha convertido en un campo extenso en los últimos años, y ha tomado mucha relevancia debido al impacto que ha dejado en la tecnología. Hoy en día la cantidad de información que se maneja es inmensa, grandes cantidades de datos a través de internet son enviados y recibidos por distintos equipos en milésimas de segundo a nivel mundial.

El rápido avance de la tecnología ha posicionado a la seguridad informática como un área esencial en la actualidad. Cada día, se transmiten exorbitantes cantidades de datos a través de internet a velocidades asombrosas. Sin embargo, este progreso trae consigo amenazas que ponen en riesgo nuestra privacidad e información personal. Ante esta realidad, es imprescindible contar con mecanismos que protejan dicha información. Y uno de estos mecanismos es la Criptografía.

La Criptografía es el arte y ciencia de transformar la información para hacerla incomprensible a personal no autorizado. Se basa en principios matemáticos para convertir la información original en una serie de números y símbolos que no revelen su contenido original.

A lo largo de este capítulo, introduciremos definiciones clave que ayudarán a comprender la importancia y aplicabilidad de la Criptografía en la era digital.

2.1. Acontecimientos históricos de la Criptografía

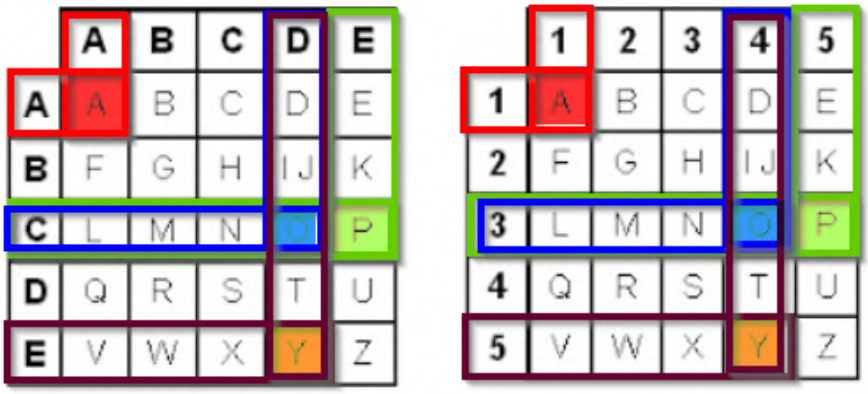
Desde la antigüedad, la necesidad de proteger la información ha impulsado el desarrollo de la criptografía. En contextos de guerra o conflictos políticos, hay que asegurar que los mensajes no fueran comprendidos por el enemigo podía ser la diferencia entre la victoria y la derrota.

Se cree que uno de los primeros usos de la Criptografía se remonta al Antiguo Egipto, con jeroglíficos inscritos en monumentos hace más de 4500 años. En tiempos de guerra, los egipcios usaban una técnica aún más ingeniosa, escribiendo mensajes secretos en las cabezas afeitadas de sus esclavos, que se ocultaban una vez que el cabello crecía. (Sanz, 2015)

Por su parte, entre los años 500 y 600 A.C los hebreos del antiguo Israel adoptaron un sistema de cifrado llamado atbash, que invertía el alfabeto, convirtiendo, por ejemplo, la a en z y viceversa. (Thomas, 2023)

Más adelante, en los años 200 a.C. el escritor griego Polybius introdujo una técnica que implicaba colocar el alfabeto dentro de una cuadricula de 5x5 y el sistema de cifrado sustituía un carácter del mensaje original por el número o letra de una columna o fila de la cuadricula.

Cifrar la palabra *Apoyo*:

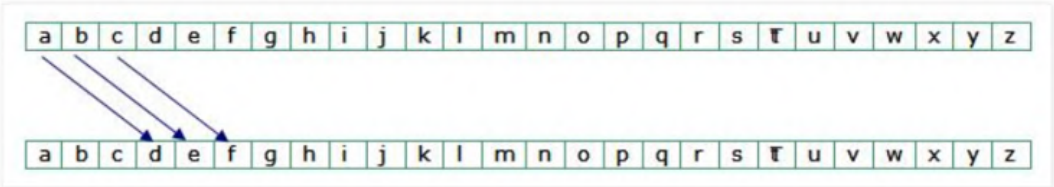


Mensaje:	**A**	**P**	**O**	**Y**	**O**
Cifrado 1:	AA	CE	CD	ED	CD
Cifrado 2:	**11**	**35**	**34**	**54**	**34**

Figura 2.1: Cifrado Polybius.

Asimismo, el Cifrado de César, usado por el propio Julio César, es otro ejemplo de la evolución en técnicas de cifrado. Consiste en la sustitución de una letra inicial por otra letra que se encuentra desplazada tres caracteres más adelante en ese alfabeto.

Cifrar la palabra *refuerzos*:



Mensaje:	**r**	**e**	**f**	**u**	**e**	**r**	**z**	**o**	**s**
Cifrado:	u	h	i	x	h	u	c	r	v

Figura 2.2: Cifrado de César.

Con el tiempo, surgieron dispositivos mecánicos para la traducción y cifrado de mensajes. En el siglo XV, Alberti diseñó ruedas concéntricas que generaban códigos poli alfabéticos.

Pero es durante la Segunda Guerra Mundial cuando la Criptografía alcanza un estatus icónico. Máquinas como Enigma, un sistema electromecánico basado en el encriptado con técnicas de rotores diseñado por el alemán Arthur Scherbius, eran consideradas impenetrables. Sin embargo, gracias al brillante trabajo del matemático británico Alan Turing, las comunicaciones cifradas alemanas fueron descifradas en 1942, un logro que cambió el curso del conflicto.

Hoy en día, la tecnología ha llevado la Criptografía a nuevos horizontes, brindando herramientas más robustas y sofisticadas para proteger nuestra información en el mundo digital.

2.2. Conceptos de Criptografía

El término de Criptografía: deriva del alfabeto griego, compuesto por las palabras *kryptós* (traducido como secreto) y *graphé* (traducido como escritura). Por lo tanto, la criptografía se entiende tradicionalmente como *escritura oculta*.

En una definición más técnica, la criptografía se presenta como el arte y la ciencia de transformar un lenguaje o mensaje convencional mediante el uso de claves, permitiendo la creación de cifrados (códigos secretos). Paralelamente, existe el Criptoanálisis:, encargado de interpretar y descifrar esos códigos mediante técnicas y análisis determinados para obtener un mensaje convencional. (Díaz, 1995) (Fernández, s.f.)

Según la Real Academia Española (RAE), la criptografía se define como

"el arte de escribir mensajes con una clave secreta o de modo enigmático".

En la práctica, este arte implica la transformación de un texto legible (texto plano) en un texto cifrado mediante una clave específica, proceso conocido como cifrado o codificación. De manera recíproca, el descifrado o decodificación implica convertir el texto cifrado de vuelta al texto plano, todo ello con la finalidad de resguardar el contenido de la información frente a personal no autorizado. (Urbina, 2016)

Hoy en día, con la ayuda de las matemáticas y la mejora en los avances tecnológicos, la criptografía tiene un rol esencial en ámbitos como la informática y las telecomunicaciones. Su función principal es proteger y salvaguardar mensajes, archivos o cualquier tipo de información mediante el uso de algoritmos sofisticados y llaves criptográficas, garantizando así la confidencialidad, integridad y disponibilidad de la información.

2.2.1. Triada de la seguridad de la información

En el ámbito de la seguridad informática, la *"Triada de la Seguridad de la Información"* establece tres principios esenciales que garantizan la protección y preservación de la información: confidencialidad, integridad y disponibilidad.

Confidencialidad: Se encarga de asegurar que la información sólo sea accesible para aquellos que tengan autorización. Para garantizar esto se requiere:

- Realizar el descifrado de manera sencilla para quienes tienen la clave.
- De manera inversa, se debe ser considerablemente complicado descifrar la información si no se tiene la clave correcta.

Integridad: Este principio garantiza que la información no sea alterada ni eliminada sin autorización durante su ciclo de vida. Asegura que los datos recibidos o enviados se mantengan intactos y no se modifiquen de manera no autorizada.

Disponibilidad: Garantiza que la información y los sistemas estén siempre disponibles para los usuarios autorizados cuando lo requieran. (CABALLERO GONZÁLEZ y CLAVERO GARCÍA, 2017).

2.3. Definición de criptosistema y sus tipos

Un criptosistema es un conjunto de algoritmos que transforma un mensaje legible o texto claro en un texto cifrado, asegurando que solo aquellos con la clave adecuada puedan descifrarlo. Esta transformación es vital para proteger la información durante su transmisión en canales de comunicación (Andrade y Cedillo, 2004).

Los criptosistemas se clasifican según la naturaleza y el uso de sus claves:

- **Criptosistemas simétricos:** Utilizan una única clave para el cifrado y el descifrado del mensaje. Ambas partes, emisor y receptor, deben compartir esta clave de manera segura para garantizar la confidencialidad del mensaje.
- **Criptosistemas asimétricos:** Operan con un par de claves; una clave pública, que puede ser compartida libremente, y una clave privada, que se mantiene en secreto. El mensaje cifrado con una de estas claves solo puede ser descifrado con la otra, garantizando de esta manera tanto la confidencialidad como la autenticidad del mensaje.

2.3.1. Criptografía Simétrica

La criptografía simétrica, también llamada de clave secreta, se caracteriza por utilizar una única clave tanto para cifrar como para descifrar la información. Esta clave, al ser compartida entre el emisor y el receptor, debe mantenerse en absoluto secreto. Si un atacante o usuario no autorizado logra obtenerla, la seguridad del sistema quedaría comprometida.

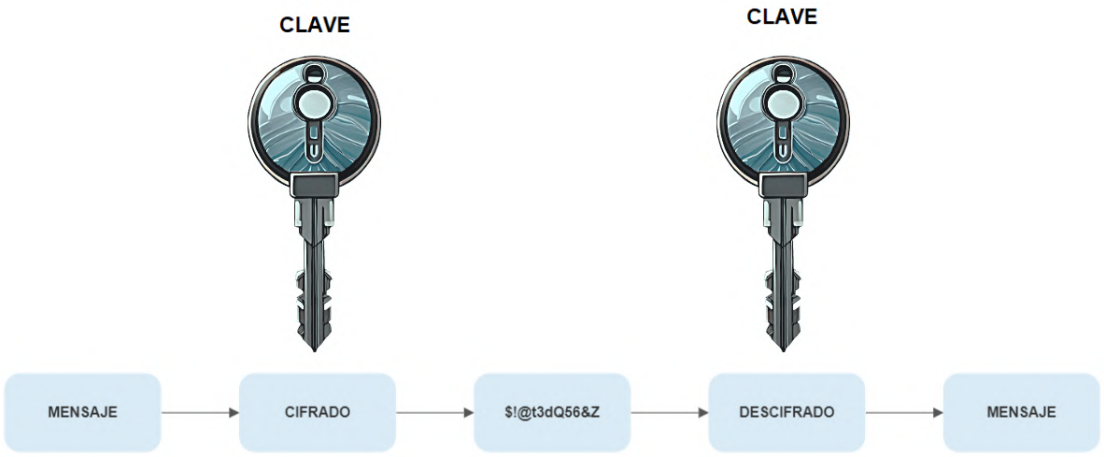


Figura 2.3: Criptografía Simétrica.

Durante la década de los setenta, los sistemas de cifrado simétrico fueron la principal herramienta para la comunicación segura. Sin embargo, su eficacia residía en la capacidad de resguardar la clave secreta, ya que se debía tener mucho cuidado al enviar esta clave entre el emisor y el receptor sin que fuera interceptada. Además, la criptografía asimétrica presentó grandes desafíos para intercambiar información entre más usuarios. Imaginemos que, en una gran red de computadoras, si solo hubiera una clave compartida entre dos usuarios, sería inviable manejar sistemas simétricos. La logística de tener claves diferentes para cada usuario dentro de la red sería un desafío insuperable.

No obstante, uno de los principales atractivos de la criptografía simétrica es su velocidad de cifrado. Con claves que solo tienen unos cientos de bits, se puede garantizar una seguridad robusta. Los ataques efectivos contra este tipo de sistemas son DES [1], AES [2] o Blowfish [3], los cuales se basan en la fuerza

[1] Data Encryption Standard (DES) fue publicado en 1977 como un algoritmo de encriptación simétrico el cuál emplea una clave de 56 bits. Para su funcionamiento se requiere que tanto el receptor como el transmisor compartan la misma clave (Georgina Arcos, 2018).

[2] Advanced Encryption Standard (AES) surgió en el año 2011 como un reemplazo al DES, manejando un cifrado de bloques y aumentando la longitud de su clave en un rango entre 128 a 256 bits (Georgina Arcos, 2018).

[3] El algortimo Blowfish fue desarrollado en 1993 por el criptógrafo Bruce Schneier el cuál además de ser muy compacto y

bruta, lo que indica la solidez de estos algoritmos.

2.3.2. Criptografía Asimétrica

La criptografía asimétrica, también conocida como de clave pública, se diferencia de la simétrica en que utiliza un par de claves; una pública y una privada. Mientras que la clave pública se puede compartir libremente y se utiliza para cifrar mensajes, la privada, que se mantiene en secreto, se usa para descifrarlos. Lo que hace que este sistema sea seguro es la complejidad computacional de deducir la clave privada a partir de la clave pública.

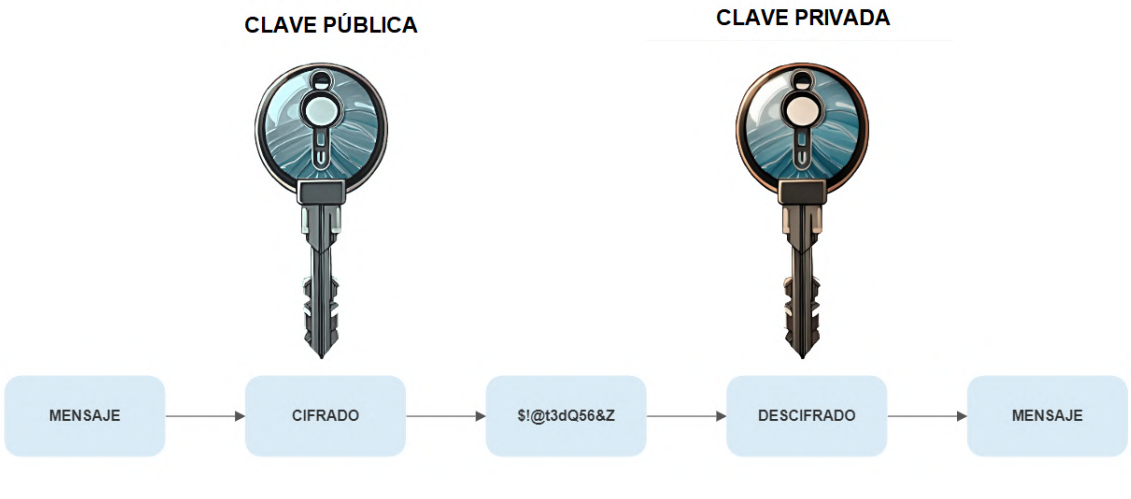


Figura 2.4: Criptografía Asimétrica.

Las figuras 2.3 y 2.4 ilustran claramente la diferencia entre los criptosistemas simétrico y asimétrico. En el asimétrico, la clave con la que se cifra un mensaje no es la misma con la que se descifra, lo que añade una capa adicional de seguridad. La aplicación del algoritmo puede variar dependiendo del uso que se le dé a las claves. Si se utiliza la clave pública para cifrar, la clave privada será para descifrar, y viceversa.

Este tipo de criptografía fue introducido en la década de 1970 por Whitfield Diffie y Martin Hellman. Desde entonces, varios algoritmos asimétricos han surgido, pero solo algunos, como RSA [4], El Gamal [5] y Rabin [6], han ganado relevancia (Andrade y Cedillo, 2004).

Por razones de seguridad, las claves en la criptografía asimétrica suelen ser de mayor longitud que en la simétrica. Por ejemplo, mientras que una clave segura en un algoritmo simétrico podría tener 128 bits, en un algoritmo asimétrico, a menudo se requieren al menos 1024 bits. Sin embargo, esta seguridad adicional viene con un costo: el cifrado y descifrado asimétrico son procesos más lentos que sus contrapartes simétricas debido a la complejidad de los cálculos.

Una ventaja destacada de la criptografía asimétrica es que, al no ser necesario compartir la clave privada, es más segura para enviar información a través de canales que podrían no ser totalmente seguros.

---

fácil de implementar, cuenta con una longitud variable que alcanza incluso los 448 bits (Stallings, 2004).

[4] Rivest, Shamir y Adleman (RSA) que recibe el nombre de sus inventores representa los mensajes mediante números, es decir, que cada carácter se representa con un número. Además, cada participante comparte una clave para el cifrado y conserva de manera privada otra clave para el descifrado (Johnsonbaugh, 1999).

[5] ElGamal surgió en 1985. Es un algoritmo cuya seguridad se basa en el problema del logaritmo discreto, es decir, la función empleada va en un solo sentido y es muy difícil de calcular en sentido inverso (Maria Gonzalez, 2021).

[6] Rabin fue publicado en 1979. Es un algoritmo de clave pública cuya seguridad se basa en la complejidad del problema de la factorización y el problema de la raíz cuadrada módulo de un número compuesto (Broncano, 2015).

2.4. Funciones HASH y su importancia

Se define como un algoritmo criptográfico que se encarga de transformar cualquier texto, contraseña o archivo en una serie de caracteres de longitud fija (Sola, 2021). Una función hash, recibe un archivo inicial de texto plano y en base a este, crea una cadena alfanumérica única y de longitud fija que representa un resumen o extracto de toda la información recopilada. cabe mencionar, que este valor hash no depende de la longitud de los valores de entrada.

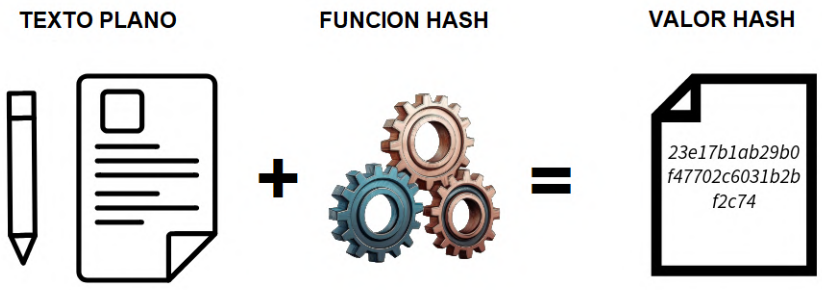


Figura 2.5: Función hash.

Algunas de las aplicaciones que se le pueden dar a las funciones hash está en la protección de contraseñas. Lo que sucede aquí es que, al generar una contraseña, esta creará un hash único para esta y será almacenada dentro de una base de datos. Cuando un usuario se autentica para acceder a un determinado servicio, el algoritmo calcula el hash de la contraseña ingresada y después, esta es comparada con la que se almacenó anteriormente en la base de datos. Si estas son iguales la clave será correcta, y el usuario podrá ingresar sin problemas.

Los hashes también ayudan a la detección de malware creando listas negras o listas públicas. Estas listas están formadas por valores hash de distintos tipos de malware creando así un registro de todos los malware conocidos. Esto le permite a los usuarios y las empresas tener una fuente confiable donde puedan consultar si un archivo sospechoso está catalogado como malware. Algunos de los repositorios más utilizados son VirusTotal, VirusBay, Malpedia y MalShare. (34, 2023)

Otra aplicación muy útil está en mantener la integridad de los mensajes. El método para esto, es comprobar los hashes creados antes y después de transmitir el mensaje. Si los hashes son exactamente iguales significa que la comunicación ha sido segura ya que se avala que la información no fue alterada. Caso contrario, si estos no coinciden significa que la información ha sido modificada por un tercero.

Una propiedad muy importante de los algoritmos hash y que permite brindar la seguridad de hoy en día está en que funcionan en una dirección, es decir, no se les puede aplicar ingeniería inversa. Si generamos un hash a un archivo, no será posible generar el archivo inicial con el hash. La única opción sería con fuerza bruta o al azar, y esta es la razón por la que se han actualizado estos algoritmos de cifrado, a consecuencia de que el avance tecnológico y computacional ha dejado obsoletos algunos algoritmos de cifrado. Sin embargo, los algoritmos utilizados en la actualidad están diseñados para que no sea posible descifrarlos, ya que de intentarlo tomaría años llegar a los datos de entrada, además de que se necesitaría muchísima potencia computacional.

Algunos ejemplos de estos algoritmos son; MD5, KDF y SHA. De los cuales, este último es el que más destaca, y el que se abarcará más a detalle a lo largo de esta tesis.

2.4.1. Algoritmo SHA

El término SHA se definió por la NSA [7] y el NIST [8] en 1993 como Algoritmo Hash Seguro cuya finalidad es generar un hash único en base a una norma decretada.

El primer protocolo se llamó SHA-0, pero no tomó relevancia hasta dos años después con la aparición del SHA-1 con mejor resistencia y seguridad al anterior. A pesar de ello, los avances tecnológicos y la aparición de nuevos ataques informáticos lo convirtieron en un algoritmo obsoleto. Por lo que años más tarde se creó el SHA-2, un algoritmo con cuatro variantes de acuerdo con el número de bits de salida, estos son SHA-224, SHA-256, SHA-384 y SHA-512 (López, 2022a).

Características de los algoritmos SHA2:

- Tamaño de salida: se refiere al tamaño de caracteres que ocupará el hash. Por ejemplo, SHA-224 (224 bits), SHA-256 (256 bits) etc.
- Tamaño del bloque: es el tamaño del bloque que maneja el algoritmo.
- Tamaño máximo del mensaje: se refiere a la magnitud máxima del mensaje al que se desea aplicar el algoritmo.
- Interacciones o rondas: número de operaciones que realiza el algoritmo para llegar al hash final.
- Longitud de la palabra: es la longitud en bits de la operación que aplica en cada ronda el algoritmo.
- Operaciones soportadas: operaciones que lleva a cabo el algoritmo para obtener el hash final.

2.4.2. SHA-256

Utiliza una clave de 256 bits para tomar un dato inicial y transformarlo en una cadena de datos completamente irreconocible. Dado que este valor está expresado en hexadecimal, sólo se visualizarán números, y letras de la *a* a la *f*. Ejemplo:

Texto plano: **esto es un hash**
SHA256: **bd7711490abf22f20f9c58a535f206c8223f20081d46d8a44f8c5831e4148b73**

2.4.3. SHA-512

De igual forma que el anterior, este emplea una clave de 512 bits. Ejemplo:

Texto plano: **esto es un hash**
SHA512: **833f55d93cd6001c9f175cc28dd667fdb99ce348763180291ad8e200a503df22fac9b0c104 81ca2fb9ff7e3952bc3676a1f5bf861e2e4e708ec2faacb07003fe**

Más detalles sobre cómo calcular un algoritmo SHA se explorará en el apéndice A.

[7] National Security Agency (Agencia de Seguridad Nacional) es una institución que se encarga de recopilar y procesar información para el estado mediante procesos de Criptología: y ciberseguridad.

[8] National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología) es una agencia estadounidense encargada de desarrollar y promover estándares, medidas y tecnologías para mejorar la seguridad y la competitividad económica del país.

Capítulo 3

Conceptos básicos de Blockchain

Se le da el nombre de Blockchain (cadena de bloques) debido a la estructura de su base de datos ya que toda la información que se maneja en esta tecnología es almacenada y organizada dentro de bloques. Los bloques se ordenan de manera cronológica y son identificados por una dirección, esta dirección no es más que un código alfanumérico conocido como hash el cuál debe ser encontrado por un grupo de nodos llamados mineros. El minero que encuentra este valor es quien firma el bloque y lo añade a la cadena. Una vez añadido un bloque a dicha cadena ya no será posible modificar ni eliminar la información ya que esta será almacenada de manera permanente, manteniendo así el no repudio como una de sus características más importantes (Amengual, 2021).

La tecnología implementada en Blockchain no es nueva, ya que no se basa en utilizar algo no conocido, muy por el contrario, se basa en emplear tecnologías ya conocidas y darles una aplicación diferente. Blockchain es el resultado de la combinación de las redes peer to peer y la criptografía asimétrica las cuales ya se han definido anteriormente (Joaquín López Lérida, 2016). De esto se puede deducir que el objetivo de Blockchain está en gestionar un registro único en donde se pueden emplear transacciones y multiples operaciones mediante un sistema descentralizado en donde no se requiera la intervención de una entidad tercera para su ejecución.

En este capítulo se hablará de los puntos clave necesarios para entender el funcionamiento paso a paso detrás de esta tecnología.

3.1. Árbol de Merkle

El árbol de Merkle es un sistema de información dividido en varias capas que tiene como finalidad relacionar cada nodo con una raíz única, la cual deberá estar asociada con todos y cada uno de estos. Permiten relacionar una gran cantidad de información la cuál poco a poco se unifica de manera piramidal hasta llegar a un solo punto raíz. Este proceso se lleva a cabo de la siguiente manera:

1. Cada nodo es identificado con un identificador único (hash). Los nodos inferiores son conocidos como nodos hijos.

2. Estos hashes se asocian con un nodo superior conocido como nodo padre (o rama), el identificador único del nodo padre será el resultado de la unión de los hashes de sus nodos hijos.

3. Se repite el proceso hasta llegar a un solo nodo principal conocido como nodo raíz o raíz de Merkle.

El hash correspondiente a este nodo raíz es conocido como root hash o dirección raíz. Este root hash está relacionado con todos los hashes del árbol y se implementó para facilitar la verificación de todas las transacciones u operaciones realizadas en cada nodo. Además, esta infraestructura no puede ser modificada una vez teniendo el root hash, ya que si un hash de los nodos hijos es modificado se

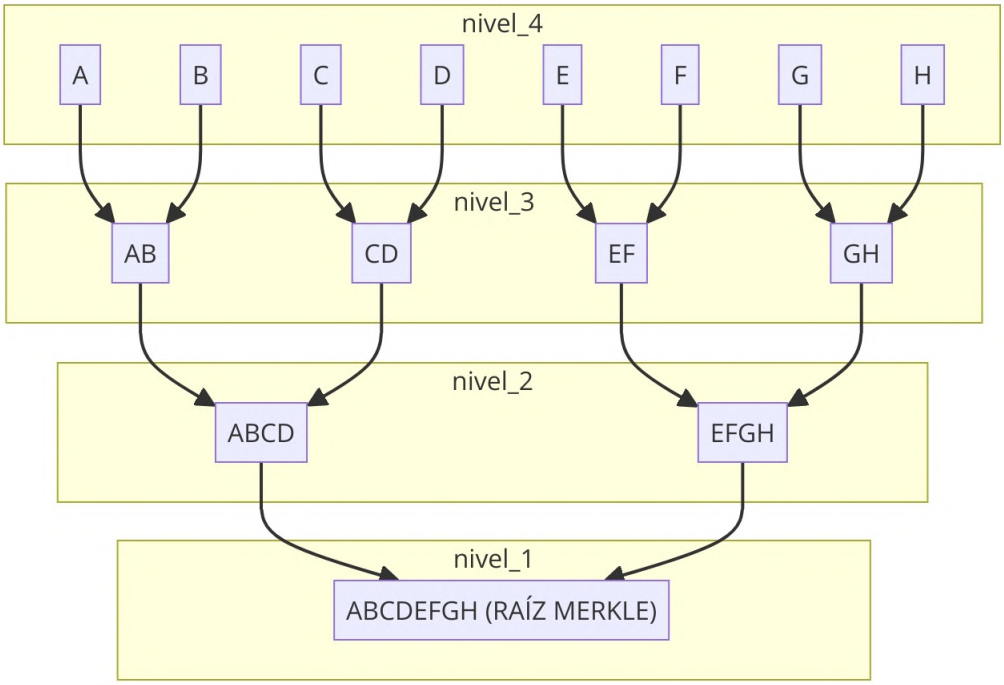


Figura 3.1: Árbol de Merkle.

cambiará toda la infraestructura hasta llegar a la raíz. Y esta característica es la que permite un gran nivel de seguridad dentro de este sistema, ya que si un hash es modificado será invalidado todo el árbol (Gómez, 2023).

3.1.1. Características de los árboles de Merkle

- Garantizan una gran seguridad y resistencia a la modificación de los datos.
- Permiten un alto nivel de rendimiento para la transmisión de datos en redes distribuidas. Esto debido a que se disminuye considerablemente la cantidad de datos a implementar.
- Permiten búsquedas de verificación mucho más rápidas, ahorran recursos de almacenamiento y son poco costosos.
- Ofrecen una gran adaptabilidad a problemas informáticos, permitiendo su aplicación en diversos sistemas como bases de datos, redes distribuidas (peer to peer), estructuras de llaves públicas etc.

Su función es que cada bloque obtenga su dirección correspondiente de manera correcta. El árbol propaga los hashes hacia arriba de modo que, si un bloque inferior es modificado, todo el hash será alterado de modo que su hash sea totalmente distinto al original. Esto causará que el bloque sea invalidado por el consenso impidiendo que sea añadido a la cadena.

Tal y como se observa en la Figura 3.2, al cambiar el valor inicial por F en el nodo 1, este cambiará al nodo 2, y lo hará sucesivamente hasta llegar a un valor completamente distinto al original.

3.2. Estructura de un bloque y su enlace en Blockchain

Blockchain requiere una gran variedad de componentes los cuales tienen distintas funciones cada uno. A continuación, se definirá a detalle cómo funciona una transacción realizada en Blockchain siguiendo los mismos pasos que se mostraron en la Figura 1.1.

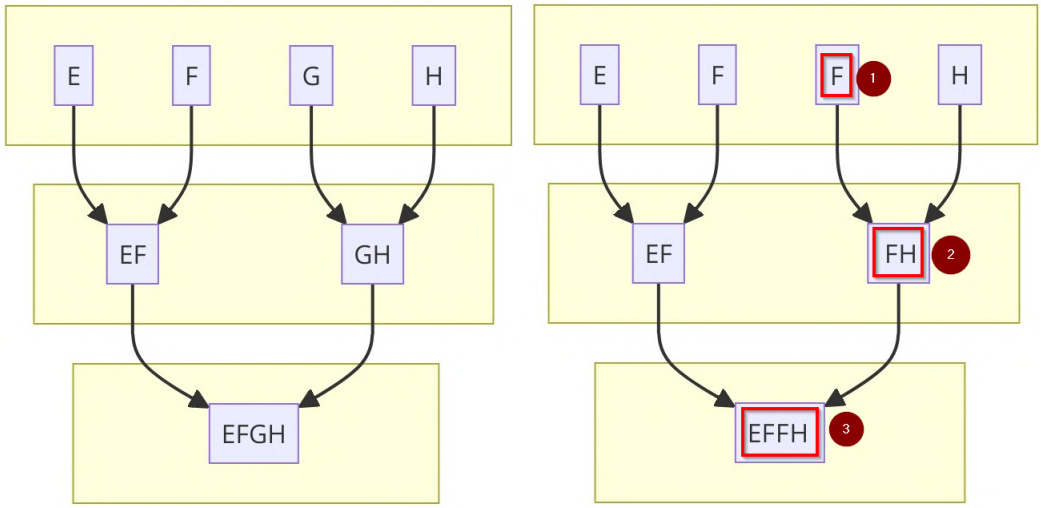


Figura 3.2: Árbol de Merkle correcto en comparación de uno modificado.

3.2.1. Hash en Blockchain

En Blockchain se requiere emplear las funciones hash de datos iniciales, dicho hash será el encabezado de cada bloque y además deberá contener el hash del bloque anterior uniendo los bloques para crear la cadena. Las funciones hash utilizadas en Blockchain (sobre todo en BTC) son SHA-256. Para comenzar a entender cómo es que se realizan estos procedimientos se darán algunos ejemplos de cómo funciona la función hash. A continuación, se coloca un ejemplo del hash resultante a una palabra de entrada, (el software empleado para estos ejemplos se puede encontrar en $https://demoblockchain.org/hash$):

Figura 3.3: Función SHA256 resultante de la palabra *cadena de bloques de bitcoin*.

Es importante destacar, que al modificar cualquier dato de la palabra de entrada se tendrá un hash completamente diferente. Ejemplo:

Se puede observar claramente que a pesar de que el cambio en la palabra de entrada sea mínimo como en la Figura 3.4 el hash final será completamente distinto al hash original que se mostró en la figura 3.3. Este es un factor muy importante que permite identificar fácilmente cuando un valor ha sido modificado o alterado sin consentimiento, preservando así la integridad de la información.

Figura 3.4: Función SHA256 resultante al modificar la palabra inicial.

3.2.2. Bloque

El segundo factor para definir en este procedimiento es el bloque. Cuando se realiza un conjunto de transacciones, BTC, por ejemplo, estas se agrupan a un espacio digital llamado bloque. Cada bloque consta de dos factores:

- Un encabezado
- Las transacciones realizadas

Por ejemplo, si Blockchain se define como un libro de registros, cada bloque correspondería a una página de dicho libro, mientras que las transacciones pasarían a ser el contenido de estas. Cuando se tiene un bloque con un valor hash como identificador, es importante que este tenga también el hash del bloque que lo antecede tal y como se muestra en la siguiente figura:

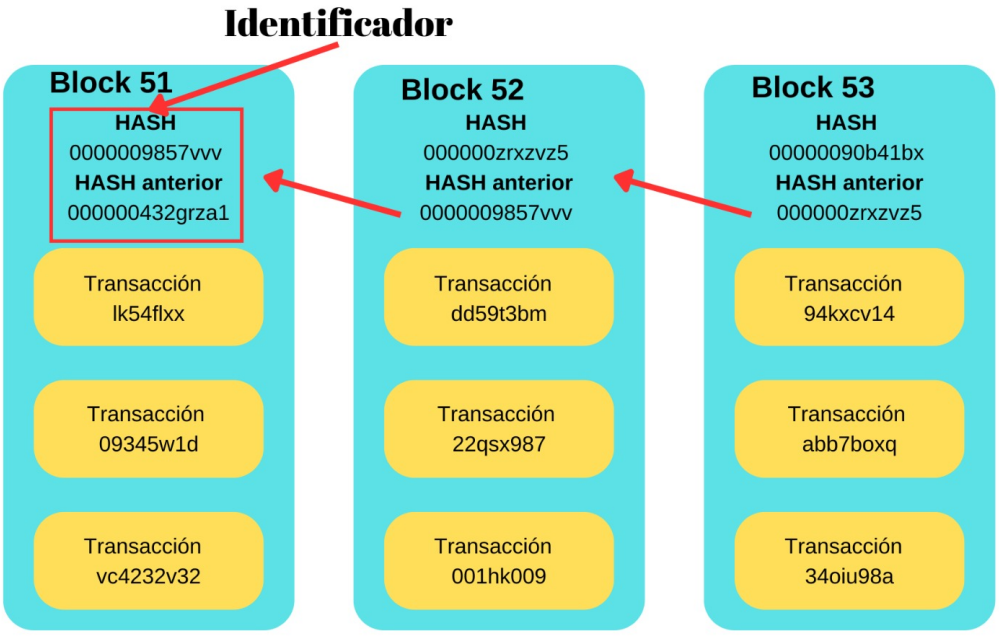


Figura 3.5: Encabezado de los bloques.

3.2.3. Tipos de Bloques

Ahora que se ha definido el encabezado de cada bloque, se explicarán los tipos de bloques que se suelen utilizar dentro de Blockchain.

- **Bloque génesis.** Es el primer bloque creado dentro de la red Blockchain.

- **Bloques huérfanos.** Son bloques válidos que al final terminan siendo rechazados. Esto sucede cuando se minan dos bloques al mismo tiempo. Cuando esto sucede se siguen validando los demás bloques, y al final se toma en cuenta la cadena que tenga más bloques, mientras que la más corta será descartada, estos bloques pasarán a ser los huérfanos.

- **Bloques obsoletos.** Cuando se mina un bloque de manera correcta, los demás bloques que seguían en este proceso pasarán a ser completamente obsoletos.

- **Bloques Umer.** Estos bloques son similares a los huérfanos, son rechazados una vez que se cuenta con una cadena más larga. Sin embargo, la diferencia está en que el minero que resuelva el bloque recibirá una pequeña recompensa por realizar el proceso de minería aunque su bloque no sea añadido a la cadena, cosa que en Bitcoin no sucede. Este tipo de bloques suelen presentarse mucho en Ethereum: (Mohanty, 2019).

El encabezado del bloque es una recopilación de información que caracteriza a cada bloque perteneciente a una red de Blockchain. Estos elementos se definen en la siguiente tabla y se muestran en la Figura 3.6, ambas definidas por Murray, M (2019). Cabe mencionar que el bloque génesis es el único que no cuenta con el ID del bloque anterior.

Campo	**Descripción**
Versión de software	Denota las reglas de validación utilizadas en esta versión del software blockchain
Tiempo	Hora de creación del bloque
ID del bloque anterior	Hash del encabezado del bloque anterior
Raíz de Merkle	Resumen único derivado de los hash de todas las transacciones incluidas en el bloque
Objetivo de dificultad	Desafio matemático del mecanismo de consenso definido, esto se relaciona con la cantidad de ceros a la izquierda que el hash encabezado del bloque debe incluir
Nonce	Valor numérico que resuelve el desafío matemático, Su término en inglés es la representación de decir *number use once* lo que significa que es un número que se utiliza una sola vez.

Cuadro 3.1: Metadata en los encabezados de bloques.

Él flujo de unión de cada bloque se forma con la agrupación que conecta a estos de forma cronológica:

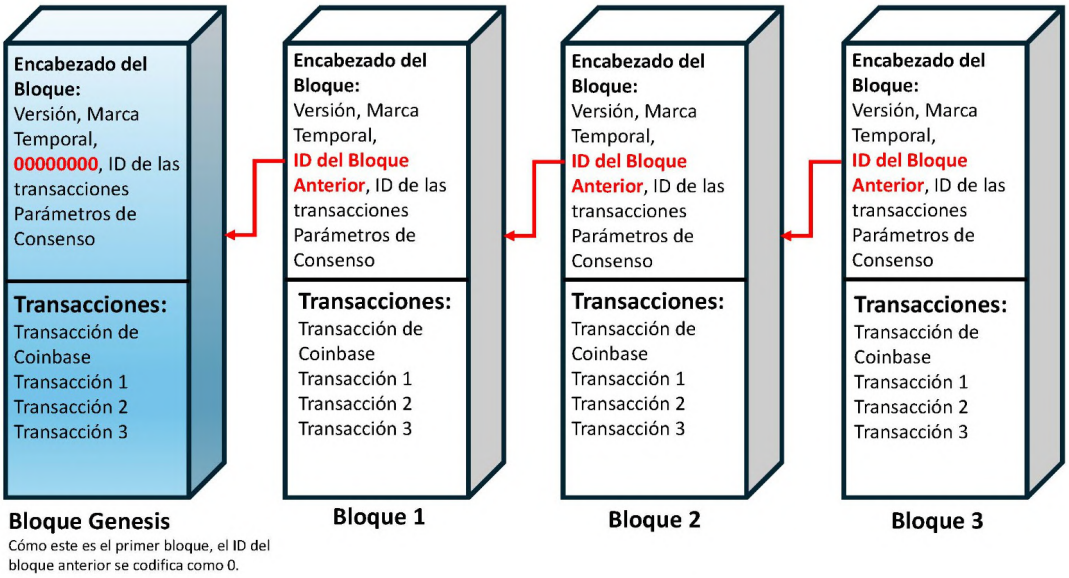


Figura 3.6: Flujo de unión de cadena de bloques.

Tal y como se puede observar el encabezado de cada bloque no sólo debe contar con su respectivo hash, sino también con el hash del bloque anterior (Murray, 2019). Por el momento, cada transacción de Bitcoin puede tardar 10 minutos en procesarse y confirmarse, sin embargo, para tener suficiente seguridad se debe esperar más tiempo (una hora aproximadamente). Para casos de transferencias más grandes puede tomar aún más tiempo, ya que se debe validar que no se trate de un problema de doble gasto (Swan, 2015).

Volviendo a nuestro simulador de cadena de bloques, si nos vamos a la sección de bloques veremos que cada bloque cuenta con la siguiente información, (para más detalle se puede visitar el sitio $https://demoblockchain.org/block$):

Figura 3.7: Flujo de unión de cadena de bloques.

Claramente se puede observar que cuenta con elementos básicos como el número de bloque, nonce, contenido y su respectivo hash (en este ejemplo todavía no se toma en cuenta el hash del bloque anterior). Sin embargo, hay una opción adicional llamada *minar*. Esta opción es la representación de los mineros que se encargan de validar que las transacciones y los bloques sean correctos permitiendo su adición a la cadena.

3.3. Componentes clave en el funcionamiento de Blockchain

En esta sección se abordarán los componentes que forman parte de Blockchain y que son clave para su funcionamiento.

3.3.1. Minería de datos

Se define a la minería de datos como una técnica asistida por computadora que se implementa para el análisis y proceso de grandes cantidades de datos. Esta técnica permite transformar datos brutos en conocimiento práctico, es decir, que se procesa la información dada de tal modo que permite aportar conocimiento para resolver problemas o analizar las consecuencias futuras de las desiciones tomadas en una empresa.

En otras palabras, el término *minería de datos* se refiere a la extracción de un significado o información valiosa de los datos analizados. Aportando conocimiento a quien implemente esta técnica. A continuación, se describe el proceso habitual de la recopilación, almacenamiento, análisis y minería de datos:

- La recopilación de datos se basa en la captura de datos provenientes de distintos origenes como comentarios de usuarios o clientes, pagos, órdenes de compra, etc.
- El almacenamiento de datos guarda la información en una base de datos.
- El análisis de datos consiste en el procesamiento y análisis posterior de los datos mediante algoritmos de software bastante complejos.
- La minería de datos es una estrategia de análisis que permite encontrar patrones ocultos o desconocidos (Amazon, 2023).

3.3.2. Mineros

En Blockchain, los mineros son los responsables de verificar las transacciones dentro de la red resolviendo las pruebas propuestas mediante un software o hardware específico. Por ejemplo, la función de un minero en Bitcoin se basa en crear cada bloque después de que se realiza una transacción para ser añadida posteriormente a la cadena. El primer minero que pueda resolver el problema es recompensado con la respectiva criptomoneda asociada a la red Blockchain. Y dado que actualmente existe una gran cantidad de mineros en las grandes redes como Bitcoin o Ethereum no es recomendable minar los bloques por cuenta propia. En lugar de esto, algunos mineros se agrupan para aumentar sus recursos computacionales y aumentar las probabilidades de éxito, una vez que se mina cada bloque se dividen la recompensa. Estas agrupaciones se conocen como *mining pool* (piscina minera).

El objetivo de la minería de Blockchain es brindar seguridad y estabilidad a la red a cambio de recibir ganancias por medio de las recompensas obtenidas. La infraestructura necesaria para el desarrollo de esta tecnología se basa en servidores, software, hardware, energía, y comunidades de mineros. Cabe mencionar que mientras más mineros se tengan en la red, más segura será la validación de sus transacciones (Álvarez Rojas, 2018).

3.3.3. Creación de bloques nuevos

El proceso de generar un nuevo bloque entre los mineros consiste en una competencia entre miles de mineros ubicados en distintas partes, el proceso de minería permite armar cada bloque con sus respectivas transacciones. Y para que un minero pueda validar cada bloque se requiere demostrar que tiene la capacidad computacional suficiente, lo cual se realiza mediante una *Prueba de trabajo (Proof of work)*, lo cuál consiste en intentar crear el hash de cada bloque. Encontrar este hash es casi imposible si se busca realizar un cálculo matemático, por lo que los mineros simplemente se dedican a calcular miles de millones de hashes al azar hasta encontrar el que corresponda al encabezado de cada bloque. Y como se ha definido anteriormente, el valor numérico que permite cambiar el hash de un bloque es el $nonce$, por lo que se debe encontrar un valor numérico de éste, de modo que al calcular su hash este corresponda al del bloque. (Levy, 2021)

Por ejemplo, en nuestra plataforma de Blockchain se va a minar un bloque para asegurarnos de que sea válido para añadirse a la cadena. En este caso particular, un bloque se considerará válido si el hash de su encabezado inicia con cuatro ceros. Dado que los algoritmos SHA 256 tienen 64 caracteres y cada carácter consiste en 16 posibilidades (las letras A-F y los números 0-9), se tiene que lograr al azar una combinación tal que contenga el número 0 en los primeros 4 caracteres de los 64 mencionados. Eso significa que se tiene que encontrar un valor que tenga las posibilidades 1 en 16x16x16x16, o, dicho de otra forma, se tiene que encontrar un hash de cada 65,536 posibilidades. En nuestra plataforma demo es fácil de encontrar debido a que es un cálculo simple.

Supongamos que se tiene un bloque con 4 transacciones y se requiere encontrar el Nonce, para validar que el hash es correcto debe iniciar con cuatro ceros. Lo que se mostrará en nuestra demo es lo siguiente:

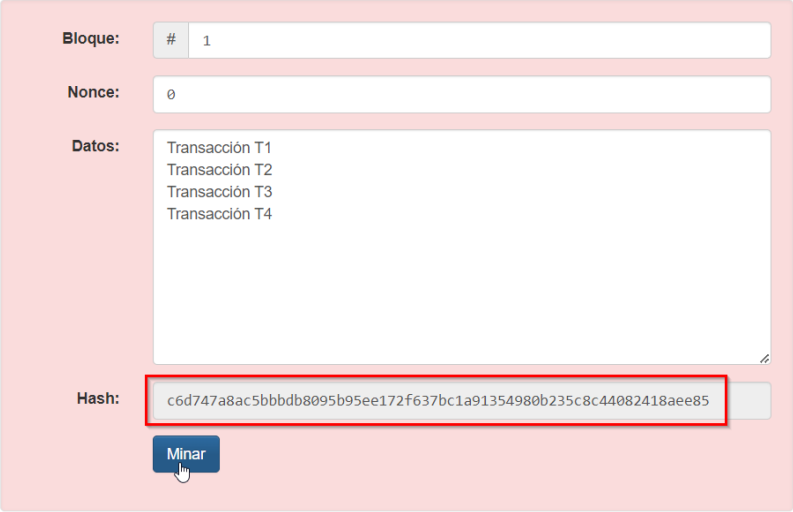


Figura 3.8: Bloque no válido.

Se puede observar que con el Nonce = 0 se tiene un hash que no inicia con los 4 ceros solicitados, por lo que se deduce que este bloque no es válido para ser añadido a la cadena. De acuerdo con lo anterior mencionado, se tiene que realizar un proceso de minería, el cual, se puede realizar en esta herramienta seleccionando la opción *minar*:

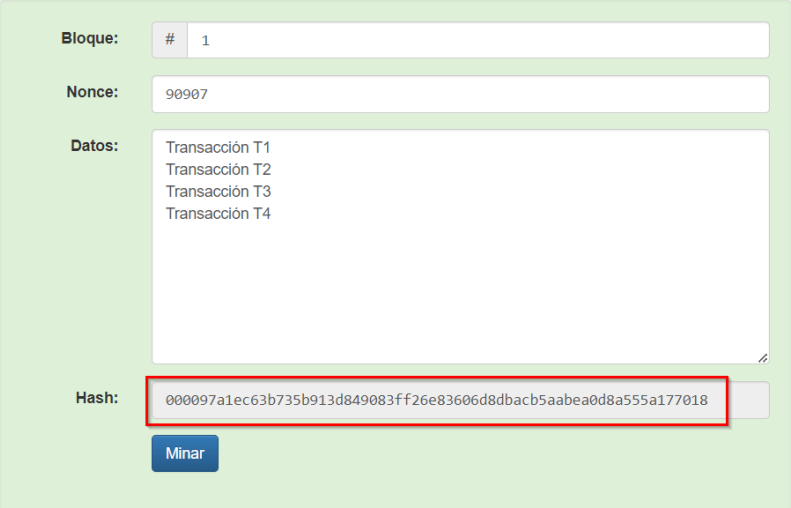


Figura 3.9: Bloque válido.

Tal y como se puede observar en la Figura 3.9 el hash del encabezado de nuestro bloque inicia con 4 ceros y fue encontrado con el Nonce = 90907, suponiendo que en este ejemplo ya se validó que el hash es correcto, el minero que lo encontró será el que reciba la recompensa y será su bloque el que se añada a la cadena de manera correcta.

En comparación, el bloque más reciente el día 15 de julio de 2023 en Bitcoin (# 798.885) tiene el hash:

$$000000000000000000d67aa92d57285ec6aaed06268bcdb8cd2f3b724c4c5c$$

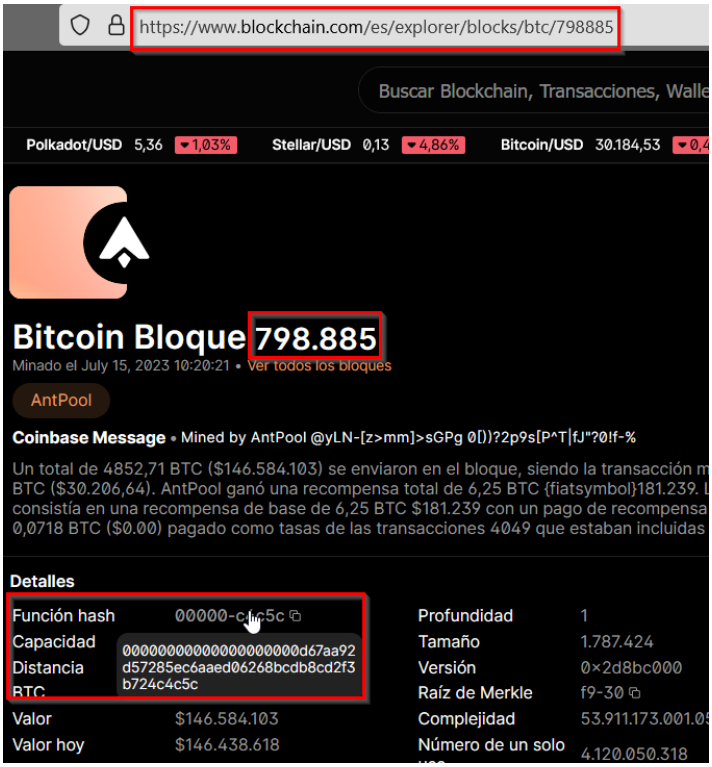


Figura 3.10: Bloque número 798 885 de la red de Bitcoin (Vease en *https* : *//www.blockchain.com/explorer/blocks/btc/*798885).

Este hash comienza con 20 ceros, lo cual es equivalente a 1 en 16x16x16x16x16x16x16x16x16x16

x16x16x16x16x16x16x16x16x16x16 de posibilidades. Es decir, que este hash se puede encontrar en cada 1,133,367,955,888,714,851,287,040 hashes. Y es por esto que los mineros necesitan mucha potencia computacional para encontrar el hash válido de cada bloque mientras compiten con otros mineros. Generando miles de millones de combinaciones por segundo. Todo esto con el objetivo de encontrar el hash válido y añadirlo a la cadena para recibir su recompensa (Levy, 2021).

3.3.4. Transacciones en Blockchain

Cuando se realiza una nueva transacción en bitcoin esta se transmite a la red, y entra al *mempool* [1]. Los mineros buscan constantemente nuevas transacciones en el mempool para agregarlas a los bloques que están por crearse. El proceso de agregar la transacción a un bloque se conoce como confirmación, ya que una vez que se añade al bloque deja de estar en el mempool. En uso práctico, un monedero no permite el acceso a los bitcoins recibidos hasta que la transacción haya sido confirmada.

3.3.5. Validación de transacciones

Para validar que cada transacción en bitcoin es correcta se utiliza un sistema de inputs (entradas) y outputs (salidas). Input se refiere a la dirección desde la cual se envía el dinero (usuario origen), y output es la dirección que recibe los fondos (usuario destino).

Los inputs o entradas hacen referencia a previas transacciones de donde se haya recibido bitcoin previamente. Dado que todas las transacciones en bitcoin han sido grabadas de manera permanente e inmutable en la cadena de bloques siempre existirá un record o historial de todos los bitcoins que se han recibido en una cartera digital (Levy, 2021).

Por otro lado, cada output o salida hace referencia a las direcciones hacia las que se envía el dinero. Es decir, las direcciones a las que las monedas ”salen”. Como una billetera puede contener varias direcciones de entrada, puede enviar dinero de una o más entradas a una o más salidas. (Noelle Acheson, 2022)

Por ejemplo, si un usuario A desea enviar 2.7 bitcoins a un usuario B pasaría lo siguiente: el monedero origen, en este caso el usuario A debe tener récord de haber recibido al menos 2.7 bitcoins previamente. Esto puede ser en una transacción previa o un gran numero de transacciones las cuales al ser agrupadas suman un total de 2.7 bitcoins o más. Y en caso contrario, si no se han recibido 2.7 bitcoins previamente a dicho monedero, no existirán transacciones en la cadena de bloques que puedan servir como inputs para la transacción que se quiere crear.

Si la transacción de 2.7 bitcoins es válida será enviada al usuario destino de manera correcta. En ese momento el monedero del usuario A creará una nueva transacción y asignará esos 2.7 bitcoins a un nuevo output que corresponde al usuario B. Mientras que el monedero del usuario B creará una transacción de 2.7 bitcoins provenientes de un nuevo input (el usuario A).

Esos 2.7 bitcoins que recibió la otra persona estarán disponibles para servir como un $input$ en una futura transacción.

3.3.6. Confirmación de transacciones

Cuando se confirma una nueva transacción, esta se agrupa con otras transacciones de manera ordenada en un nuevo bloque. Los mineros compiten entonces por validar este bloque, tarea que incluye encontrar un hash de encabezado que cumpla con ciertos criterios, como iniciar con un número específico de ceros dependiendo de la dificultad.

A continuación, se hará un breve ejemplo de cómo se desarrolla poco a poco una cadena utilizando una herramienta de simulación de Blockchain, dicha herramienta se puede encontrar en: $https$:

[1] Mempool es un almacenamiento en donde se guardan de manera momentánea todas las transacciones de los usuarios, una vez que las transacciones se almacenan en este espacio los mineros comienzan a seleccionar estas para posteriormente procesarlas (Iñigo, 2019).

//demoblockchain.org/blockchain.

En una red de Blockchain se ha minado el primer bloque, es decir, el bloque génesis. Supongamos que en esta red un bloque se considera válido si se encuentra un valor nonce que resuelva un hash que inicie con cuatro ceros, tal y como se muestra a continuación:

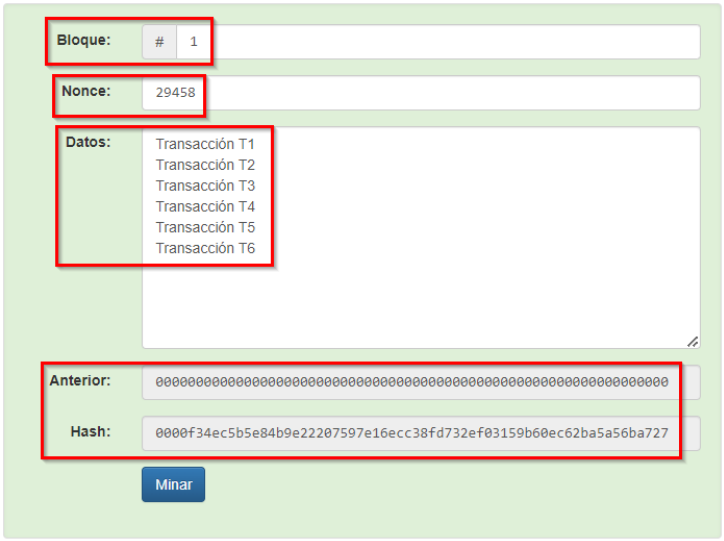


Figura 3.11: Bloque génesis.

Las características que se pueden observar son; su número de bloque, su valor nonce, las transacciones que contiene, el hash anterior (al ser el bloque génesis no tiene bloque anterior) y el hash que corresponde a su encabezado. Después de esto se realizan nuevas transacciones y se almacenan en un nuevo bloque. Tal y como se mencionó anteriormente, los mineros van a competir para encontrar el valor hash de su encabezado que comience con cuatro ceros. Una vez que este bloque sea validado de manera correcta deberá añadir su hash propio y además el hash del primer bloque minado. Este proceso daría como resultado una cadena de dos bloques:

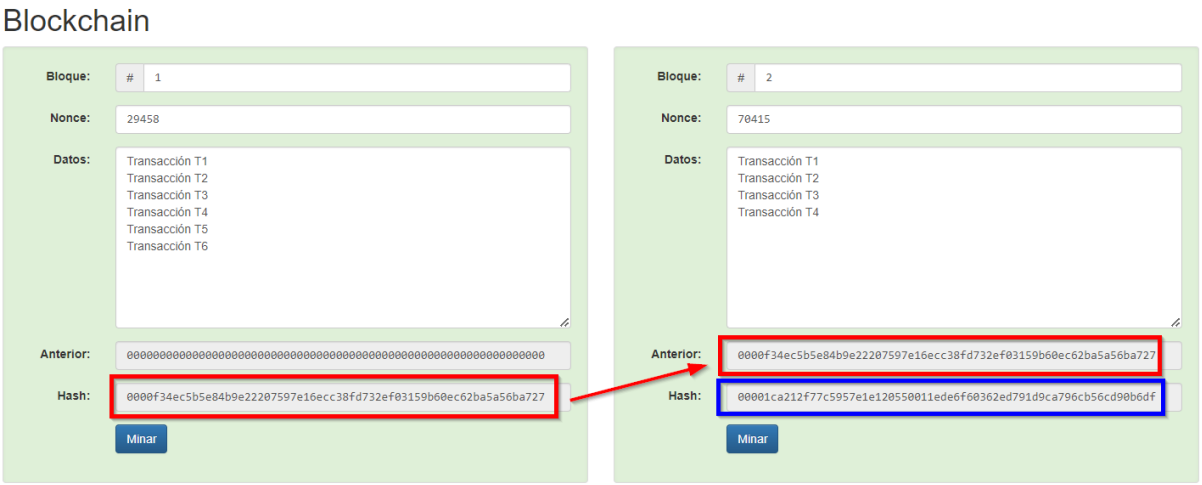


Figura 3.12: Cadena de dos bloques.

En la figura 3.12 se puede observar que el hash anterior del bloque 2 corresponde al hash del bloque 1. Determinando que estos bloques han sido añadidos y registrados a la cadena.

Suponiendo que nuevamente se han realizado más transacciones y ya se ha minado el bloque de

manera correcta, el resultado sería el siguiente:

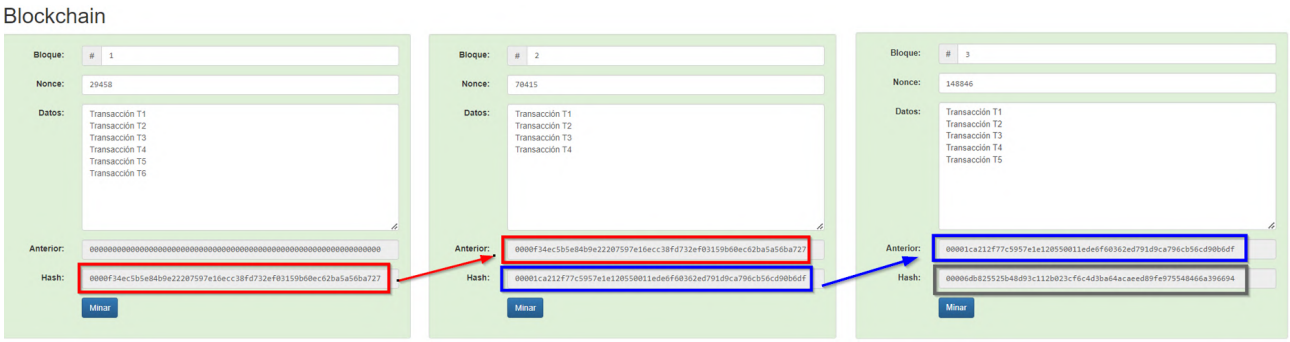


Figura 3.13: Cadena de tres bloques.

Mientras más transacciones se realicen, más bloques deberán ser minados y añadidos haciendo crecer la cadena poco a poco. Si un minero finaliza la validación y la prueba de trabajo más rápido que los demás, este publicará su bloque con nuevas transacciones. El resto de los mineros añadirán ese bloque a su respectiva cadena. Si el 51 % o más de la comunidad aprueban este bloque será añadido a la cadena.

3.4. Actualización y Consenso en Blockchain

Para que se actualice el historial de Blockchain cada vez que se mina un nuevo bloque se debe llegar a un consenso mediante un algoritmo. Un consenso en una red distribuida significa que la mayoría de los servidores o usuarios participantes están de acuerdo con el estado de la "verdad" actual del sistema. Una vez que se toma una decisión sobre un valor esta se vuelve definitiva (Álvarez Rojas, 2018).

3.4.1. Integridad en redes distribuidas

Mantener la integridad en una red distribuida es bastante complejo ya que se debe preservar la información durante el proceso de actualización que se gestiona. Para resolver este problema se utilizan los algoritmos de consenso los cuales se utilizan por todos los nodos participantes en la red. En el caso de bitcoin, todos los nodos se encargan de minar su propia copia del bloque nuevo, y una vez que aparece el primer bloque resuelto los demás mineros validan que este tenga las mismas características al suyo. Si se comprueba que el bloque es autentico se añade a la cadena.

3.4.2. Definición de consenso

El término consenso se define como un acuerdo realizado entre un grupo de nodos sobre la "verdad" de sus datos. Y aunque todavía no se tenga un concepto oficial sobre el consenso de Blockchain, el diccionario Oxford define el término consenso como *un acuerdo general* (Wattana Viriyasitavat, 2018). Por lo tanto, podemos definir a lo largo de esta tesis a un consenso como *el acuerdo de valor común entre un grupo de nodos participantes en los sistemas Blockchain*.

Se ha investigado constantemente sobre el consenso en los sistemas distribuidos con el objetivo de que sean resistentes a los fallos de los nodos, la partición de la red, los retrasos de los mensajes, los mensajes perdidos, y los mensajes comprometidos. En el contexto de Blockchain, los mecanismos de consenso permiten hacer frente a los nodos egoístas, defectuosos o maliciosos y garantizan que todos los nodos de la red estén de acuerdo en un estado global razonable. Los consensos deben abordar tres propiedades clave en base a las cuales se puede determinar su aplicabilidad y eficacia, las cuales se explican a continuación:

Seguridad. El consenso debe contar con propiedades de validez y acuerdo en sistemas distribuidos. La validez se define cuando varios procesos correctos proponen el mismo valor de un bloque, entonces dicho bloque habrá sido validado correctamente. El acuerdo por otro lado, garantiza que no existan dos o más procesos correctos que decidan de forma diferente. En general, un mecanismo de consenso es seguro si al menos un nodo honesto produce un resultado válido, entonces todos los demás nodos producirán o recibirán el mismo resultado. Los resultados son válidos e idénticos para todos los nodos, lo que se conoce como consistencia del estado compartido.

Tiempo de vida. Se conoce como la terminación en el consenso tradicional de los sistemas distribuidos, que establece que cada proceso correcto ha decidido finalmente un valor. Un mecanismo de consenso garantiza una mejor agilidad y rapidez si todos los nodos que participan finalmente producen un valor permitiendo que las peticiones correctas sean finalmente procesadas. No hay límite en el tiempo que se tarda en decidir un valor, de modo que esta propiedad no requiere que todos los nodos tengan un estado idéntico en un momento dado.

Tolerancia a fallos. Un mecanismo de consenso se considera tolerante a fallos si es capaz de resistir los problemas y fallos presentados en ciertos nodos que participen en el consenso independientemente de su ubicación física. Mientras los nodos defectuosos sean limitados, se seguirá alcanzando el consenso correcto. Los fallos de los nodos se presentan en dos categorías; los **fallos de parada o de colapso** se refieren a nodos que dejan de participar en el consenso ya sea de manera temporal o permanente. Por otro lado, los **fallos bizantinos** se refieren a nodos maliciosos especialmente diseñados para anular las propiedades de un protocolo de consenso. La segunda categoría fue bien identificada y caracterizada por Leslie Lamport como el Problema General Bizantino (Wattana Viriyasitavat, 2018).

3.4.3. Tipos de Consensos

Los mecanismos principales de consenso se mencionan a continuación.

Prueba de Trabajo (Proof of Work)
La prueba de trabajo o PoW se considera como el primer mecanismo de consenso introducido en bitcoin. En esta prueba los mineros compiten para resolver un problema matemático, y el primero en resolver dicho problema será el ganador. Después, si el 51 % de los demás mineros está de acuerdo con la solución encontrada el minero que lo haya encontrado será recompensado con una fracción de criptomonedas. Tal y como se ha mencionado con anterioridad, si se crean bifurcaciones debido a que más de un minero encontró la solución a un bloque se tomará como válida la cadena más larga, descartando las demás.

Esta prueba es utilizada por bitcoin y Ethereum, y a pesar de su gran efectividad y seguridad no es muy viable para muchos usuarios debido al consumo masivo de energía.

Prueba de Participación (Proof of Stake)
Este proceso se basa en que los validadores deben depositar algo de dinero en la red para participar dentro de la misma. En el consenso basado en esta prueba los validadores se turnan para proponer y votar por el siguiente bloque, y el peso del voto de cada validador depende del tamaño de su depósito. El proceso de validación de un nuevo bloque para obtener la fracción de la criptomoneda como recompensa se conoce como acuñación, a diferencia de PoW que se le llama minería.

Esta prueba ha sido propuesta por Ethereum, no requiere un gran desgaste de energía, y lamentablemente esta prueba es más propensa a los ciberataques ya que no se tiene un factor computacional para mantener la seguridad de la red.

Prueba de Participación Delegada (Delegated Proof of Stake)
Esta prueba es una variante del modelo anterior en donde todos los usuarios o validadores votan para seleccionar quienes serán los aprobadores finales de las transacciones de forma democrática.

Actualmente se utilza en bitshares [2], es rápido, escalable y de alta eficiencia energética.

Prueba de Autoridad (PoA)
Es una versión modificada de PoS en donde las transacciones y los bloques son validados por usuarios aprobados, llamados validadores. Esto significa que ciertos usuarios tienen derecho a ser una autoridad de aprobación si y solo si comprueban que su identidad es válida.

Se utiliza por Ethereum's Parity, en seguro, no requiere minería, mantiene un buen rendimiento y alta escalabilidad (Mohanty, 2019).

Tolerancia práctica a fallas bizantinas (PBFT)
Este método confía en que exista una diversidad de participantes éticos en el sistema distribuido, dichos participantes trabajarán en conjunto para realizar la validación de las transacciones. Y mediante el envío de mensajes entre los nodos validadores se intentará averiguar si existe algún nodo que perturba la red para aislarlo o descartarlo del sistema.

Se utiliza en Hyperledger, Ripple y Stellar, sin embargo, a pesar de su alto rendimiento en las transacciones se pierde completamente la descentralización (Álvarez Rojas, 2018).

3.5. Clasificación de Blockchain según el acceso a la información

Los tipos de Blockchain se pueden clasificar en función del acceso a la información de sus transacciones o contenido a validar. La diferencia entre los distintos tipos de blockchain está en el esquema del libro distribuido y quien puede participar en su sistema (Wattana Viriyasitavat, 2018).

3.5.1. Blockchain Pública

Las Blockchain públicas como Bitcoin y Ethereum, permiten que cualquiera pueda acceder y mantener el libro de contabilidad distribuido con permisos para validar siempre y cuando se ejecute el mecanismo de consenso establecido, determinando que no se requiere una entidad central que valide las transacciones. Una red Blockchain pública es completamente abierta y distribuida; cualquier usuario puede unirse, participar y abandonar el sistema libremente. Por lo tanto, este sistema funciona con nodos desconocidos y no confiables (Wattana Viriyasitavat, 2018).

Dado que todos los participantes pueden acceder a los datos y realizar transacciones en la red, se necesita encriptación y verificaciones avanzadas lo que requiere una gran capacidad computacional y una expansión limitada (JaeShup Oh, 2017).

3.5.2. Blockchain Privada

Por otro lado, en las Blockchain privadas los libros de contabilidad y las transacciones son compartidas y validadas por un grupo predefinido de nodos. El sistema solicita una determinada validación a los nodos que quieren formar parte del sistema. Los nodos autorizados son responsables de mantener el consenso, limitando así la cantidad de nodos a diferencia de los que forman las Blockchain públicas. La idea de Blockchain privada es recomendada para sistemas cerrados, en los que todos los nodos son de plena confianza (Wattana Viriyasitavat, 2018).

Una Blockchain privada requiere menos costos y no se pierde la autoridad de control del sistema ni la iniciativa dentro del servicio financiero. A diferencia de la Blockchain pública que proporciona

[2]BitShares es una plataforma financiera descentralizada que emplea una red blockchain pública que brinda acceso a su propio intercambio de activos digitales. Además, maneja su propia criptomoneda estable llamada Bit Share (BTS) (Garrido, 2023).

anonimato a sus nodos, en la Blockchain privada es posible identificar con más detalle a los nodos maliciosos que puedan propagarse para alterar la secuencia de ejecución o ejecutar transacciones no válidas. Además, las transacciones se gestionan con más rapidez, la expansión de la red es más sencilla y puede modificarse como desee el usuario, por lo que es apropiada para el servicio financiero. Blockchain privada es la red en la que el propietario genera y gestiona la Blockchain general. Esto es apropiado si el propietario de esta desea gestionar el Blockchain como un sistema centralizado (JaeShup Oh, 2017).

3.5.3. Blockchain Híbrida

Las Blockchain híbridas son el resultado de implementar propiedades tanto de las Blockchain privadas como las públicas, ya que incorporan muchas partes y los nodos principales se seleccionan inicial y estrictamente. Esta implementación es adecuada para sistemas semicerrados formados por unas pocas empresas, a menudo organizadas en forma de asociación.

Las propiedades de apertura de los datos pueden variar, implicando normalmente controles de acceso definidos por dicha asociación para tener control de acceso tanto en los participantes como en la información dentro de Blockchain. Aunque el sistema no sea completamente abierto, se pueden obtener algunos de los beneficios de la descentralización. Aunque la configuración de una blockchain hibrída sea susceptible a cambios, todos los tipos de Blockchain comparten las siguientes similitudes en cuanto a los beneficios que proporciona la tecnología Blockchain (Wattana Viriyasitavat, 2018):

- Operan en una red Peer-to-Peer (P2P) que proporciona cierto grado de descentralización,
- Múltiples nodos mantienen la integridad del libro de contabilidad a través de mecanismos de consenso, y
- La información se almacena en la base de datos de Blockchain que proporciona inmutabilidad, incluso cuando algunos nodos son defectuosos o maliciosos.

3.6. Diferencias entre Blockchain y otras tecnologías de bases de datos

Dando continuidad a los ejemplos mostrados sobre Blockchain, vamos a definir cómo se implementan los consensos dentro de una red de Blockchain, mostrando un ejemplo de su efectividad, (este ejemplo se pueden encontrar en $https://demoblockchain.org/distributed$).

Supongamos que se tienen tres nodos distintos lo cuales cuentan con su copia actual de la cadena y requieren competir para obtener el hash de cada bloque nuevo. Si los tres nodos (A, B y C) han validado de manera honesta sus bloques y cuentan con la misma copia se observaría lo siguiente:

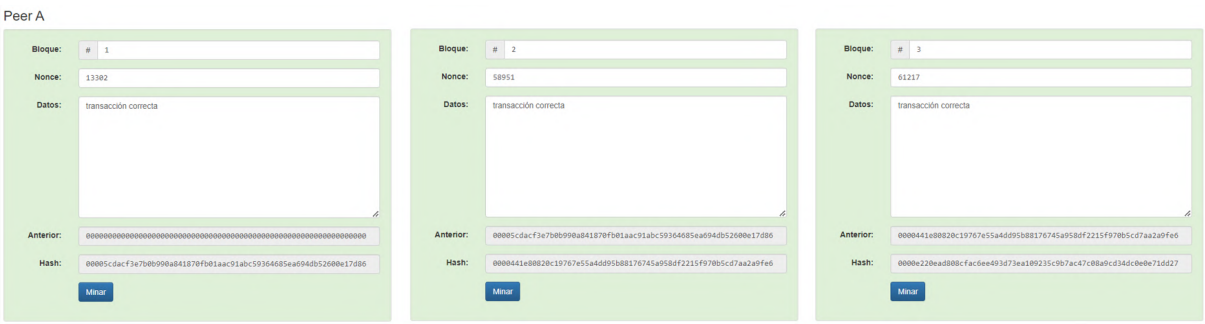


Figura 3.14: Nodo A.

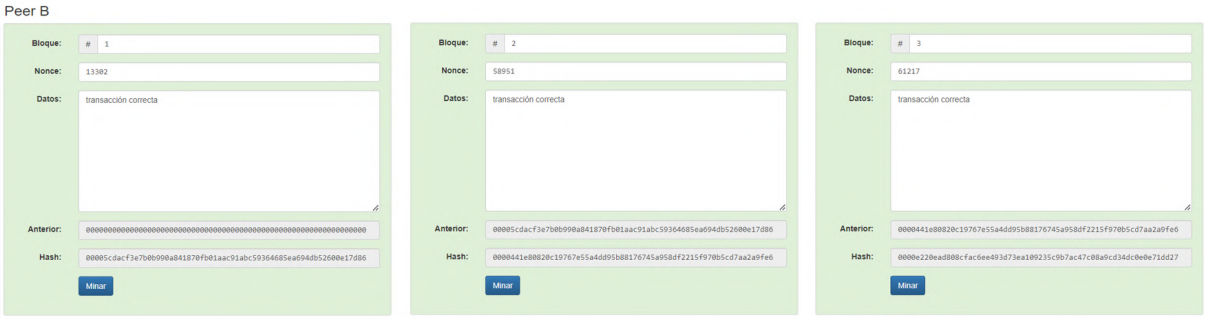


Figura 3.15: Nodo B.

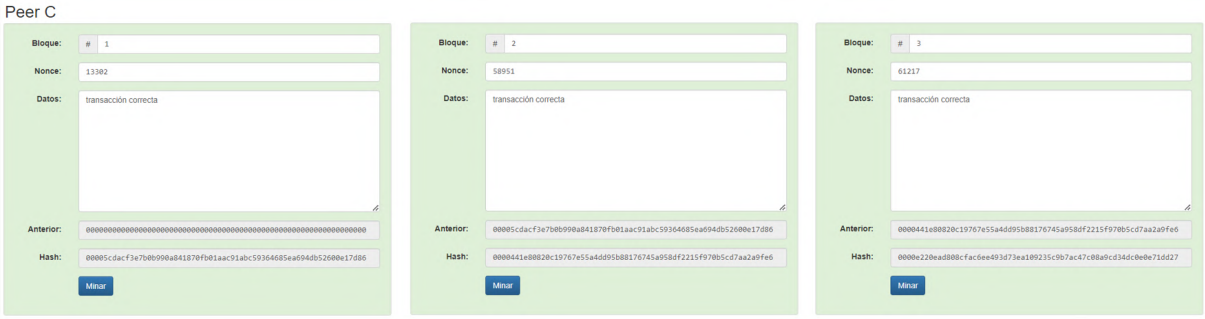


Figura 3.16: Nodo C.

Tal y como se observa en las figuras anteriores, los hashes de los bloques son los mismos para los tres nodos. Este es el resultado del consenso realizado por todos los nodos participantes en la red, manteniendo la integridad de la información. En la red de bitcoin, esto es representado con miles de nodos distintos y cada uno de ellos tienen la misma copia, teniendo así miles de copias en toda la red.

Suponiendo que de pronto uno de los nodos decide modificar la información de una transacción, llámese el nodo B. Este nodo al realizar dicha modificación obtendría lo siguiente:

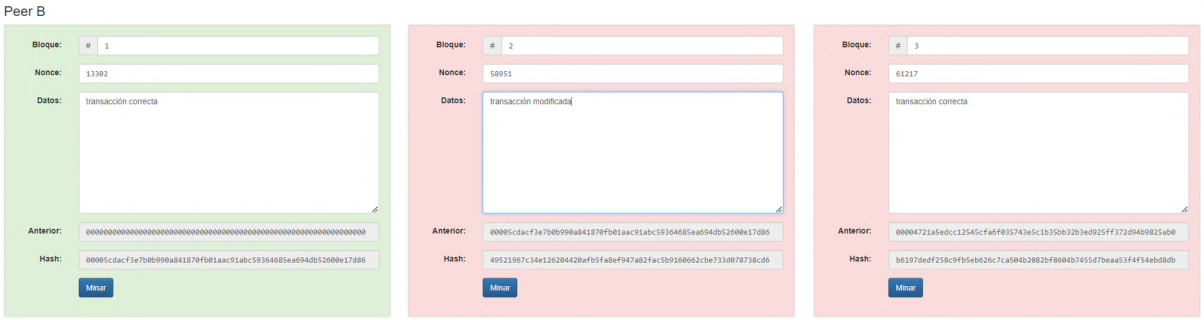


Figura 3.17: Nodo B modificado.

Tal y como se puede observar, hay una infracción en la cadena la cual nos muestra que el hash del bloque modificado también ha cambiado y no ha sido minado. En esta situación, el nodo B tendría que volver a minar dicho bloque para obtener el hash correcto de cuatro ceros. Sin embargo, aunque esto se realice de manera correcta se obtendría el siguiente resultado:

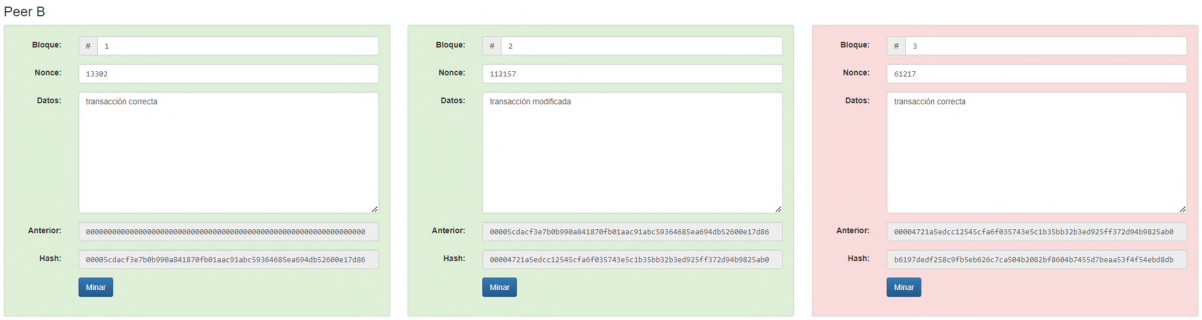


Figura 3.18: Nodo B modificado y minado.

Pese a que el bloque ya haya sido minado se observa que el resto de la cadena muestra un error debido a que los demás bloques también deben ser modificados. Esto significa que el nodo B tiene que minar cada uno de los bloques que preceden para que la infracción sea considerada válida. Considerando los conceptos definidos, esto sería prácticamente inútil ya que el resto de los nodos fácilmente se daría cuenta que el hash del bloque 2 no coincide con su propia copia. En este caso, el hash del bloque 2 no coincide con el hash que tienen los nodos A y C (véase Figura 3.14 y 3.16). Al darse cuenta de que esta cadena no coincide con la mayoría de la red, estos en consenso rechazarían la cadena alterada y la transacción del nodo B sería eliminada.

Capítulo 4

Aplicaciones de Blockchain

Como se ha definido con anterioridad en el Capítulo 2, Blockchain utiliza elementos importantes de la criptografía para su funcionamiento. Estos elementos como la elaboración de hashes y las llaves públicas y privadas permiten que esta tecnología tenga la seguridad de hoy en día.

4.0.1. Elementos criptográficos de Blockchain

Un hash es un algoritmo capaz de brindar un elemento único de salida con longitud fija en base a un dato de entrada. Este dato será único y constante, independientemente del tamaño o contenido de la entrada.

En Blockchain, se utiliza el árbol de Merkle para asegurar que no se pueda modificar ningún hash, ya que cualquier modificación en un bloque afectará a todos los bloques subsiguientes, manteniendo la integridad de la cadena.

4.0.2. Transferencia de criptomonedas

Cuando alguien envía criptomonedas (como BTC) a través de Blockchain, lo que se envía en realidad es una llave pública. Y tal y como se mencionó anteriormente, cada llave pública es creada en base a una llave privada. Esta última deberá ser tratada con cuidado y guardarse de manera correcta. La llave privada podría definirse como la llave maestra para el casillero de los usuarios dentro de Blockchain donde almacenan sus criptomonedas. Cuando se tiene una llave privada, se puede generar matemáticamente una llave pública la cuál será derivada de la anterior. Esta llave pública será traducida como un hash que indicará la dirección a la cuál otros usuarios podrán enviar criptomonedas. En pocas palabras, la llave pública es el número de cuenta del usuario, mientras que la llave privada es la NIP empleada para tener acceso a su cuenta del banco.

A continuación, se muestra de manera gráfica cómo funciona este proceso:

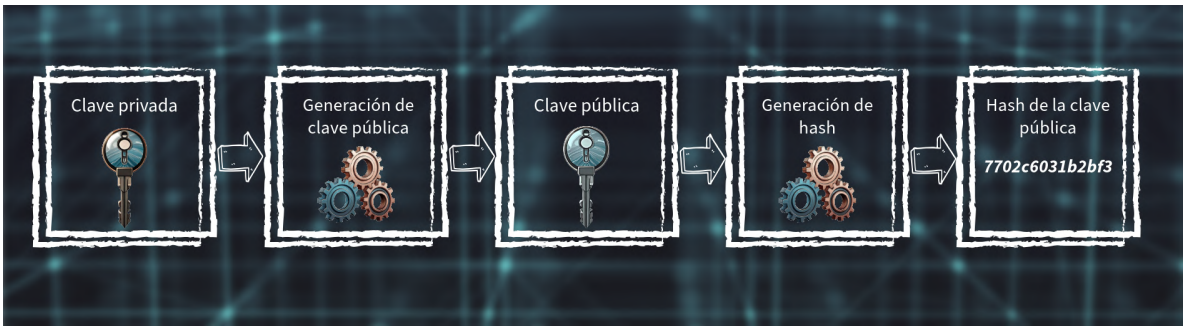


Figura 4.1: Relación de claves públicas y privadas.

De acuerdo con la Figura 4.1 se puede observar que la clave pública debe ser fácil de generar en

base a la llave privada previamente ya generada. Sin embargo, un punto importante a recalcar es que el algoritmo que se encarga de relacionar estas dos llaves no puede ser capaz de revertir el proceso. Es decir, que es muy difícil encontrar una llave privada en base a una pública, ya que el cifrado está programado para que no se pueda realizar este proceso. (Mohanty, 2019)

Tras repasar los principios criptográficos fundamentales utilizados en Blockchain, procederemos a explorar en detalle cómo opera esta tecnología, desglosando sus componentes más esenciales a detalle.

4.1. Contratos inteligentes (Smart Contracts)

Un contrato inteligente se define como un código ejecutable que se aplica sobre la cadena de bloques para facilitar, ejecutar y hacer cumplir un acuerdo entre partes no fiables sin la participación de un tercero de confianza. (Maher Alharby, 2017)

Un contrato tradicional se define como un acuerdo o negociación entre dos o más entes para hacer o anular algo a cambio de un activo, propiedad o cualquier cosa que sea de interés de las personas implicadas. Los contratos inteligentes mantienen la misma esencia, pero cambia la forma en que se lleva a cabo. Son capaces de administrar y ejecutar de manera automática y autónoma dicho acuerdo (Swan, 2015).

Los tres elementos de los contratos inteligentes que los distinguen son:

- **Autonomía.** Después de su inicio y ejecución no se requiere el contacto de los usuarios implicados.
- **Autosuficiencia.** Los contratos inteligentes son autosuficientes para reunir recursos, recaudar fondos mediante la emisión de capital o prestaciones de servicios, y en base a ello gastarlo en recursos necesarios para su funcionamiento como mayor capacidad de procesamiento o almacenamiento.
- **Descentralización.** No existen en un servidor fijo centralizado, sino que se distribuyen en todos los nodos participantes de la red de Blockchain.

Ejemplo práctico.
Supongamos que Mérida desea comprar un producto de $499 dólares. Si empleamos un contrato inteligente para esta adquisición, el código del contrato tendrá la instrucción de otorgarle el producto a Mérida una vez que este haya pagado el total de su precio. Cuando se cumpla la condición definida, el contrato se encargará de entregar el producto comprado a su respectivo comprador que en este caso es Mérida. Si diseñamos el diagrama de flujo para el contrato se tendría lo siguiente:

Figura 4.2: Transacción de Mérida mediante un Smart Contract.

Resumiendo, podemos definir que el objetivo principal de un contrato inteligente es ejecutar de manera automática los términos de un acuerdo una vez que se cumplen las condiciones especificadas.

Así, los contratos inteligentes prometen mayor efectividad en comparación con los sistemas tradicionales que requieren que un tercero de confianza aplique y ejecute los términos de un acuerdo.

4.1.1. Origen de los contratos inteligentes

El concepto de contrato inteligente surgió en 1993 cuando el criptógrafo estadounidense Nick Szabo definió este término. Szabo propuso un cambio en los contratos tradicionales proponiendo un sistema que permita que estos se ejecuten de manera automática, y a pesar de que no tuvo éxito por las limitaciones tecnológicas de ese tiempo, su situación cambió en 2009 con la aparición de Bitcoin. Los contratos inteligentes necesitaban un sistema de pagos que los pudiese poner en práctica, y fue ahí cuando entró la tecnología Blockchain. Su artículo donde define dicha tecnología de puede encontrar en: $https$: $//firstmonday.org/ojs/index.php/fm/article/view/548/469$.

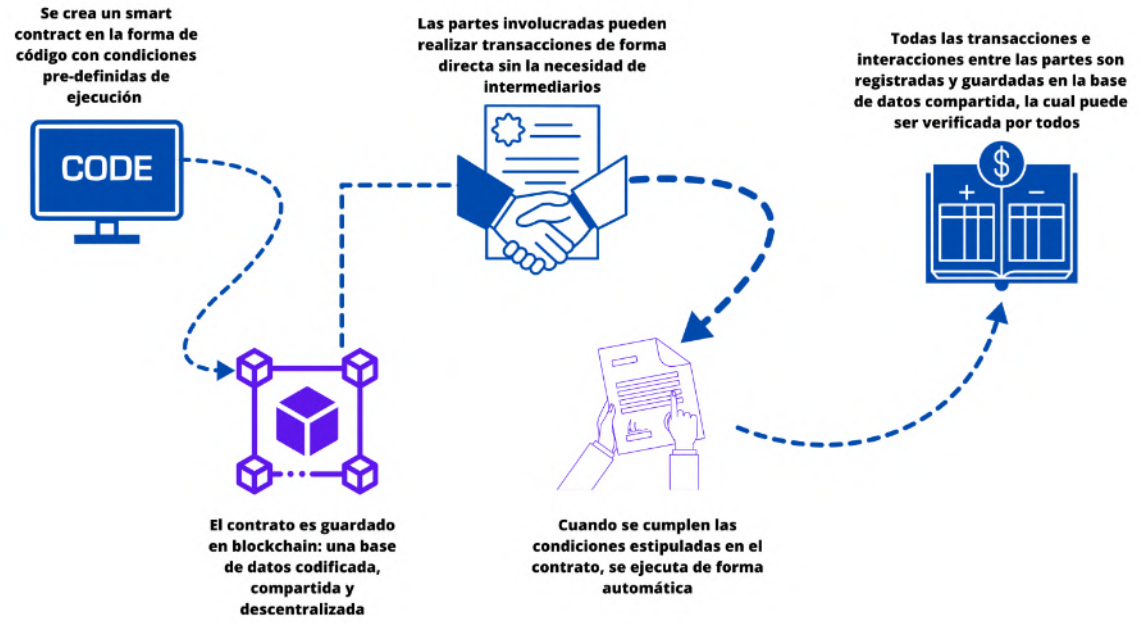


Figura 4.3: Sistema de un contrato inteligente (Calderon, 2023).

4.1.2. Composición y funcionamiento

Un contrato inteligente se compone de un saldo de cuenta, datos de almacenamiento y un código ejecutable. El estado del contrato se almacena en la cadena de bloques y se actualiza cada vez que se utiliza. La Figura 4.3 muestra cómo funciona el sistema de contratos inteligentes (Maher Alharby, 2017).

Cuando se concreta un contrato inteligente, se almacena en código dentro de un bloque. Después de ser minado será añadido a la cadena para su registro. Para realizar el pago total o parcial de lo negociado, los usuarios deben enviar una transacción a la dirección del contrato, con estos datos los nodos de consenso de la red se encargarán de validar que la operación se realice de manera correcta. Y después de validar dicha transacción el estado del contrato se actualizará de manera automática.

4.1.3. Tipos de contratos inteligentes

Existen dos tipos de contratos inteligentes: los deterministas y los no deterministas (Maher Alharby, 2017). Un contrato inteligente determinista es un contrato que no requiere ninguna información de una parte externa a la Blockchain para ejecutarse. Un contrato inteligente no determinista es un contrato que si depende de la información de una parte externa a la Blockchain para su ejecución. Por ejemplo, un

contrato que requiere la información meteorológica actual para ejecutarse, que no está disponible en la Blockchain.

Los contratos no hacen posible nada que antes era imposible, tan solo permiten que los problemas comunes se resuelvan de una manera que minimiza la necesidad de confianza. La confianza mínima a menudo hace que las cosas sean más convenientes al eliminar el juicio humano de la ecuación, lo que permite una automatización completa. (Swan, 2015)

4.1.4. Ventajas de los contratos inteligentes

Precisión

Dado que la mayoría de los contratos implican el intercambio de dinero en efectivo. Los contratos inteligentes pueden sincronizarse con criptomonedas como Ethereum, Lite Coin o Bitcoin para mejorar la solidez, la precisión y el rendimiento de todo el sistema. La automatización de los contratos inteligentes evita la mayoría de los problemas que se encuentran en los contratos tradicionales, ya que sus términos y condiciones son explícitos y más precisos.

Comunicación clara y transparencia

Cuando se establece un contrato, los cambios no podrán aplicarse fácilmente. Cada una de las transacciones realizadas por cualquiera de las partes del contrato será supervisada y controlada por otros nodos de la red en la Blockchain. Como resultado, se promueve la transparencia y se eliminan los problemas de fraude. Mientras un contrato tradicional requiere de un marco legal como intermediario, los contratos inteligentes sólo necesitan nodos de la red que garanticen que cada una de las transacciones realizadas sean precisas y válidas. Más adelante se hablará a detalle acerca del marco legal en México.

Rapidez y eficacia

Cuando se activa un contrato inteligente, las instrucciones especificadas se autoejecutan. Esto es posible con el uso de eventos desencadenantes [1] que se definen como condiciones al elaborar el contrato. Un evento desencadenante puede ser una fecha, una hora o incluso una actividad iniciada por una de las partes del contrato. Por ejemplo, para las organizaciones basadas en suscripciones en línea, renuevan la suscripción de un cliente una vez que se recibe una unidad específica de criptomoneda como pago.

Como tal, ya no se requiere de un sistema desarrollado por la organización para determinar los contratos con los clientes. Cada contrato es una entidad independiente, y cada transacción, independientemente de su origen, se valida de forma rápida y resistente.

Seguridad

Debido a que los contratos inteligentes son implementados a través de la tecnología Blockchain, estos requieren el uso de una red descentralizada formada por elementos no confiables. Y a causa de esto se implementa una alta encriptación de los datos y el uso de claves privadas y públicas para leer las transacciones en cada Blockchain, así como para ejecutar cualquier transacción. Esta medida permite aumentar la seguridad de estas tecnologías, debido a que al realizarse una transacción de cualquier nodo se tiene que validar por el resto de la comunidad.

Reducción de costos

Cómo se ha mencionado anteriormente, la implementación de contratos inteligentes a través de Blockchain no requiere de un intermediario para sus validaciones. Entre estos intermediarios se encuentra el personal jurídico. Al no existir este elemento, disminuyen los costos organizativos generales para las organizaciones, beneficiando más a aquellas empresas multinacionales que administran un gran número de contratos diarios o semanales. Sin embargo, es fundamental señalar que, a pesar de los aspectos

[1] Los eventos desencadenantes se definen como un evento tangible o intangible que, una vez violado o cumplido, hace que ocurra otro evento.

de seguridad, reducción de costes y eficiencia asociados a los contratos inteligentes, éstos al igual que muchos algoritmos computacionales no son perfectos y, por tanto, pueden estar sujetos a fallos.

Por ejemplo, la calidad y la ejecución del contrato dependen en gran medida de los datos de entrada, que es básicamente la versión codificada del contrato. Si se presentan errores en la configuración de los contratos inteligentes, estos tendrán efectos negativos y menor calidad en los resultados obtenidos. (Nzuva, 2019).

4.1.5. Limitaciones de los contratos inteligentes

A pesar de las diversas ventajas señaladas anteriormente, también es importante señalar que los contratos inteligentes están asociados a diversas limitaciones, la cuales restringen su aplicación en diversos entornos de la vida real. (Nzuva, 2019)

Inmutabilidad

Dado que los contratos inteligentes se escriben como una pieza de código, una vez que los datos son establecidos no se pueden modificar fácilmente. En los contratos tradicionales, se suele recurrir a la modificación de los términos y condiciones, especialmente en los contratos a largo plazo cuya ejecución depende de la dinámica de la vida real, y las condiciones que no dejan de cambiar.

Debido a la precisión que presentan los contratos inteligentes una vez establecidos, estos dan lugar a una gran variedad de problemas prácticos, sobre todo en lo que respecta a la facilidad para modificar los términos del contrato en función de diversas situaciones externas.

Los contratos convencionales tienen disposiciones que permiten la anulación, incrustación y modificación de estos. Sin embargo, la implementación de contratos inteligentes difícilmente podrán cumplir con estos objetivos, ya que esto requeriría más costos y consumo de tiempo, dependiendo de la organización en donde se implemente la negociación.

Secreto contractual

Blockchain implica compartir el contrato inteligente en todos los nodos de la red, ya que todas las transacciones se registran en el libro mayor utilizando permisos codificados en cada uno de los nodos. Sin embargo, no hay privacidad en la ejecución del contrato. Esto significa que a pesar de que los nodos sean anónimos en sus operaciones, el libro de contabilidad se mantiene público, y por lo tanto, las transacciones serán visibles para todos los nodos de la red.

Aunque la esencia de los contratos inteligentes es mantener un libro de contabilidad público que sea visible para todas las partes de la red y controlar la validez y exactitud de los impuestos, también es necesario desarrollar un protocolo que pueda ayudar en la verificación de las transacciones sin leer necesariamente el contenido de la transacción. Esto se debe a que, aunque los participantes y el origen de la transacción sean anónimos, el contenido no lo es y, de hecho, cada nodo puede leer el contenido de la transacción. En base a lo anteriormente mencionado es fundamental desarrollar medidas para disminuir estos problemas de privacidad, ya que la seguridad no consiste únicamente en el anonimato y la encriptación, sino que también implica garantizar que el contenido de la transacción está protegido frente al acceso de terceros. Por lo tanto, este aspecto de los contratos inteligentes aún no se ha abordado plenamente.

Adjudicaciones legales y ejecutabilidad

Tradicionalmente, el establecimiento de un contrato legítimo abarca varios elementos que lo hacen legalmente válido. Las características clave que validan legalmente un contrato son; la oferta de una persona o una empresa, la aceptación de la otra persona o la otra empresa, una promesa, una contraprestación y la reciprocidad de la capacidad jurídica y, en algunos contratos, un instrumento escrito. Aunque estos elementos de un contrato son muy importantes, algunos de ellos no son aplicables a los contratos inteligentes.

Por ejemplo, el sector financiero está sujeto a inmensas regulaciones por parte del gobierno, y a pesar de la concesión de licencias y aprobaciones asociadas, la validez legal de los contratos inteligentes aún no se ha establecido y sincronizado con la ley de contratos, así como otras leyes que dan las

transacciones financieras. Por lo tanto, es necesaria la traducción del marco legal que rige los contratos en la lógica del software para garantizar que, además de que el contrato inteligente sea autoejecutable, también se adhiera a la normativa legal de los contratos conocidos. (Nzuva, 2019)

4.1.6. Marco regulatorio en México

Actualmente, no existe un consenso universal entre aquellos que estudian los contratos inteligentes respecto a su concepto, alcance, naturaleza jurídica, aplicación y tampoco la jurisdicción en la que recaen. A pesar de que los contratos inteligentes continúan en constante evolución no se descarta que puedan resolver los problemas de corrupción y transparencia en México. Además, su aplicación en el comercio electrónico podría reforzar la confianza de los consumidores, resolviendo problemas de entrega de productos, reembolsos, cancelación de productos, cobros indebidos, etc.

Para que los contratos inteligentes tengan reconocimiento y una adopción a gran escala en nuestro pais es importante plantear las bases que garanticen la protección de datos personales. Sin embargo, a pesar de que el uso de esta tecnología no incumple con la GDPR [2] ni la LFPDPPP [3], la legislación existente no es suficiente para tener la certeza de la protección de los datos de sus usuarios.

En México no se cuenta con una regulación específica sobre los contratos inteligentes, sin embargo, esto no implica que lo realizado con estas tecnologías esté aislado de la aplicabilidad de los derechos, y tampoco que no tenga consecuencias jurídicas. Los contratos inteligentes son válidos en la legislación, y además cumplen con principios de libre contratación y equivalencia funcional adoptado en el Código de Comercio.

Algunas propuestas que podrían permitir a la legislación mexicana adaptar o regular la implementación de los contratos inteligentes con la finalidad de crear caminos que promuevan su uso pueden ser mediante:

- Generación de un entorno jurídico seguro
- La inclusión de normas genéricas que preparen al marco jurídico a los cambios tan rápidos que puedan presentarse en la tecnología.
- Formar un equipo multidisciplinario conformado por programadores, abogados, economistas y contadores que participen en la legislación y actualización de las nuevas necesidades de la sociedad.

El estudio de los contratos inteligentes no está concluido, ya que, no existe un consenso universal que respalde su naturaleza jurídica. Sin embargo, esto no descarta que en un futuro se pueda implementar debido a que, al aplicarse de manera correcta puede traer grandes beneficios a la sociedad de nuestro país, en donde es muy necesaria la transparencia, el cumplimiento de las obligaciones sin discrecionalidad, inversión económica etc. (Arteaga, 2023)

4.1.7. Implementación de contratos inteligentes

La implementación de contratos inteligentes abre incontables posibilidades para la transferencia y gestión de activos digitales, transformando la manera en que organizaciones, clientes y proveedores interactúan. Los contratos inteligentes permiten automatizar procesos tradicionales, como transacciones financieras o la ejecución de acuerdos legales, ofreciendo una alternativa digital más eficiente y segura.

[2] General Data Protection Regulation (Reglamento General de Protección de Datos) es un reglamento creado por el Consejo de la Unión Europea y la Comisión Europea con la intención de proteger los datos de las personas dentro de la Unión Europea.

[3] La Ley Federal de Protección de Datos Personales en Posesión de Particulares es una ley instaurada en México desde el año 2010 con la intención de regular el manejo de datos personales en poder de las empresas.

Transferencia de activos digitales

Los contratos inteligentes son capaces de transformar la transferencia tradicional de activos en una transferencia digital. Por ejemplo, si se trata de una organización que maneja tarjetas de crédito, como un banco, esta puede almacenar la información del importe gastado y los saldos de las cuentas en una base de datos principal. Dicha base de datos dispondrá de una tabla con información de las transacciones realizadas como el importe, el propietario, el tipo de activo entre otros (Fairfield, 2014).

Supongamos que se tiene una base de datos en donde dos usuarios tienen los siguientes datos de entrada; *"Mérida", "$20"* y por otro lado, *"Félix", "$0"*.

La interpretación del primer registro indicaría que Mérida tiene un saldo de $20, mientras que Félix tiene un monto de $0. Supongamos que Mérida transfiere $15 a Bob, al realizar la transacción Mérida tendría $5, mientras que Félix pasaría a tener $15 tal y como se muestra en la figura 4.4.

Registro de Mérida en BTC	Registro de Félix en BTC
Saldo actual $20	Saldo actual $0

Registro de Mérida en BTC	Registro de Félix en BTC
Saldo actual $20	Saldo actual $0
Mérida transfiere $15 a Félix	Félix recibe $15 de Mérida
Saldo actual $5	Saldo actual $15

Figura 4.4: Fondos iniciales y finales de Mérida y Félix respectivamente.

Complementando lo anteriormente mencionado, se puede determinar que la transacción realizada es un ejemplo de transferencia de activos digitales, ya que el efectivo se considera un activo que puede expresarse en forma digital. Lógicamente, aunque los usuarios finales reciben el saldo actualizado de la cuenta al instante, lo que ocurre es la manipulación de los registros almacenados en la base de datos tal y como funciona con las cuentas bancarias.

4.1.8. Aplicaciones de contratos inteligentes

Una de las aplicaciones más frecuentes está en los préstamos. Un contrato inteligente puede almacenar cualquier operación sobre un préstamo con sus respectivas condiciones y políticas dentro de Blockchain. Asegurando una propiedad como garantía para poder proporcionar dicho préstamo. Si el pago solicitado se realiza de manera correcta y cumpliendo los acuerdos la operación será finalizada. Sin embargo, si no se efectúa el pago según las condiciones establecidas, la propiedad que se establezca como garantía al préstamo quedará automáticamente transferida. Esta transferencia se puede realizar anulando la llave privada que da acceso a la propiedad y generando una nueva que pasaría a ser propiedad de la cuenta que realizó el préstamo.

Las apuestas o predicciones de mercado son otro tipo de contrato inteligente. Dos partes envían una cantidad al contrato inteligente en base al resultado de una predicción o evento. Una vez que se lleve a cabo el evento y se tenga un resultado, el contrato se encargará de transferir la cantidad depositada por

las dos direcciones a la dirección que haya acertado en la predicción. (Joaquín López Lérida, 2016)

Los contratos inteligentes también pueden implementarse en sistemas de compromiso como Kickstarter [4]. Las personas realizan compromisos en línea que están codificados en una cadena de bloques, y si o solo si se alcanza el objetivo de recaudación de fondos del empresario, se liberarán los fondos de Bitcoin de las billeteras de los inversores. Hasta que no se reciban todos los fondos no se liberará ninguna transacción. Además, la tasa de consumo, el presupuesto y el gasto del empresario serían ubicados por las transacciones de salida posteriores de la dirección de Blockchain que recibió la recaudación de fondos (Swan, 2015).

Una posible aplicación está en las herencias. Estas se pueden automatizar de forma que permitan validar un fallecimiento en base al acceso de un registro oficial de personas fallecidas, una vez hecha la actualización de la información la propiedad se podrá transferir a la dirección Blockchain receptora de la misma. Esta transferencia se puede hacer igualmente anulando las llaves privadas del propietario original y proporcionando una llave privada nueva al heredero de acuerdo a las condiciones y políticas establecidas (Joaquín López Lérida, 2016).

4.2. Aplicaciones empresariales

4.2.1. Agro

Dentro de las diferentes aplicaciones que hay en cadena de suministro, hay una muy importante que es la agronomía. Con apoyo de la corporación multinacional de tiendas Walmart se logró mejorar con más claridad el abastecimiento de alimentos con ayuda de Hyperledger Fabric, una plataforma de código abierto. Gracias a su socio tecnológico, IBM. Walmart cambió su cadena de suministro con la intención de volverse completamente autónoma mediante la implementación de una red Blockchain privada.

Con ayuda de este proyecto basado en Blockchain en unión de dos socios líderes en sus industrias como Walmart e IBM, se consiguió brindar certificados de autenticidad en los productos permitiendo verificar a los vendedores, proveedores, distribuidores y transportistas que participaron en todo el proceso de suministro de los productos. Con esto, se podría tener acceso a la fecha de vencimiento del producto, la temperatura del almacén, origen de la granja, números de lote, la calidad del suelo, fertilizantes utilizados, etc. Toda esta información sería compilada y relacionada al paquete de los productos mediante códigos QR incorporados aumentando así la confianza en el producto a consumir y todo a una velocidad sin precedentes, pasando de un tiempo inicial de 7 días a tan solo 2.2 segundos de validación.

Todo esto permitió obtener un seguimiento de trazabilidad de más de 25 productos de 5 proveedores distintos, y una expansión escalable a más productos y proveedores. Todo gracias a la tecnología Blockchain brindando más oportunidades y mejoras a los consumidores y a las empresas que actúan en el sector agro. (Anirudh, 2022)

4.2.2. Manufactura

Toda aplicación en manufactura debe estar ligada a un proceso de abastecimiento y distribución, y un ejemplo fundamental de eso es la producción de inmunización (vacunación) en India por NITI Aayog con el objetivo de mantener una infraestructura unificada y mejorada mediante Blockchain.

La India ha sufrido un gran índice de mortalidad infantil a nivel mundial, causada por enfermedades prevenibles como el sarampión, rubéola, hepatitis, neumonía, diarrea y malaria, etc.

La aplicación de la tecnología de Blockchain en un programa de vacunación para una población tan grande y diversa como la India, podría traer los siguientes beneficios:

[4] Kickstarter es una plataforma de crowdfunding que recauda dinero del público con el objetivo de crear un proyecto de financiación definiendo también una fecha límite. Si el contrato no alcanza la meta de financiamiento, no se realiza la transacción de fondos (Millán, 2023).

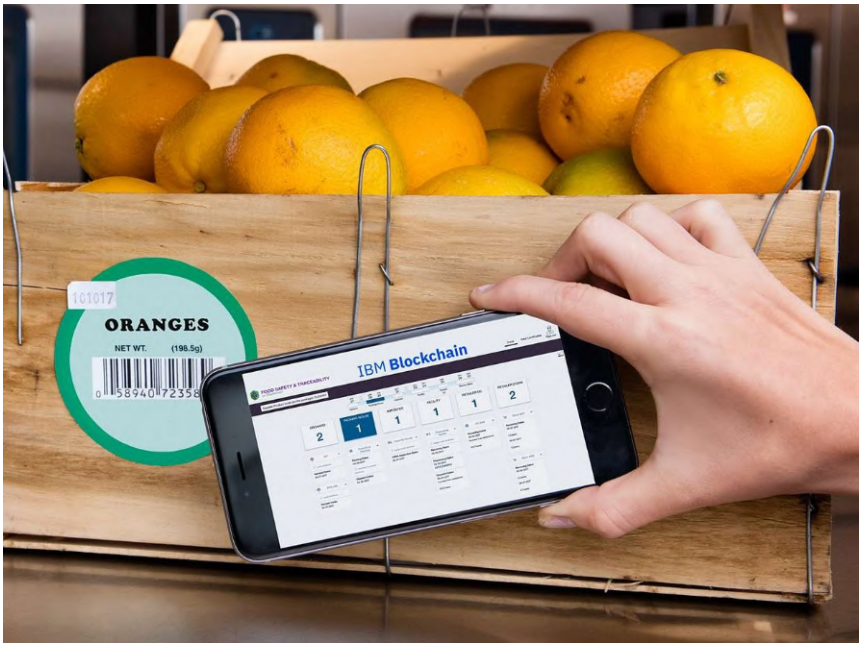


Figura 4.5: Escaneo de productos mediante un código QR (Anirudh, 2022).

- Datos precisos, fiables y en tiempo real para mantener un seguimiento constante de la cobertura y consumo de vacunas para facilitar su planificación y evaluación.
- Gestión de la cadena de suministro de vacunas (cadena fría) para garantizar que las vacunas se almacenen y transporten a la temperatura recomendada desde el punto de fabricación hasta el punto de distribución. Mediante Blockchain se podrá saber quién quiere un determinado tipo de vacuna, dónde y cuándo mediante un código QR a cada contenedor junto con un localizador GPS.
- Informar a los padres o tutores mediante un sistema automático de alerta que notifique a los padres afectados sobre los recordatorios, sitios y progreso de vacunación mediante un SMS.

La integración de los datos de vacunación en una infraestructura de cadena de bloques reforzaría las transferencias y la entrega de vales de vacunación, además podría crear una base para la innovación futura como el uso de contratos inteligentes para recompensar a los trabajadores sanitarios. (Arnab Kumar, 2020)

4.2.3. Salud

Entre la gran diversidad de activos que se pueden intercambiar con ayuda de la tecnología Blockchain se encuentran los activos de salud digital, lo cual se conoce como Blockchain Health. El beneficio clave detrás de esta idea es que Blockchain proporcione una estructura que permita almacenar datos de salud en su base de datos, de modo que estos se puedan analizar manteniendo su privacidad. Y para compensar dicha contribución y uso de datos se utilizaría un valor económico incorporado, conocido como Healthcoin. Dicho valor se define como la moneda o token empleada para el gasto en salud la cuál podría permitir que los servicios en los planes nacionales de salud puedan clasificarse y pagarse con este. (Swan, 2015).

Los registros de salud personales podrían almacenarse y administrarse a través de Blockchain como un gran sistema de registro médico electrónico. Codificando la dirección digital de los pacientes como activos digitales para colocarse en la cadena de bloques como moneda digital. Las personas pueden otorgar a los médicos, farmacias, compañías de seguros y otras partes acceso a sus registros de salud según sea necesario a través de su clave privada (Swan, 2015).

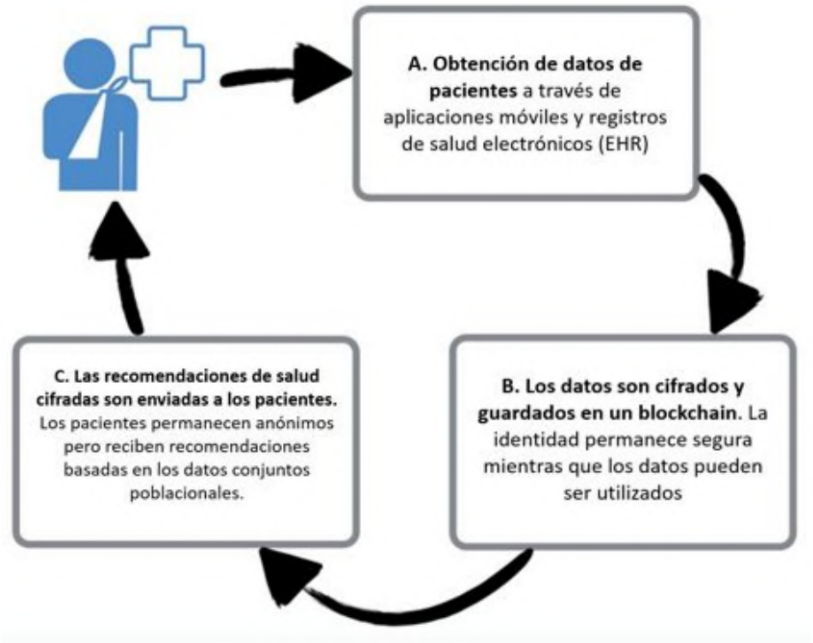


Figura 4.6: Aplicación del blockchain sanitario para recomendaciones basadas en datos conjuntos poblacionales (Joaquín López Lérida, 2016).

El acceso a la información de salud privada para determinados tratamientos sería de forma automática sin depender de la burocracia, su localización, saturación de servicio etc. El aprovechamiento de Blockchain generaría para cada ciudadano un registro personal de salud que tendría múltiples aplicaciones tanto a nivel personal como a nivel de descendencia. Cada paciente sería dueño de su historial sanitario, y este podrá compartirlo con quien quiera de forma anónima o de forma verificada (Joaquín López Lérida, 2016).

4.2.4. Gobierno

Uno de los proyectos más ambiciosos de Blockchain está en las aplicaciones descentralizadas orientadas al gobierno y los ciudadanos. Esto no se limita únicamente a que los ciudadanos puedan votar por las decisiones de su país, se trata de implantar una dinámica en la administración que no ha sido posible hasta la fecha. La urgencia en el cumplimiento de acciones y promesas políticas, podrían llevarse a cabo a través de Smart Contracts mediante la aplicación de técnicas relacionadas a Blockchain 3.0 asociadas a IoT y BigData. Por lo tanto, las necesidades individuales por los ciudadanos podrán ser atendidas, las organizaciones ciudadanas podrían optar por mejores o peores servicios en función de sus necesidades en ciertas áreas. Por ejemplo, un grupo de ciudadanos podría decidir mejorar el servicio escolar pagando por ello. Y esto sería posible de forma automática, asignando un incremento en sus impuestos acordados de antemano que automáticamente repercutiría, vía Smart Contracts, en la calidad de los servicios recibidos.

Se han propuesto tokens llamados *AccidentCoin* los cuales servirían para que las personas involucradas en accidentes puedan pagar por la reparación de las vías de forma automática. Otro tipo de tokens son los *RoadCoincon* con los que se pagarían impuestos de forma automática en función del uso de carreteras. Los usuarios en posesión de estos últimos tokens de carretera podrían opinar con sistemas PoS (Proof of Stake) sobre la modificación de los Smart Contract asociados a la administración de estas.

4.2.5. Conclusiones

Los contratos inteligentes presentan gran variedad de ventajas significativas como la precisión, la rapidez y la seguridad en la ejecución de acuerdos, además de la reducción de costos operativos. Sin embargo, pese a esto, también enfrentan desafíos relacionados con su inmutabilidad, la privacidad de los datos y la integración en el marco legal existente.

La implementación de contratos inteligentes promete revolucionar la manera en que se realizan y gestionan los acuerdos en diversos campos, desde el financiero hasta el gubernamental, permitiendo una mayor eficiencia, seguridad y transparencia. La adaptación de la legislación para abordar sus desafíos será clave para maximizar su potencial y asegurar su integración exitosa en la sociedad. Estos ejemplos ayudarían a generar un mundo más equilibrado, democrático y sin la necesidad de intervención de terceras partes. Permitiendo un sistema de autocontrol de activos que relaciona las definiciones de Big Data y la IoT creando lo que se conoce como Ciudades Inteligentes, lo cual se define más adelante. (Joaquín López Lérida, 2016)

Capítulo 5

Ecosistema Blockchain

La tecnología Blockchain no solo puede reinventar todas las categorías de mercados monetarios, pagos, servicios financieros y economía, sino que también tiene la capacidad de ofrecer posibilidades de reconfiguración similares para todas las industrias y de una manera más amplia. Este nuevo modelo, basado en la descentralización, promete reducir los desacuerdos y aumentar la eficiencia de las actividades a una escala sin precedentes, superando con creces los límites de los sistemas actuales.

Gracias a la descentralización como modelo general de Blockchain es posible interconectar a todos los humanos a un alcance universal y global. Algo que antes no era posible. Con la asignación de recursos cada vez más automatizada de activos del mundo físico y de activos humanos puede ser posible esta interconexión.

Facilita la coordinación y el reconocimiento de todo tipo de interacción humana, aumentando el nivel de colaboración y posiblemente dando paso a un futuro camino para la interacción entre humanos y máquinas. Además, no es sólo un mejor modelo organizacional funcional, práctico y cuantitativo; al requerir consenso para operar, el modelo también tiene el potencial de una mayor libertad, igualdad y empoderamiento cualitativamente. (Swan, 2015).

Blockchain se propone como una solución integral, capaz de aportar mejoras significativas tanto en el aspecto funcional y práctico como en el cualitativo, prometiendo una sociedad más conectada, equitativa y eficiente. Su aplicación va más allá de la mera transferencia de valor, ofreciendo un nuevo marco para la gestión de datos, la propiedad intelectual y las relaciones contractuales, entre otros. En resumen, Blockchain no es solo una tecnología, sino un cambio de paradigma que ofrece una gran variedad de posibilidades para reimaginar y mejorar nuestra forma de interactuar, trabajar y vivir, marcando el comienzo de una era de innovación y cooperación sin precedentes.

5.1. Big Data

En términos simples, Big Data (datos masivos) es la expresión que define a una gran cantidad de datos la cual crece de manera exponencial con el paso del tiempo. Comprende el análisis, la autenticación de datos, búsqueda, intercambio, almacenamiento, transferencia, visualización, consulta y privacidad de la información. También se emplea en el análisis predictivo para extraer valor de los datos, encontrar patrones en grandes cantidades de información y definir un tamaño de conjunto de datos. Con ayuda de Big Data también se puede conducir a la toma de decisiones con más confianza (Aritmetrics, 2023).

Estos conjuntos de datos son tan voluminosos y complejos que ningún software de procesamiento de datos convencional tiene la potencia de almacenarlos y procesarlos de manera eficiente.

5.1.1. Las tres V de Big Data.

Big Data abarca datos que constan de una mayor variedad, volúmenes crecientes y a una velocidad superior. Esto se conoce como "las tres V" las cuales se definen a continuación (Oracle, 2023):

- **Volumen.** Big data procesa grandes volúmenes de datos tanto estructurados como no estructurados de baja densidad. Pueden ser de datos de valor desconocido, feeds de datos [1] de Twitter, flujos de clics de una página web o aplicación para móviles, o equipo con sensores. Para algunas organizaciones, esto puede requerir decenas de terabytes de datos, petabytes y hasta exabytes.

- **Velocidad.** Se refiere al ritmo al que se reciben los datos y al que se aplica alguna acción. La mayor velocidad de los datos normalmente se transmite directamente a la memoria, en vez de escribirse en un disco. Esta velocidad puede variar dependiendo de la cantidad de datos a procesar, y el orden en la transferencia de estos. Algunos autores definen las fases de Big Data como; generación, adquisición, almacenamiento y análisis de datos (Casas, 2019).

- **Variedad.** Hace referencia a los diversos tipos de datos disponibles tanto estructurados como no estructurados. Actualmente se maneja gran variedad de datos, tales como emails, fotos, videos, sistemas de monitorización, archivos PDF, ficheros de sonido, etc. Estos datos requieren un preprocesamiento adicional para poder obtener significado y habilitar los Metadatos:. Algunas de las herramientas que se pueden implementar para procesar los datos no estructurados son; plataformas escalables, desarrollo de algoritmos, procesos de depuración y creación de estructuras complementarias.

5.1.2. Blockchain & Big Data

Big Data es uno de los sectores de más rápido crecimiento en el mundo ya que las empresas desean obtener información sobre los patrones de uso de sus consumidores, los cuales se vuelven más difíciles de gestionar con el tiempo. La cantidad de datos masivos se validan utilizando modelos estadísticos avanzados y minería de datos. Con el aumento de los datos, el análisis se vuelve cada vez más complejo, ya que se presentan problemas como los datos corruptos o sucios, datos inaccesibles y problemas de privacidad. Y a medida que el Big Data aumenta de tamaño, la red de dispositivos conectados crece a tal grado que las empresas se vuelvan más susceptibles a posibles incidentes de seguridad.

Las empresas que se ocupan de grandes bases de datos deben asegurarse de que sus datos estén limpios, seguros, sin modificaciones y que provengan de una fuente legítima. Deben asegurarse de que la última versión esté sincronizada entre todos los centros de datos en tiempo real y también se tiene que asegurar la disponibilidad de la información.

Asegurar e interpretar cantidades tan grandes de información no es una tarea fácil. Y es aquí donde entra Blockchain. Esta tecnología podría solucionar muchos de los desafíos de la gestión y el análisis de Big Data ya que cuenta con cuatro propiedades esenciales: descentralización, distribución, inmutabilidad y seguridad.

- **Descentralización.** No se tienen puntos de fallo, ya que los datos son distribuidos a través de múltiples nodos.

- **Seguridad.** Mediante los algoritmos de consenso descentralizado, la criptografía y la gran potencia informática necesaria, valida los datos de forma tal que se garantiza su integridad, privacidad y su integridad.

[1] Un feed de datos se define como un archivo que contiene información estructurada, vigente y actualizada. Se suele utilizar en sitios web, aplicaciones y otras herramientas online. Por ejemplo, los feeds de noticias y los feeds de productos (Axinte, 2023).

- **Distribución.** Comparte cada transacción en toda la red, haciéndose más segura por diseño. Impidiendo su falsificación debido a la arquitectura de red. Esto ayuda a que su proceso sea más transparente debido a que no se puede cambiar nada sin la aprobación de cada servidor en la red, todos pueden ver los cambios realizados en todo momento.

- **Inmutabilidad.** La información permanece en el mismo estado durante el tiempo que la red exista. Si la cantidad de datos que necesita ser examinada se modifica de alguna manera, el análisis resultante tendrá poco valor.

Las ventajas y aportaciones de integrar Blockchain con Big Data son muchas. Su adopción en combinación es capaz de traer resultados incomparables para las empresas "de todos los tamaños". Existe una gran variedad de beneficios que Blockchain puede aportar a los sistemas de análisis de datos. Puede beneficiar a Big Data con la garantía de la calidad, accesibilidad y seguridad de los datos. Más datos de calidad con más ideas significa más valor ya que permite una mejor gestión de grandes volúmenes y variedad de información. En la siguiente tabla, se muestran algunos de los beneficios: (Meijer, 2019):

Beneficios	**Concepto**
Mejor calidad de datos	Blockchain sustituye los métodos de almacenamiento tradicionales permitiendo a las empresas una mejor calidad en los datos ya que están más completos y estructurados. Aumenta la precisión y facilita un análisis exhaustivo para ofrecer información rica y confiable para el negocio.
Facilita el acceso a los datos	Al almacenar la base de datos en una cadena de bloques, se desarrolla una sola fuente de información inmutable donde únicamente podrá acceder el personal autorizado a los registros deseados.
Gestión del intercambio de datos	Los datos obtenidos en un estudio pueden almacenarse en una red Blockchain. De modo que, los equipos del proyecto no repitan el análisis de datos ya realizado por otros equipos, ni reutilizar erróneamente los datos que ya se han recopilado.
Prevención de fraudes	Las instituciones financieras verifican cada transacción en tiempo real, y ya no sería necesario evaluar los datos históricos después de presentarse el fraude. En lugar de analizar los registros de un fraude que ya sucedió, los bancos pueden identificar transacciones riesgosas o fraudulentas en el momento y prevenir la estafa por completo. Si las instituciones financieras aprovechan esta tecnología como un medio para realizar transacciones, finalmente podrán evaluar el riesgo e identificar patrones sospechosos en tiempo real.
Más agilidad de Big Data	Al almacenar datos en un libro mayor descentralizado, las empresas de Big Data podrían procesar todos los datos de una manera más eficiente y rápida. Podría acelerar el proceso de transacción (haciéndolo casi instantáneo) y reduciría el costo de las transferencias al eliminar las barreras de seguridad y las verificaciones de riesgos involucradas.

Cuadro 5.1: Beneficios de Blockchain a Big Data.

5.1.3. Futuro de la integración de Blockchain y Big Data

Blockchain tiene el potencial de cambiar la forma en que se trata y analiza Big Data, ya que permite aumentar su seguridad y calidad de datos, por mencionar algunos. Es probable que en el transcurso de los años se tenga un mayor progreso en la asociación de Big Data Analytics y Blockchain a medida que continúen los desarrollos en este espacio. Tan pronto como la tecnología madure y traiga más innovaciones, se identificarán más casos de uso concretos para beneficiar la gestión de Big Data y el análisis de datos. A medida que se recopilen más datos en tiempo real, será fascinante observar que esta tecnología continuará revolucionando diferentes industrias y brindando una mejor privacidad de datos.

“ Blockchain tiene la capacidad de convertir ideas y preguntas en activos. Puede brindar una mayor confianza en la integridad de los datos que ve. Entradas inmutables, marca de tiempo basada en el consenso, auditoría, senderos y certeza sobre el origen de los datos (p. un sensor o un quiosco) son todas las áreas donde verá mejoras a medida que la tecnología Blockchain se vuelva más convencional. ” VentureBeat.

5.2. Inteligencia Artificial (IA)

La IA es una de las ramas de las ciencias de la computación que más interés ha despertado en la actualidad, debido a su inmenso campo de aplicación el cuál continúa creciendo con el paso de los años. La búsqueda de mecanismos que nos ayuden a comprender la inteligencia y realizar modelos y simulaciones de estos, es algo que ha motivado a muchos científicos a elegir esta herramienta como área de investigación (Julio Ponce, 2014). El origen del término “IA” se remonta a la intuición del genio matemático inglés Alan Turing y el sobrenombre “Inteligencia Artificial” se debe al informático John McCarthy quien definió una gran cantidad de conceptos relacionados a la IA en un artículo publicado el año 2007, este se puede encontrar en la referencia (McCarthy, 2007). En dicho artículo define a la inteligencia artificial como se muestra a continuación:

“Es la ciencia y la ingeniería de la fabricación de máquinas inteligentes, especialmente programas informáticos inteligentes. Está relacionada con la tarea similar de usar computadoras para entender la inteligencia humana, pero la IA no tiene que limitarse a métodos que son biológicamente observables.”John McCarthy

En un principio, la Inteligencia Artificial se creó en base a conocimientos y teorías existentes en otras áreas del conocimiento. Las principales fuentes que sirvieron de inspiración y conocimiento para iniciar en esta área fueron las ciencias de la computación, la filosofía, la neurociencia, las matemáticas y la psicología. Cada una de estas ciencias no solamente aportó sus propios conocimientos, sino que también contribuyó con sus herramientas y experiencias; contribuyendo así a la gestación y desarrollo de esta nueva área del conocimiento. La filosofía fundó las bases de la inteligencia artificial al imaginar a la mente humana como una máquina capaz de funcionar en base a conocimiento codificado asignado, con el fin de concebir una acción determinada produciendo conclusiones racionales. Las matemáticas proporcionaron las herramientas de certeza lógica y de cálculo que permitieron la modelación de diferentes algoritmos que facilitaron el manejo del razonamiento. La psicología fortaleció la idea de que los animales y los seres humanos puedan considerarse como máquinas que son capaces de procesar la información. Las ciencias de la computación aportaron con el avance de velocidad y memoria de los equipos de cómputo de hoy en día, lo cuál es fundamental para la implementación de la IA. Y por último, la neurociencia contribuye con los conocimientos recabados hasta la actualidad sobre la forma en que el cerebro humano procesa la información (Julio Ponce, 2014). Y aunque cada una de estas ciencias tratan de definir las bases para entender la IA, la realidad es que la mente humana es mucho más complicada, y esto es un factor importante a considerar para programar una red neuronal artificial.

En términos simples, la inteligencia artificial es la base a partir de la cual se simulan o repiten los procesos lógicos y aritméticos de inteligencia humana. Se lleva a cabo mediante la aplicación de algoritmos que son creados en un entorno dinámico de computación con el objetivo de que la IA piense y actúe como los seres humanos. Sin embargo, es importante destacar que, mientras más se pretenda que la IA tenga un comportamiento humano, más almacenamiento y capacidad se necesitará, aunque no será de la misma forma que el cerebro humano almacena la información (NetApp, 2023).

5.2.1. Blockchain & la Inteligencia Artificial

Una de las aplicaciones de la inteligencia artificial dentro de Blockchain está en los contratos inteligentes. Con ayuda de la IA sería posible que estos sean autónomos, descentralizados y ejecutables de forma seudónima en la cadena de bloques. Permitiendo que las plataformas de los contratos inteligentes se ejecuten en etapas progresivas aumentando su automatización, autonomía y complejidad. La IA también puede aportar a las Dapps, DAO, DAC y DAS dentro de Blockchain. La implementación dentro de estos sistemas reforzaría la potencia y automatización de las operaciones que realizan (Swan, 2015).

A continuación, se muestran algunos ejemplos de las aplicaciones prácticas en donde se utiliza la combinación de Blockchain e inteligencia artificial, en donde se tratan algunas dificultades específicas como la descentralización, la privacidad, la transparencia y la eficiencia en el ámbito de la IA (Talan, 2023).

- **SingularityNET** es una plataforma implementada en Blockchain que permite a los desarrolladores publicar, compartir y monetizar modelos de IA a través de contratos inteligentes.
- **Ocean Protocol** es una fundación que mediante la tecnología Blockchain emplea un mercado descentralizado de datos y servicios de IA que proporciona servicios de datos para ecosistemas cripto a través de tokens de datos. Los proveedores comparten y monetizan sus conjuntos de datos, y los consumidores tienen acceso a datos de alta calidad para mejorar sus modelos de IA.
- **DeepBrain Chain** es una plataforma que utiliza la tecnología blockchain para crear un mercado descentralizado de recursos de computación, donde los usuarios pueden comprar y vender potencia de cálculo utilizando el token nativo DeepBrain Chain (DBC) con el objetivo de mejorar la eficiencia del entrenamiento de IA a gran escala.
- **Numerai** es un fondo de cobertura basado en el Machine Learning: que predice la rentabilidad de acciones, impulsa la participación con criptomonedas, centraliza la creación de carteras digitales y gestiona sus riesgos. Todos estos modelos son llevados a cabo de manera precisa con ayuda de la inteligencia artificial.
- **Humans** es un proyecto de última generación que emplea la tecnología Blockchain y la IA para que cualquier persona pueda crear y escalar su potencial. Con esta plataforma, los usuarios pueden expandir y dar vida a sus ideas con ayuda de herramientas avanzadas de IA.

Figura 5.1: Plataformas que implementan IA y Blockchain (Talan, 2023).

5.2.2. Futuro de la integración de la IA y Blockchain

Hoy en día, la IA ha adquirido un uso práctico relevante para las actividades de la vida diaria, adquiriendo una gran importancia en casi todos los sectores de la economía, como los servicios financieros y bancarios, la salud, el transporte, entre otros. Además, con una amplia y casi infinita variedad de aplicaciones, podríamos estar ante el comienzo de un mundo automatizado impulsado por la interconexión entre máquinas y la economía de estas.

Es evidente que la IA y Blockchain serán dos de las principales tecnologías que impulsarán el ritmo de la innovación. Introduciendo cambios radicales en todos los sectores de la industria. Y a pesar de que cada tecnología tiene su propio grado de complejidad técnica, y de implicación empresarial. Es cuestión de tiempo para que muchas organizaciones apliquen estas dos tecnologías en conjunto para rediseñar todo el paradigma tecnológico (y humano) desde cero.

5.2.3. Organizaciones líderes en la integración de IA y Blockchain

Algunas de las organizaciones que trabajan en el aprovechamiento de estas tecnologías incluyen a CognativeScale, es una Startup: de IA respaldada por IBM, Intel y Microsoft que busca utilizar la tecnología Blockchain para almacenar de forma segura los resultados de una aplicación de IA con el objetivo de llevar a cabo el cumplimiento normativo en el mundo de los mercados financieros. Una industria que está estancada con muchas regulaciones hoy en día. Si se consigue regular las decisiones derivadas de una IA, podría ayudar a los participantes del mercado a mantenerse al tanto de los costosos requisitos de presentación de informes.

IBM también está considerando la idea de unir su oferta de cadena de bloques (basada en Hyperledger Fabric [2]) y su plataforma de IA Watson [3] para diversos sectores. Uno de estos proyectos es Everledger, el cuál emplea la tecnología Blockchain para rastrear la procedencia de artículos de lujo, incluido el comercio de diamantes. Por ejemplo, IBM emplea esta tecnología aprovechando el almacén de datos de Everledger sobre las características individuales de los diamantes los cuales son protegidos por la cadena de bloques de IBM. Del mismo modo, IA Watson aplica el conocimiento de miles de normativas para garantizar que los diamantes cumplen los decretos establecidos por la ONU para evitar la venta de Minerales conflictivos: (Rabah, 2018).

5.3. Internet de las Cosas (IoT)

Actualmente, el esquema de la información basada en Internet permite el intercambio de bienes y servicios entre todos los dispositivos conectados a la red. El internet de las cosas se refiere a la vinculación o conexión en red de todos los dispositivos cotidianos, que normalmente están equipados con inteligencia en su sistema. En este sentido, Internet se define como una plataforma para dispositivos que se comunican electrónicamente y comparten información y datos específicos con el mundo que les rodea. De esta manera, la IoT puede verse como el siguiente paso a la evolución de lo que conocemos como Internet actualmente. Ya que, con ayuda de la IoT se podría añadir una interconectividad más extensa, una mejor noción de la información y servicios inteligentes más completos (Jordi Salazar, 2016).

El Internet de las Cosas (Internet of Things - IoT) hace referencia a un conjunto de dispositivos conectados a la red, dichos equipos emplean tecnologías que facilitan la comunicación entre ellos, como puede ser la nube o entre ellos mismos. Algunos de estos dispositivos pueden utilizar sus sensores los cuales tienen algoritmos inteligentes con el fin de reunir gran cantidad de información para procesarla y así aprender las necesidades de los usuarios (Román, 2023).

[2] Hyperledger Fabric es un software de código abierto liderado por Linux Fundation el cuál se encarga de llevar a Blockchain a los espacios empresariales, permitiendo un mayor desarrollo en donde los usuarios son beneficiados (Maldonado, 2022).

[3] IA Watson es una plataforma que permitirá incorporar herramientas de inteligencia artificial a los datos del usuario para mejorar la optimización de procesos y diseños de flujos de trabajo (Services, 2023).

La IoT, es una arquitectura técnica global emergente basada en Internet que facilita el intercambio de bienes y servicios en redes de cadenas de suministro globales, tiene un impacto en la seguridad y la privacidad de las partes interesadas involucradas. Por lo que es necesario establecer medidas que garanticen la resistencia de la arquitectura a los ataques, la autenticación de datos, el control de acceso y la privacidad del cliente (Weber, 2010).

Internet ha dejado una marca en la calidad de vida de las personas, ya que proporcionó una gran cantidad de nuevas oportunidades de acceso a la información, servicios de educación, seguridad, asistencia sanitaria, transporte, etc. La IoT tiene el potencial para incrementar la productividad de las empresas, ya que provee una amplia distribución de internet, redes locales inteligentes y nuevos servicios que pueden adaptarse dependiendo de las necesidades de los usuarios o clientes. Y también, tiene el potencial de crear nuevos dispositivos interconectados inteligentes y explorar nuevos modelos de negocio en el futuro (Jordi Salazar, 2016).

5.3.1. Blockchain & el Internet de las Cosas

El objetivo por el cuál existe una gran cantidad de equipos conectados a internet está en la necesidad de simplificar muchas de nuestras actividades cotidianas, y para ello, se requiere que los dispositivos que nos rodean comiencen a ser cada vez más autónomos e inteligentes. Por ejemplo, un automóvil ya incorpora dispositivos y sensores que permiten manipular muchas de las funciones propias del coche, pero ¿es posible que el vehículo solicite la cita en el taller en caso de que aparezca una alarma de posible avería? Esta es una de tantas preguntas que podemos plantearnos sobre un objeto tan común cómo un automóvil, sin embargo, las respuestas a estas preguntas pueden estar bastante sujetas a la realidad en un futuro (Joaquín López Lérida, 2016).

5.3.2. Aplicaciones prácticas

- **Automatización y Mantenimiento de Vehículos.** Los vehículos equipados con IoT pueden automatizar la programación de citas de servicio y mantenimiento al detectar posibles fallas, comunicándose directamente con talleres y proveedores de servicios.
- **Gestión de la Cadena de Suministro.** Blockchain puede mejorar la trazabilidad y la fiabilidad de las cadenas de suministro al proporcionar un registro inmutable de las transacciones y movimientos de productos, desde el origen hasta el consumidor final.
- **Seguridad en Dispositivos IoT.** La integración de Blockchain ofrece un nivel superior de seguridad para los dispositivos IoT, protegiendo la información contra accesos no autorizados y asegurando la integridad de los datos transmitidos.
- **Automatización del Hogar.** Los sistemas de automatización del hogar pueden beneficiarse de Blockchain al garantizar que las transacciones y los comandos entre dispositivos sean seguros y confiables, facilitando un ecosistema doméstico más inteligente y eficiente.

5.3.3. Desafíos y consideraciones futuras

Blockchain protege su información preservando la confidencialidad de sus datos y garantiza la seguridad de las transacciones, por mencionar algunas. En la IoT es importante que los dispositivos conectados a internet puedan intercambiar información de confianza y transacciones seguras sin intenciones maliciosas. Además, con ayuda de esta tecnología las transacciones entre los dispositivos serían más seguras y rápidas de acuerdo al sistema de validación que se gestiona. Por último, Blockchain tiene la ventaja de llevar un esquema descentralizado en el cual no existe un nodo central del cuál dependa toda la red. Por lo que es posible operar con nuestros dispositivos conectados a internet en todo momento,

aunque se pierda conexión de algunos nodos de esta.

Blockchain puede aportar muchas cosas al Internet de las Cosas, simplificando gran parte de las soluciones y garantizando la seguridad de la información con la que nuestros dispositivos trabajan actualmente (Joaquín López Lérida, 2016).

Capítulo 6

Desafíos Técnicos y sociales

Para este punto, es importante aclarar la importancia de la seguridad dentro de Blockchain y algunos de los problemas que este puede presentar y cómo se solucionan.

6.1. Problema del 51 %

A pesar de que la tecnología Blockchain represente una gran innovación dentro de la tecnología, esto no impide que tenga ciertos puntos débiles. Un punto débil que tiene muy marcado (y que tal vez sea el único) está en el problema del 51 %. Como se ha mencionado anteriormente, las transacciones realizadas en Blockchain son aprobadas a través de un sistema de votación en donde el bloque una vez autorizado se coloca en la cadena de manera permanente.

Sin embargo, es importante plantearse la siguiente pregunta, ¿qué pasaría si un usuario tuviera el control de más del 51 % de los nodos en una Dapp? Lo que sucedería en esta situación es que dicho usuario tendría poder teórico para modificar el contenido de Blockchain, debido a que esta funciona por consenso de todos los nodos que la conforman. Es decir, si la mayoría de los nodos aprueba un bloque cuya información dice A, aunque el bloque correcto sea el que contiene B, se aprobará el primero debido a que la mayoría de los nodos habría votado por A.

6.1.1. Exploración y soluciones

Es importante dejar claro cuáles son los puntos débiles que puedan presentarse al momento de interesarse en emplear una nueva tecnología, ya que esto es un factor muy importante con el cuál se puede tener un punto de partida para reforzar su seguridad y tratar de corregir o arreglar ese punto débil. En este caso, pese a que se trate de una clara vulnerabilidad que puede suceder, sus probabilidades son bastante bajas por los siguientes aspectos:

- Si es una Dapp pequeña, lo más probable es que al existir algún usuario que tenga control de 51 % o más de esta sea el mismo creador. Pero la seguridad recae en la poca probabilidad de que esto ocurra, ya que al ser una Dapp pequeña no tiene mucho sentido alterarla porque se perdería por completo el interés de los demás usuarios. Causando que no haya confianza ni seguridad dentro de la Dapp llevándola al fracaso.

- Caso contrario, si se presenta en una Dapp grande como Bitcoin la probabilidad sigue siendo bastante baja. Ya que, para que alguien pueda llevar a cabo dicha acción necesitaria poseer un mínimo del 51 % de la capacidad computacional de toda la red de la Dapp. En Bitcoin, por ejemplo, se requeriría una inversión tan descomunal que no sería rentable, ya que al contar con un buen equipo computacional sería más accesible participar dentro de la red y obtener las recompensas por el descifrado de bloques dentro de la misma siguiendo las reglas del protocolo. (Joaquín López Lérida, 2016)

6.1.2. Estrategias de mitigación adicionales

Si lo anterior mencionado no llegara a funcionar, todavía se cuentan con más opciones que podrían evadir el problema del 51 %. Gavin Andresen líder actual de Bitcoin licenciado en Ciencias de Computación por la Universidad de Princeton en 1988, es el encargado de llevar a cabo el proyecto teniendo control del repositorio de código fuente y la clave de alerta de la red después de que Satoshi Nakamoto se la haya transferido de manera definitiva. Satoshi Nakamoto se desvinculó de manera definitiva y Andresen se convirtió en la primera persona responsable de Bitcoin que sea identificable. Solo una semana después de la desaparición de Satoshi, Andresen publicaría uno de los mensajes más importantes y recordados de los orígenes de Bitcoin:

"Con la bendición de Satoshi, y con gran renuencia, comenzaré a hacer una gestión de proyectos más activa para Bitcoin. Todos por favor sean pacientes conmigo; he tenido mucha experiencia en gestión de proyectos en startups, pero este es el primer proyecto de código abierto de cualquier tamaño en el que he estado involucrado." (Salces, 2022)

En palabras de este Andresen, se plantean algunas soluciones adicionales que ayudarían perfectamente a evadir el problema del 51 % solo en caso de ser necesario (Joaquín López Lérida, 2016):

- **Detección de Ataques:** Un atacante del 51 % puede evitar que otros acepten nuevas transacciones que no sean las de este, sin embargo, al hacer esto se puede detener el procesamiento de pagos y dejar inutilizada a la red. Esto sería más que obvio para el resto de los usuarios dentro de la red, dejando claro que algo está ocurriendo.

- **Requisitos para el Atacante:** Se le puede obligar al atacante contar de manera simultánea con un gran poder computacional y una gran cantidad de Bitcoins antiguos de alta prioridad. En caso de no tenerlo, se tendrían que incluir las transacciones de los demás nodos, o en su defecto rechazar su cadena.

6.1.3. Implicaciones y futuro de Blockchain

El problema del 51 % destaca la importancia de la seguridad y la descentralización en la tecnología Blockchain. A pesar de que estas soluciones y mitigaciones propuestas refuerzan la fortaleza de la red, es importante destacar la necesidad de vigilancia continua y desarrollo tecnológico para prevenir vulnerabilidades en el futuro. La discusión sobre los desafíos técnicos y sociales de Blockchain, particularmente en torno a la seguridad, es fundamental para el desarrollo y crecimiento futuro de esta tecnología. A medida que Blockchain continúa evolucionando, la comunidad debe permanecer proactiva en la identificación de riesgos y en la implementación de soluciones para asegurar un ecosistema digital confiable y seguro para todos los usuarios.

6.2. Solución al problema de doble gasto

Como se ha mencionado anteriormente, Bitcoin es una moneda digital que no requiere su empleo de manera física, sin embargo, existe un desafío técnico llamado problema de doble gasto en donde un atacante envía el mismo billete o moneda digital a distintos usuarios. El término "doble gasto"significa que el dinero utilizado se puede gastar en varias ocasiones aumentando la inflación y devaluando su valor como criptomoneda.
Por ejemplo, supongamos que un atacante intenta enviar dos veces el mismo Bitcoin. Este proceso funcionaría de la siguiente manera:

Mérida le transfiere un BTC a la cuenta de Leo tal y como se muestra en la figura 6.1:

Figura 6.1: Mérida le transfiere 1 BTC a Leo.

Después de esto, Leo se encarga de gastar el mismo BTC cuatro veces a distintas personas:

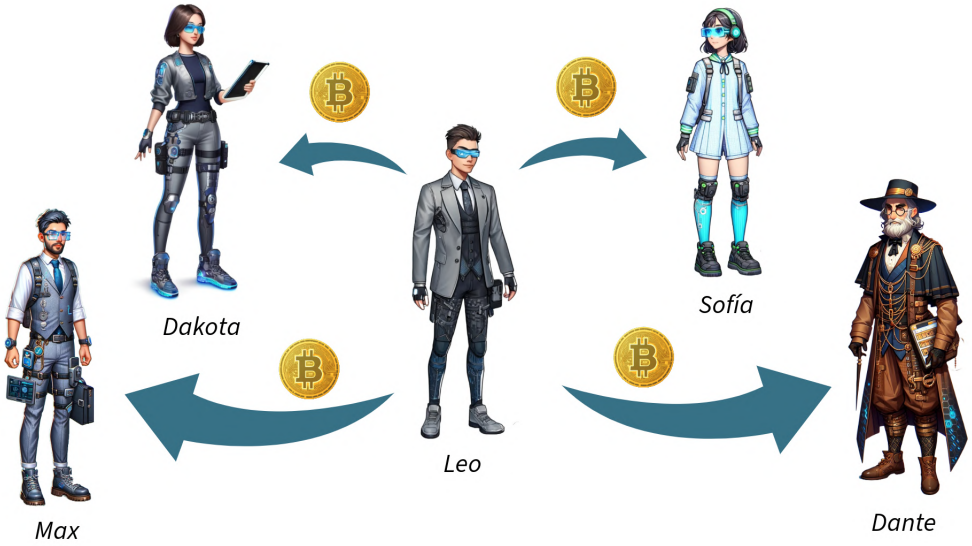


Figura 6.2: Leo transfiere el mismo BTC a distintos usuarios.

6.2.1. Mecanismo de consenso

A pesar de esto, Blockchain resuelve el problema de doble gasto mediante la criptografía, lo que hace estadísticamente más complicado crear operaciones no válidas. La propiedad de la moneda (BTC, por ejemplo) se registra en el libro mayor público de Blockchain, la cual se valida por los mineros y los protocolos criptográficos establecidos evitando así que se realice una transacción con una moneda ya gastada. Para este punto, es importante recalcar que se debe tener confianza en el software de protocolo de la cadena de bloques, ya que este será el que se encargue de evitar que se agreguen bloques a la cadena con la información repetida o alterada.

Si un atacante requiere añadir dos bloques gastando el mismo BTC con distintos usuarios, necesitaría convencer a una parte considerable de la red para que acepte la primera transacción y a otra parte de la red para aceptar la segunda. Esto causará que la red se divida en dos flujos, conocidos como forks o bifurcaciones. Esto último es más común en Blockchain de lo que parece, sin embargo, sus creadores supieron resolver este problema dificultando cada vez más los enlaces entre bloques.

6.2.2. Regla de la cadena más larga

Si se crearan dos bloques distintos al mismo tiempo, el protocolo Bitcoin dejaría pendiente esos dos bloques y dejaría que se continúe minando el resto de la cadena. Tan pronto como se minen los primeros dos bloques se tomaría en cuenta la cadena más larga, descartando la cadena anterior y volviendo así a un solo libro.

De acuerdo con lo anterior mencionado, es prudente esperar a que se minen un par de bloques antes de hacer válida la transacción. Después de su confirmación, la transacción será añadida a la cadena y ya no será posible su eliminación o modificación (Norman, 2019). Los nodos siempre considerarán la cadena más larga como la verdadera, descartando las transacciones en la cadena más corta, lo que efectivamente previene el doble gasto en este escenario.

6.2.3. La Importancia de las confirmaciones

Para los usuarios y las transacciones de gran valor, esperar múltiples confirmaciones (por ejemplo, 6 confirmaciones en el caso de Bitcoin) antes de considerar una transacción como finalizada es una práctica común que ofrece una mayor seguridad contra el doble gasto, especialmente en transacciones de alto valor. En resumen, la combinación de mecanismos de consenso distribuido, el proceso de confirmación de transacciones, la regla de la cadena más larga y el alto costo asociado con un ataque del 51 %, trabajan juntos dentro de la tecnología Blockchain de Bitcoin para solucionar de manera efectiva el problema del doble gasto, manteniendo la integridad y la confiabilidad del sistema.

6.3. Blockchain y Ciberseguridad

Blockchain ha ganado popularidad y reconocimiento con el paso de los años. Sin embargo, todavía hay algunos puntos que deben aclararse sobre sus capacidades más importantes, y algunos de estos puntos son; su escalabilidad, su sostenibilidad y también la seguridad de la tecnología. La evolución de Blockchain se puede comparar con el crecimiento exponencial que se ha dado en Internet. Y no cabe duda de que esta tecnología ha llegado a cambiar o innovar algunas industrias como la salud, el sector público, servicios de finanzas entre otros. De acuerdo con las palabras del Director General de Deloitte [1] en Estados Unidos, Dabid Schatsky, *"la tecnología proporciona una forma de registrar transacciones o cualquier integración digital de una forma que sea segura, transparente, altamente resistente a interrupciones, auditable y, eficiente." (DTT, 2023)*

Por otro lado, el líder de tecnología de Deloitte Alemania Milan Sallaba, menciona que; *"en alguno de los primeros casos de uso que hemos visto estaban desplegando Blockchain por el simple hecho de hacerlo, sin centrarse suficientemente en los atributos centrales de la tecnología, que de hecho tiene el potencial de generar eficiencias sustanciales en los procesos a través de varias industrias y es probable que contribuya a modelos de negocios completamente nuevos"(DTT, 2023).* Es por este motivo que la industria Blockchain debe reforzar muy bien un factor que es clave para el mundo de la tecnología de hoy en día. Su seguridad y su privacidad. Esto con el objetivo de convertirse en el impulso tecnológico que pueda cambiar el mundo industrial y social al que aspira ser.

Como bien sabemos, la dependencia de la tecnología en la actualidad ha traído consigo muchos modelos de negocios y una gran circulación de ingresos para grandes y pequeñas organizaciones. No obstante, esto normalmente ha dejado grietas que han sido aprovechadas por los ciberataques. Los ataques cibernéticos se han vuelto cada vez más complejos y sofisticados debido a la utilización de Malware: más avanzado con el fin de robar información como propiedad intelectual, datos personales, registros

[1] Deloitte es una marca que brinda servicios de auditoría, consultoría, manejo de riesgo, asesoramiento financiero y asesoramiento en impuestos a las principales empresas del mundo (DTT, 2023).

médicos e información financiera. Los ciberataques utilizan técnicas avanzadas de Ransomware: e interrumpen las operaciones del negocio en general mediante ataques de DDoS. De momento, aunque se ha intentado atacar la Blockchain de bitcoin con ataques DDoS: no se ha tenido éxito. Blockchain puede ayudar a potenciar la defensa cibernética previniendo actividades fraudulentas por medio de mecanismos de consenso, además de que permite detectar la alteración de información gracias a sus elementos de inmutabilidad, transparencia, encriptado y adaptabilidad operacional.

6.3.1. Confidencialidad

De acuerdo con el NIST, la confidencialidad se define como ”la propiedad que impide que la información sensible se divulgue a personas, entidades o procesos no autorizados.”

Aunque Blockchain fue creado con controles específicos de acceso público, existen algunas implementaciones que permiten reforzar el acceso a la información mejorando el control de accesos mediante el cifrado de datos de bloque. Esto se basa en cifrar los datos de la cadena completamente para evitar que sus datos sean expuestos cuando estos se encuentran en circulación. Algunas de las recomendaciones para mejorar la seguridad en un control de accesos están en la implementación a nivel aplicación, convirtiéndose en la primera línea de defensa, sobre todo en situaciones donde un atacante obtiene acceso a la red de área local. Otra recomendación es considerar cómo manejar los nodos que ya no estén comunicados o aquellos que permanezcan intermitentemente activos, ya que la cadena deberá seguir funcionando con o sin dichos nodos, y a su vez, debe ser capaz se restablecerse rápidamente una vez que estos regresen a su función original.

Si en la actualidad un ciber atacante pudiera acceder a una red Blockchain, no significa que pueda leer o descargar información. Esto es gracias al cifrado de los datos que son aplicables para aquellos datos que se encuentran en tránsito dentro de la red garantizando de manera efectiva su confidencialidad. El cifrado de extremo a extremo permite que únicamente el personal autorizado tenga acceso a la información cifrada, esto se hace mediante una llave privada que permite descifrar la información para su lectura. Las claves o llaves son usadas para numerosos objetivos dentro del ecosistema Blockchain, tales como; protección del usuario de la información, su confidencialidad, su autenticación y la respectiva autorización a la red (Lory Kehoe, 2018).

6.3.2. Integridad

De acuerdo con el NIST, la integridad se define como ”la protección en contra de la modificación o destrucción inadecuada de la información además asegura el no repudio y preserva la autenticidad de la información.”

Mantener la estabilidad de la información y garantizar la integridad de la misma es fundamental en cualquier sistema de información. El cifrado de datos, la comparación de hash y las firmas digitales son algunos elementos que permiten preservar la integridad de la información, esto sin depender de que se encuentre en curso, en reposo o simplemente en almacenamiento.

Blockchain conserva su inmutabilidad permitiendo que los usuarios confíen en que las transacciones almacenadas en su base de datos no validarán las transacciones falsificadas. Los protocolos que se basen en el consentimiento o aprobación de transacciones permiten que las organizaciones aseguren sus datos sin ningún problema, ya que a grandes rasgos el 51 % o más en la comunidad de Blockchain debe estar de acuerdo en que una transacción es válida para ser añadida a la cadena.

Garantiza la trazabilidad en cada transacción, ya que al registrarse una nueva transacción esta es firmada digitalmente con una marca de tiempo. Esto permitirá que las organizaciones puedan rastrear cada transacción realizada y ubicarla de manera exacta dentro de la cadena.

Blockchain no puede garantizar (al menos de momento) la mejora en calidad de los datos una vez introducidos. Solo tiene la responsabilidad de mantener la exactitud y la calidad de la información después de ser introducida a la cadena de bloques, debido a que los datos se transmitirán de un sistema origen propio de las organizaciones hacia una cadena de bloques, las entidades responsables deben garantizar que los canales utilizados para el intercambio de la información sean seguros, ya que este será un punto de ataque de entrada para los ciber atacantes. (Lory Kehoe, 2018)

6.3.3. Disponibilidad

El NIST define a la disponibilidad como "asegurar el acceso y uso oportuno y confiable de la información".

Si se retira un nodo de Blockchain, los datos seguirán siendo accesibles por otros nodos dentro de la red, esto gracias a que todos los nodos participantes tendrán una copia completa del bloque mayor en cualquier momento. Su infraestructura permite una accesibilidad a los datos en todo momento por cualquier nodo conectado, sin importar que algunos hayan sido afectados por un ataque DDoS.

De acuerdo con lo anterior mencionado, no se puede descartar que Blockchain no tenga puntos débiles. Por ejemplo, si por alguna razón ocurriera una interrupción de internet a nivel global, las redes más grandes de Blockchain como Bitcoin o Ethereum claramente se verían afectadas. Aunque en un caso así la mayoría de las tecnologías serían afectadas. Es por esto que las redes privadas de Blockchain que cuentan con un menor número de nodos deben tener muy en cuenta la distribución global de su red. La recomendación es que su red esté lo más distribuida posible a nivel global evitando tener puntos únicos de falla. Esto podrá garantizar que las operaciones trabajen sin afectación en caso de presentarse algún ciberataque coordinado o algún desastre natural.

Blockchain mantiene su alta disponibilidad gracias a la combinación de su naturaleza peer to peer, los nodos que trabajan dentro de la red en todo momento, la distribución de la red y también la capacidad computacional que manejan sus nodos. Esto permitirá que no se vea afectación para aquellas organizaciones que implementen la tecnología Blockchain, incluso si algunos de los nodos se ven afectados. (Lory Kehoe, 2018)

6.3.4. Estrategias y evolución de la ciberseguridad en Blockchain

Blockchain no solo proporciona un marco seguro para la transacción y almacenamiento de datos, sino que también promueve la innovación en modelos de negocio y procesos industriales. Su aplicación en campos como la salud, finanzas y el sector público, entre otros, destaca su potencial para transformar y fortalecer la infraestructura de seguridad digital en diversas industrias. Algunas de las estrategias que se pueden implementar para una gestión más segura dentro de Blockchain son:

- **Manejo de Claves** La gestión segura de las claves privadas es vital para mantener la confidencialidad y el acceso a la información. Las organizaciones deben implementar políticas robustas para el almacenamiento y recuperación de claves.
- **Riesgo de Ataques del 51 %** Aunque poco probable en redes grandes debido a su elevado costo, las redes Blockchain más pequeñas deben considerar mecanismos para prevenir la concentración del poder computacional que podría comprometer la red.
- **Distribución Global de la Red** Para redes Blockchain privadas, es recomendable una distribución geográfica amplia de nodos para evitar puntos únicos de fallo y asegurar la continuidad del servicio ante posibles contingencias.

Es importante mencionar que en el mundo de la tecnología no existe un sistema completamente infalible. La constante evolución de las amenazas cibernéticas requiere que las soluciones de Blockchain

se adapten y actualicen continuamente para enfrentar nuevos desafíos. La colaboración entre expertos en ciberseguridad y desarrolladores de Blockchain es esencial para avanzar hacia sistemas más seguros, transparentes y eficientes.

En resumen, Blockchain ofrece herramientas poderosas para mejorar la ciberseguridad, pero su implementación debe ser cuidadosa y considerada, complementada con otras prácticas de seguridad para proteger contra la diversidad y sofisticación de las amenazas cibernéticas actuales. La educación continua, la investigación y el desarrollo de nuevas soluciones serán clave para aprovechar al máximo las capacidades de Blockchain en la defensa cibernética.

6.4. Desafíos éticos y legales

Los desafíos éticos y legales asociados con la tecnología Blockchain son tan significativos como sus oportunidades de innovación. La adaptación de la sociedad a estas tecnologías emergentes requiere no sólo de avances técnicos sino también de consideraciones profundas sobre sus implicaciones en diferentes aspectos de nuestras vidas.

6.4.1. Rendimiento

Uno de los problemas que presenta la red de Bitcoin está en el Rendimiento:, ya que, solo puede procesar una transacción por segundo (tps) con un máximo de 7 (tps), en comparación, las transacciones con VISA pueden procesar de 2000 a 10,000 tps. Y aunque la solución esté en un aumento de la capacidad de cada bloque, la realidad es que al implementar esto, muy probablemente se tenga que lidiar con otros problemas sobre su tamaño y la expansión de la cadena de bloques. De momento, los desarrolladores sostienen que este límite se aumentará cuando sea necesario (Swan, 2015).

6.4.2. Sostenibilidad

La minería consume una enorme cantidad de energía por cuestiones de prueba de trabajo, comprometiendo la Sostenibilidad:. El consumo de energía hace confiable este sistema ya que los participantes no están dispuestos a participar si no es con el fin de obtener una recompensa. Sin embargo, no se descarta que esto puede traer daños medioambientales en el futuro (Swan, 2015). De acuerdo con el Centro de Finanzas Alternativas (CCAF) de la Universidad de Cambridge el consumo eléctrico de Bitcoin se encuentra, hasta agosto de 2023, en 70,4 tera vatios-hora (TWh) aproximadamente (Herrera, 2023). En comparación, un tera vatio-hora (TWh) podría alimentar 70,000 hogares en Estados Unidos durante un año. De acuerdo con la Agencia Internacional de la Energía [2] (International Energy Agency) se estima que para el año 2026 habrá un aumento del 30 % en el consumo de energía en lo que a criptomonedas se refiere. (Andersen, 2024)

6.4.3. Escalabilidad

Algunas limitaciones presentadas en su Escalabilidad: está el tamaño de bloque ya que estos crecen cada vez más con el paso de los años. Además, si Blockchain no es capaz de ofrecer una velocidad similar o igual a la que ofrecen los sistemas centralizados, será muy complicado que ofrezca una alternativa viable para el público en general. Si aumenta la cantidad de transacciones se presentará un mayor tiempo de espera para su validación, así como el aumento en las comisiones que reciben los mineros (Rodriguez, 2019).

[2] Agencia creada en 1974 por el marco de la Organización para la Cooperación y el Desarrollo Económico (OCDE) con el fin de implementar un programa de energía mundial que permita aumentar la seguridad energética, ahorro de energía y desarrollo de fuentes de energía alternativas.

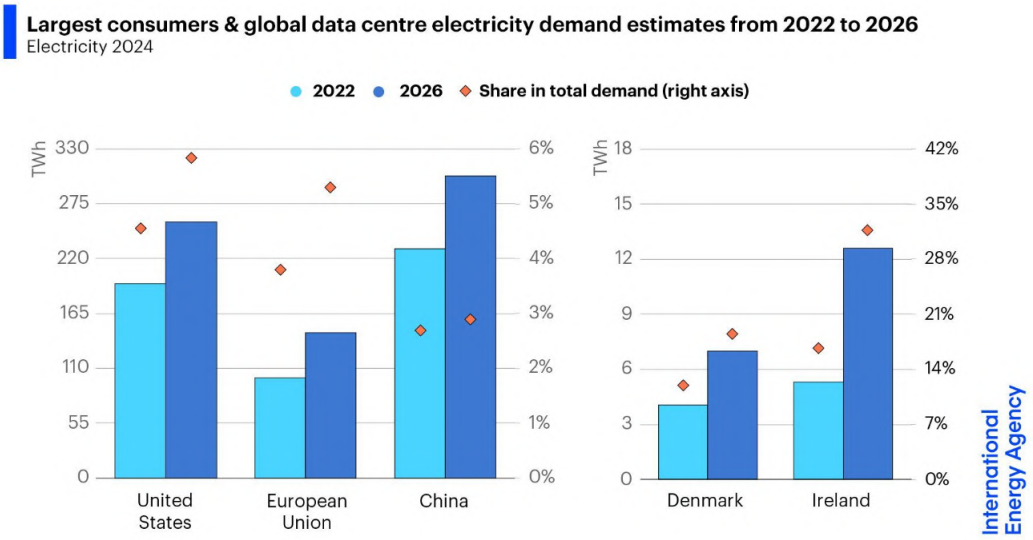


Figura 6.3: Aumento de consumo de energía del 30 % para el año 2026 (Andersen, 2024).

6.4.4. Privacidad

El sistema público de Blockchain puede contradecir bastante a lo que Privacidad: se refiere. Esto puede presentar inconvenientes para las empresas que manejan datos sensibles y que necesitan tener los límites muy definidos (APD, 2019).

6.4.5. Regulación legal

Tal y como se definió anteriormente, todavía no hay una regulación ni entidad legal específica al respecto que asegure la utilización de Blockchain (APD, 2019).

Sin embargo, esto no descarta que en algún futuro no se pueda implementar. Al regular Blockchain de manera legal, se pueden traer varios beneficios tales como la validez jurídica, los sellos de tiempo, la identidad del usuario, los mecanismos contractuales y la protección de datos, por mencionar algunos (Aparo, 2023).

6.4.6. Consideraciones éticas y legales

Más allá de estos desafíos técnicos y legales, la implementación de Blockchain plantea preguntas éticas y sociales importantes. ¿Cómo aseguramos que la tecnología beneficie a todos equitativamente y no solo a unos pocos? ¿Cómo manejamos los dilemas éticos en el diseño y uso de Blockchain, especialmente en aplicaciones críticas como el voto electrónico, la identidad digital y la gestión de registros médicos? La tecnología Blockchain ofrece un potencial transformador para numerosas industrias, pero su adopción y desarrollo sostenible dependen de abordar estos desafíos éticos, técnicos y legales de manera integral. La colaboración entre tecnólogos, legisladores, usuarios finales y otros stakeholders es crucial para navegar estas complejidades y asegurar que la tecnología se desarrolle de manera que refleje los valores y necesidades de la sociedad.

Capítulo 7

Metodologia de la investigación del aula virtual

Un aula virtual se define como un entorno digital que permite llevar a cabo un proceso de intercambio de conocimientos con el objetivo de posibilitar un aprendizaje entre los usuarios que participan dentro de esta.

Es decir, un aula virtual es un espacio dentro de un servidor con aplicaciones de uso compartido en la que profesores y alumnos comparten contenidos donde se atienden consultas, dudas y evaluaciones de los participantes sobre una materia o tema en particular. Los alumnos pueden acceder a diversas herramientas en donde se puede conversar, leer documentos, ver imagenes y videos, participar, realizar prácticas, ejercicios y evaluaciones, etc. Una de las ventajas de las aulas virtuales está en su independencia con los límites físicos y temporales, ya que los alumnos pueden disponer de su contenido sin estar sujetos a disponibilidad de horarios o desplazamientos físicos (Euroinnova, 2023).

Algunas de las herramientas que contienen las aulas virtuales son:

- **Recursos:** publicación de materiales del curso como documentos, URLs o archivos multimedia
- **Guía de docente:** guía de la asignatura como temario, competencias y sistema de evaluaciones
- **Calendario:** programa de actividades y eventos como fechas de entrega o sesiones
- **Anuncios:** anuncios de la materia
- **Mensajes privados:** en donde el profesor y el alumno pueden mantener una comunicación para asesorías
- **Foros:** debates sobre las materias de estudio
- **Chats:** espacio de conversación para los estudiantes del aula
- **Tareas:** entrega de actividades y prácticas que son evaluadas por el profesor
- **Orla:** listado de los miembros de la asignatura
- **Exámenes:** pruebas y evaluaciones realizadas sobre los temas abordados en la asignatura
- **Calificaciones:** permiten al profesor evaluar las tareas y examenes de los alumnos para otorgar una nota final, esta nota puede ser visible para los alumnos
- **Videoconferencias Web:** para realizar sesiones de trabajo virtuales

7.1. Learning Managment System (LMS)

Un sistema de gestión de aprendizaje (LMS) es un software que permite crear, implementar y desarrollar un programa de entrenamiento o un proceso de aprendizaje específico por la web. Estas plataformas permiten interactuar a los usuarios mediante videoconferencias, foros de discusión y aplicación de exámenes o laboratorios. Además, permite que los instructores y administradores puedan gestionar el registro de los usuarios, el contenido de los cursos, calendarios, certificaciones y notificaciones, etc.

Los elementos que se utilizan en estas plataformas son; el hardware que soporta la funcionalidad del curso, y la interfaz con la que interactúa el usuario. Estos dos elementos son operados por instructores, estudiantes y administradores.

La finalidad de un LMS es la gestión del aprendizaje. Ya que estos permiten reunir y administrar el conocimiento de una organización en base a los documentos o recursos recopilados. En términos corporativos también se pueden emplear para entrenamiento y reclutamiento de personal, permite la capacitación y actualización de nuevas herramientas para sus usuarios. Algunas compañías de tecnología brindan un entrenamiento a sus clientes para emplear correctamente el producto que adquirieron. Manteniendo un sistema de entrenamiento abierto que mejora la experiencia del cliente.

Los diferentes tipos de LMS implementados son; auto hospedados, aplicaciones móviles, aplicaciones de escritorio y hospedados en la nube. De este último, los LMS se implementan mediante un modelo de negocio de software como servicio SaaS: en donde el proveedor o administrador se encarga de gestionar el mantenimiento y la administración del sitio. Y dado que se encuentra en la nube permite que los usuarios en línea puedan acceder al sistema desde cualquier sitio a cualquier hora, mediante un registro de usuario y contraseña (Anáhuac, 2023).

Algunos de los LMS más implementados son Chamilo, Evolcampus, Docebo y Moodle. En este proyecto de tesis se implementará Moodle, el cual se explicará en la siguiente sección.

7.1.1. Moodle

Se define a Moodle como una plataforma de aprendizaje online de código abierto diseñada para brindar un sistema integrado único, robusto y seguro. Inicialmente se creó para entornos personalizados con el fin de fomentar la interacción, investigación y colaboración. En la actualidad Moodle se implementa en organizaciones enfocadas en áreas distintas al sector educativo. Se implementa esta herramienta para el desarrollo de cursos en línea, procesos de contratación y entrevistas, capacitaciones y para comunidades de expertos.

Moodle permite integrar herramientas de colaboradores externos, tales como; foros, wikis, chats, blogs etc. Tiene la función específica de construir una estructura compleja para evaluar a detalle el progreso de los alumnos de modo que permita ofrecer contenido más avanzado conforme se suba de nivel. Moodle también tiene su aplicación para dispositivos móviles en Android e iOS, mediante esta se puede consultar el contenido de los cursos, así como recibir notificaciones y compartir imágenes y vídeos (Aritmetrics, 2022).

Figura 7.1: Logo de la herramienta Moodle.

Algunas de las ventajas de Moodle que sirvieron para elegir esta plataforma en este proyecto de tesis son:

- **Gratuita:** no tiene costo ya que tiene como finalidad la enseñanza libre
- **Interfaz amigable:** ya que fue diseñada por profesionales de la educación, psicólogos y psicopedagogos
- **Flexible:** está pensada para todo público, al ser se código abierto puede ser personalizado a cualquier forma deseada
- **Compatible:** permite contenido interactivo de diversos formatos multimedia y funciona con todos los navegadores web. Además, cuenta con más de 120 idiomas para que usuarios de diversos países puedan interactuar
- **Acualizado y seguro:** constantemente se está revisando y mejorando para adecuarse a las necesidades de los usuarios. Con esto se preserva la seguridad y privacidad de estos
- **Escalable:** puede soportar las necesidades tanto de clases pequeñas como de grandes organizaciones
- **Prestigio:** es implementado por diversas administraciones públicas y universidades
- **Disponible:** al estar basado en la web puede accederse desde cualquier dispositivo en cualquier momento y en cualquier lugar

Si se desea conocer más sobre Moodle se puede ingresar al sitio:

https://docs.moodle.org/all/es/Acerca_de_Moodle

7.2. Estándares de Competencia CONOCER

El CONOCER (Consejo Nacional de Normalización y Certificación de Competencias Laborales) es una entidad paraestatal que conforma la Secretaría de Educación Pública, esta es dirigida por el Secretario de Educación Pública y cuenta con la participación de las Secretarías de Trabajo, Economía, entre otras por parte del gobierno federal como; Consejo Coordinador Empresarial (CCE), Confederación Patronal de la República Mexicana (COPARMEX) y Confederación de Cámaras Industriales de los Estados Unidos de México (CONCAMIN), por parte del sector empresarial y Confederación Revolucionaria de Obreros y Campesinos (CROC), Confederación de Trabajadores de México (CTM) y Congreso del Trabajo por parte del sector laboral.

El propósito de la entidad CONOCER es permitir mediante el Sistema Nacional de Competencias de las personas, un instrumento impulsado desde el sector educativo, que permita fortalecer su competitividad económica, su capacidad de crecimiento y progreso social para beneficio de todos los mexicanos. El Sistema Nacional de Competencias, es un gran acuerdo nacional entre líderes de los sectores empresariales, de los trabajadores, del sector social, académico y de gobierno, que busca impulsar y desarrollar la competitividad de las organizaciones con estándares de competencias relevantes, y certificar las competencias y aptitudes de las personas con estructuras y mecanismos de alcance nacional (OIT, 2024).

7.2.1. Qué es un Estándar de Competencia (EC)

Es el documento oficial que permite evaluar y certificar la competencia de las personas. El Estándar de Competencia describe un conjunto de conocimientos, habilidades, destrezas y actitudes, que son necesarias para demostrar que una persona es capaz de ejecutar una actividad laboral, con un alto nivel de desempeño.

Para desarrollar un Estándar de Competencia, el Comité de Gestión por Competencias se apoya en grupos técnicos de expertos, quienes son capacitados por el CONOCER en el proceso de elaboración

del Estándar (CONOCER, 2024).

El INAP (Instituto Nacional de Administración Pública) es una entidad acreditada ante el CONOCER como Entidad de Certificación y Evaluación de Competencias (ECE). Por medio del Centro de Consultoría en Administración Pública (CECAP), el INAP es capaz de ofrecer servicios que permiten contribuir a la construcción de capacidades en organizaciones públicas y del sector social a través de la capacitación, evaluación y certificación de personas en diversos Estándares de Competencias (EC) inscritos en el Registro Nacional de Estándares de Competencias (RENEC). Estos estándares están disponibles para que los sectores, dependencias y diversas instituciones los integren como parte esencial en sus procesos de profesionalización, desarrollo de recursos humanos y gestión de talento.

Además, permiten un mejor desarrollo en programas curriculares alineados para las instituciones educativas, para reforzar la formación mediante cursos de capacitación específicos (INAP, 2024).

Algunos de los Estándares de Competencia ofrecidos por la entidad CONOCER se muestran en la siguiente tabla, si se desea conocer más de estos estándares se puede ir al sitio $http://conocer.gob.mx:6060/conocer/\#/renec$:

Código	**Título**
EC0076	Evaluación de la competencia de candidatos con base en Estándares de Competencia.
EC0217.01	Impartición de cursos de formación del capital humano de manera presencial grupal.
EC0401	Liderazgo en el servicio público.
EC0554	Trabajo en equipo.
EC0775	Administración de los servicios municipales.
EC0778	Inscripción de actos y hechos jurídicos relativos al estado civil de las personas.
EC0301	Diseño de cursos de formación del capital humano de manera presencial grupal, sus instrumentos de evaluación y manuales del curso.
EC0366	Desarrollo de cursos de formación en línea.

Cuadro 7.1: Listado de Estándares de Competencia (EC) definidos por la entidad CONOCER.

En este proyecto de tésis se hablará sobre el Estándar de Competencia EC0217.01.

7.2.2. Estándar de Competencia EC0217.01

Este documento contempla las funciones sustantivas de preparar, conducir y evaluar cursos de capacitación para la impartición de cursos de formación del capital humano de manera presencial y grupal. La elaboración de técnicas instruccionales y grupales que faciliten el proceso de aprendizaje, realizando evaluaciones antes, durante y al final del curso considerando la satisfacción de los participantes/capacitandos. El presente Estándar de Competencia se fundamenta en criterios rectores de legalidad, competitividad, libre acceso, respeto, trabajo digno y responsabilidad social.

También establece los conocimientos teóricos, básicos y prácticos con los que debe contar para realizar un trabajo, así como las actitudes relevantes en su desempeño.

Los apoyos y requerimientos para este estándar son:

- Tener un aula con capacidad suficiente para impartir el curso con al menos 4 participantes/capacitandos, ya sea que todos estén presentes de forma física, o con la mitad conectada vía remota.
- En caso de que los participantes/capacitandos se encuentren conectados vía remota a través de herramientas de comunicación síncrona, se deberá contar con una correcta visualización y audio para propiciar la correcta interacción entre los participantes.

- Se deberá contar con recursos materiales didácticos y equipo de apoyo.

Los elementos que conforman el Estándar de Competencia EC0217.01 son:

- Elementos EC0217.01
  - Preparar el curso de formación
    - Clasificación de objetivos
    - Condiciones de interacción
    - Planeación del curso
    - Dominios de aprendizaje cognitivo
    - Dominios de aprendizaje psicomotriz
    - Dominios de aprendizaje afectivo
    - Verificar/Evaluar el aprendizaje
    - Sujeto de aprendizaje
    - Modalidad de capacitación presencial
    - Objetivo general
    - Objetivo particular
    - Secuencia de tipo inductivo
    - Técnicas instruccionales
    - Técnicas grupales
    - Teorías del aprendizaje
  - Conducir el curso de formación
    - Emociones positivas
    - Contrato de aprendizaje
    - Formulación de compromisos
    - Modulación lingüística
    - Retroalimentación positiva
    - Técnica grupal de integración
    - Técnica grupal de cierre
    - Uso sustentable de recursos didácticos
    - Tipo de grupos y participantes
  - Evaluar el curso de formación
    - Tipos de evaluación

7.2.3. Rúbricas de evaluación

Las rúbricas de evaluación son documentos o tablas que combinan criterios específicos y medibles con niveles de logro del estudiante. Estos documentos se comparten con los estudiantes al inicio del curso para que puedan entender cómo se evaluará su rendimiento. Las rúbricas detallan claramente los requisitos para alcanzar diferentes calificaciones en diversos objetivos de aprendizaje (Díaz, 2022).

Las partes que conforman una rúbrica de evaluación son:

- **Indicadores o criterios (filas)** son aspectos que requiere el estudiante para cumplir con su evaluación.

- **Niveles de logro (columnas)** permite escalar el grado de consecución del objetivo clasificado por niveles.

A continuación se muestra un ejemplo de rúbrica de evaluación:

RÚBRICA DE EVALUACIÓN	EXPERTO	BIEN	NOVEL	PESO X
CRITERIOS	2	1	0	100% (70%)
Manejo de ChemSpider	El alumno es capaz de dibujar la molécula que quiere sin ningún error en los enlaces y átomos que componen la molécula	El alumno ha cometido uno o dos errores al dibujar su molécula en ChemSpider	El alumno no ha dibujado su molécula o tiene mas de dos errores al dibujarla	20%
Identificación grupo funcional principal	El alumno ha identificado el grupo funcional principal de al menos el 90% de las moléculas propuestas.	El alumno ha identificado el grupo principal de más del 50% de las moléculas propuestas	El alumno no ha realizado la tarea o no identifica el grupo principal de las moleculas de forma correcta en mas del 50% de ellas	20%
Identificación cadena principal	El alumno ha identificado la cadena principal de al menos el 90% de las moléculas propuestas.	El alumno ha identificado la cadena principal de más del 50% de las moléculas propuestas	El alumno no ha realizado la tarea o no identifica la cadena principal de las moleculas de forma correcta en mas del 50% de ellas	20%
Formulación	El alumno ha nombrado correctamente al menos un 90% de las moléculas propuestas.	El alumno ha nombrado correctamente al menos un 50% de las moléculas propuestas.	El alumno no ha realizado la tarea o no nombra las moleculas de forma correcta en mas del 50% de ellas	20%
Educaplay	El alumno completa el ejercicio en menos de 2 minutos y con no más de 2 errores.	El alumno completa el ejercicio en menos de 5 minutos y no más de 2 errores.	El alumno no realiza la tarea, tarda más de 5 minutos en completarlo o tiene más de 2 errores.	20%

Figura 7.2: Rubrica de evaluación de ejemplo (Díaz, 2022).

7.3. Estructura general del curso de Blockchain

Al finalizar este curso, los estudiantes de la Universidad Autónoma de la Ciudad de México estarán equipados con una comprensión esencial de la tecnología Blockchain, cubriendo su origen, evolución, la criptografía que la sustenta y sus principios básicos, además del impacto ético y social. Los estudiantes explorarán activamente herramientas y plataformas Blockchain, aplicando sus conocimientos y habilidades en proyectos prácticos sencillos de asimilar, y desarrollarán una actitud crítica y ética hacia el uso de esta tecnología. A través de actividades colaborativas y de comunicación, fomentarán habilidades relacionales y sociales, esenciales para su desarrollo profesional y personal.

En el contexto de la gamificación en educación, una misión y un reto pueden ser términos que a menudo se utilizan indistintamente, pero suelen tener diferencias sutiles en cómo se aplican dentro de un curso:

1. **Misión** Generalmente se refiere a un objetivo más amplio o a un conjunto de objetivos que los estudiantes deben alcanzar, que puede incluir varios retos o tareas. La misión puede abarcar un módulo completo o una serie de lecciones que se enfocan en un tema más grande y más integrador.

2. **Reto** Es más específico y suele ser una tarea o actividad individual que los estudiantes deben completar para progresar hacia el cumplimiento de una misión. Los retos son los componentes individuales que, juntos, ayudan a cumplir la misión. Cada reto contiene una descripción, objetivo, actividad y sus recursos (documentos, simulaciónes, software etc).

7.3.1. Consideraciones del curso

Esta estructura busca equilibrar el contenido académico con actividades prácticas e interactivas, fomentando un aprendizaje profundo y aplicado de la tecnología Blockchain.

Interacción y participación del estudiante Para fomentar una mejor participación de parte de los estudiantes en el aula virtual se crearon actividades como:

1. Foros de discusión: para cada módulo, con temas específicos.

2. Trabajos en grupo: proyectos colaborativos en línea.

Accesibilidad y adaptabilidad De modo que los estudiantes cuenten con las herramientas necesarias para trabajar en el aula.

1. Materiales en diferentes formatos: texto y herramientas de software online.
2. Evaluaciones diversas: para adaptarse a diferentes estilos de aprendizaje.

7.4. Módulo 1: Introducción a Blockchain

La tecnología actual ha experimentado un crecimiento acelerado, impactando positivamente en el desarrollo e innovación de diversas industrias, incluyendo la comercialización, salud, política y seguridad de la información. La tecnología Blockchain ofrece aplicaciones que mejoran los procesos en estas áreas, despertando interés por su eficacia, seguridad y beneficios.

Blockchain resuelve un problema creciente en internet: la confianza en transacciones y sistemas de intercambio de activos que funcionan sin intervención física. Esto abre nuevas posibilidades para modelos de negocio en el mundo digital.

En este módulo se explicará de manera breve los elementos básicos de Blockchain, resumiendo la información explicada en el capítulo 1 de esta tésis. Las lecciones a definir en el primer módulo son:

1. ¿Qué es Blockchain? Definición
2. Origen de la tecnología Blockchain
3. Atributos clave de la tecnología Blockchain
4. Evolución hasta la actualidad

El objetivo particular es comprender la historia y la evolución de la tecnología Blockchain desde su creación. Los objetivos particulares son:

- **Cognitivo** Describir la evolución de Blockchain y su impacto en diferentes sectores
- **Psicomotor** Investigar y presentar estudios de caso sobre aplicaciones tempranas de Blockchain
- **Afectivo** Reflexionar sobre el impacto transformador de Blockchain en la sociedad moderna

7.4.1. Retos del módulo 1

Los retos a realizar en este módulo son los siguientes:

1.1. Reto I. Cuestionario de opción múltiple | Crononautas del Blockchain
Propósito de aprendizaje: Evaluar la comprensión de los estudiantes sobre los conceptos fundamentales de Blockchain, incluyendo su definición, características, y funcionamiento, a través de un cuestionario de opción múltiple. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

1.2. Reto II: Creación de una línea de tiempo | Crononautas del Blockchain
Ahora es el momento de poner a prueba tus conocimientos sobre el origen de la tecnología Blockchain. Este reto te permitirá explorar y organizar cronológicamente los eventos clave en el desarrollo de Blockchain, desde sus inicios hasta su implementación práctica. ¡Aprovecha esta oportunidad para mostrar tu comprensión de la historia de Blockchain y crear una representación visual clara y atractiva!

Propósito de aprendizaje: Valorar la capacidad de los estudiantes para identificar y secuenciar correctamente los eventos clave en la historia de Blockchain, utilizando herramientas de edición online para crear una línea de tiempo visual que represente de manera clara el desarrollo de la tecnología. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

1.3. Reto III. Foro de discusión y opinión personal | Crononautas del Blockchain
Ahora es el momento de poner a prueba tus conocimientos sobre Blockchain. Este reto te permitirá demostrar tu comprensión de sus atributos clave y te dará la oportunidad de interactuar y aprender de tus compañeros. ¡Aprovecha esta oportunidad para profundizar en un tema innovador y hacer valiosas contribuciones al grupo!

Propósito de aprendizaje: Valorar la habilidad de los estudiantes para entender y comunicar de manera efectiva las características de Blockchain mediante sus aportaciones en un foro, así como fomentar interacciones constructivas con las publicaciones de sus compañeros. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

1.4. Reto IV. La evolución de Blockchain | Crononautas del Blockchain
Este reto te permitirá demostrar tu comprensión de las tres fases principales de Blockchain y su impacto en diversas áreas. Además, tendrás la oportunidad de reflexionar sobre cómo esta tecnología puede transformar sectores como la educación, la salud y el gobierno. ¡Aprovecha esta oportunidad para hacer valiosas contribuciones al grupo y mejorar tu análisis crítico!

Propósito de aprendizaje: Comprender la evolución de Blockchain desde sus inicios hasta la actualidad, y analizar su impacto en diversos sectores a través del análisis de casos específicos. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

7.5. Módulo 2: Fundamentos de la Criptografía en Blockchain

El área de la seguridad informática se ha convertido en un campo extenso en los últimos años, tomando mucha relevancia debido al impacto que ha dejado en la tecnología. Hoy en día, la cantidad de información que se maneja es inmensa, con grandes cantidades de datos enviados y recibidos a través de internet en milésimas de segundo a nivel mundial.

El rápido avance de la tecnología ha posicionado a la seguridad informática como un área esencial, debido a las amenazas que ponen en riesgo nuestra privacidad e información personal. Por lo que es imprescindible contar con mecanismos de protección, y uno de estos es la criptografía.

La criptografía es el arte y ciencia de transformar la información para hacerla incomprensible a personas no autorizadas. Utiliza principios matemáticos para convertir la información original en una serie de números y símbolos que no revelan su contenido. A lo largo de este capítulo, introduciremos definiciones clave que ayudarán a comprender la importancia y aplicabilidad de la criptografía en la era digital.

En este módulo se explicarán los fundamentos más importantes de la Criptografía aplicados en Blockchain, resumiendo la información explicada en el capítulo 2 de esta tésis. Las lecciones a definir en el segundo módulo son:

1. Acontecimientos históricos de la Criptografía
2. Conceptos básicos de Criptografía
3. Criptosistemas: Simétricos y Asimétricos
4. Funciones Hash y algoritmos SHA

El objetivo particular de este módulo es entender los principios de la criptografía que sustentan la seguridad en Blockchain. Los objetivos particulares son:

- **Cognitivo** Explicar acontecimientos históricos, y cómo la criptografía asegura las transacciones y los datos en Blockchain

- **Psicomotor** Recordar técnicas de criptografía básica mediante ejercicios prácticos en plataformas de simulación
- **Afectivo** Valorar la criptografía como un pilar esencial para la confianza y seguridad en las transacciones digitales

7.5.1. Actividades del módulo 2

Los retos a realizar en este módulo son los siguientes:

2.1. Reto I. Foro de discusión Fundamentos de la Criptografía | Guardianes de la Criptografía
Este reto te permitirá demostrar tu comprensión de los hitos históricos clave en el desarrollo de la criptografía y reflexionar sobre cómo esta disciplina ha evolucionado hasta el presente. Además, tendrás la oportunidad de analizar cómo los avances en criptografía han sido fundamentales en momentos históricos importantes. ¡Aprovecha esta oportunidad para profundizar en la importancia de la criptografía y cómo se aplica hoy en día!

Propósito de aprendizaje: Comprender la evolución de la criptografía a lo largo de la historia, desde sus primeros usos en el Antiguo Egipto hasta los avances tecnológicos actuales, como en el caso de Blockchain. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

2.2. Reto II. Aplicación de conceptos básicos de Criptografía | Guardianes de la Criptografía
En este reto, aprenderás sobre el cifrado César y practicarás su aplicación resolviendo un mensaje cifrado. Además, aplicarás los principios de la triada de la seguridad de la información: confidencialidad, integridad y disponibilidad. ¡Aprovecha esta oportunidad para afianzar tus conocimientos y participar activamente en la práctica de estos conceptos clave en criptografía!

Propósito de aprendizaje: Entender los conceptos básicos de la criptografía, aplicar el cifrado César, y reconocer los principios esenciales de la triada de la seguridad de la información. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

2.3. Reto III. Comparación de criptosistemas simétricos y asimétricos | Guardianes de la Criptografía
Este reto te permitirá demostrar tu comprensión de las diferencias clave entre la criptografía simétrica y asimétrica, dos métodos esenciales para proteger la información en el mundo digital. Además, podrás reflexionar sobre cómo cada uno de estos sistemas se aplica en la práctica y cuáles son sus ventajas y desafíos. ¡Aprovecha esta oportunidad para profundizar en el estudio de estas técnicas criptográficas y cómo juegan un papel vital en la seguridad digital moderna!

Propósito de aprendizaje: Comprender y analizar las diferencias clave entre la criptografía simétrica y la criptografía asimétrica mediante una comparación detallada de sus características y aplicaciones. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

2.4. Reto IV. Funciones Hash y algoritmo SHA | Guardianes de la Criptografía
En este reto tendrás la oportunidad de experimentar directamente cómo las funciones hash transforman cualquier dato en una cadena única e irrepetible. A través de la generación de hashes, podrás observar cómo incluso los cambios más pequeños en un texto pueden generar resultados completamente diferentes. ¡Aprovecha esta oportunidad para profundizar en el funcionamiento de estas herramientas criptográficas y entender su importancia en la seguridad digital!

Propósito de aprendizaje: Comprender el concepto y la importancia de las funciones hash en criptografía, así como su funcionamiento práctico mediante la generación y análisis de hashes utilizando el

algoritmo SHA. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

7.6. Módulo 3: Conceptos básicos de Blockchain

Blockchain, o cadena de bloques, se refiere a una estructura de base de datos donde la información se almacena y organiza en bloques vinculados cronológicamente. Cada bloque contiene un código único, conocido como hash, que lo identifica. Los mineros, a través de un proceso de validación, añaden estos bloques a la cadena. Una vez insertado un bloque, su contenido queda permanentemente registrado, asegurando inmutabilidad y confiabilidad.

Contrario a lo que se podría pensar, la tecnología de Blockchain no es innovadora por utilizar elementos desconocidos; su genialidad radica en combinar tecnologías existentes, como las redes peer-to-peer y la criptografía asimétrica, para ofrecer una solución única. Esta permite crear un registro inalterable de transacciones y operaciones sin necesidad de una autoridad central que las supervise.

A lo largo de este capítulo, explicaremos los conceptos esenciales que permiten comprender cómo funciona Blockchain, desglosando cada elemento que contribuye a su operación descentralizada.

En este módulo se explicarán los conceptos básicos y más importantes de Blockchain. La información explicada en este módulo es un resumen de los capítulos 3 y 4.1, además, se incluye un apartado de simulación en Python. Las lecciones a definir en el tercer Módulo son:

1. Árbol de Merkle
2. Elementos de un bloque y el proceso de minado
3. Cadena de bloques
4. Cadena de bloques distribuida
5. Primeros pasos con Python y Google Colaboratory

El objetivo particular es adquirir un conocimiento profundo de los componentes fundamentales, arquitectura y funcionamiento de la tecnología Blockchain. Los objetivos particulares son:

- **Cognitivo** Identificar y describir los conceptos clave y componentes de Blockchain
- **Psicomotor** Elaborar materiales conforme a especificaciones de una cadena de bloques
- **Afectivo** Apreciar la importancia de la transparencia y descentralización en las tecnologías digitales

7.6.1. Actividades del módulo 3

Los retos a realizar en este módulo son los siguientes:

3.1. Reto I. Foro árbol de Merkle | Arquitectos de Blockchain

Ahora es el momento de poner en práctica tus conocimientos sobre los árboles de Merkle. Este reto te permitirá explorar cómo esta estructura de datos es utilizada para garantizar la integridad de la información en sistemas distribuidos, como Blockchain. A lo largo de esta actividad, verás cómo cualquier modificación en los datos afecta directamente al Root Hash, y cómo este mecanismo asegura que los datos no sean alterados sin ser detectados. Aprovecha esta oportunidad para profundizar en el funcionamiento de los árboles de Merkle y su aplicación práctica en la tecnología Blockchain. ¡Prepárate para realizar una serie de simulaciones que te ayudarán a visualizar estos conceptos de manera tangible!

Propósito de aprendizaje: Comprender la estructura y el funcionamiento de los árboles de Merkle y cómo esta estructura garantiza la integridad y seguridad de los datos en sistemas distribuidos, como Blockchain. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

3.2 Reto II. Comprender los elementos de un bloque y el proceso de minado | Arquitectos de Blockchain

Profundiza en el entendimiento de cómo cada bloque en Blockchain se enlaza criptográficamente al siguiente, formando una cadena ininterrumpida e inalterable. Este reto te proporcionará una comprensión práctica de la estructura fundamental de un bloque y cómo estos se conectan entre sí para asegurar la integridad y la seguridad de toda la cadena.

Propósito de aprendizaje: El propósito de este reto es que los estudiantes comprendan cómo se relacionan los elementos clave de un bloque en Blockchain, específicamente el Nonce, el hash y los datos, y cómo el proceso de minado asegura que el bloque sea válido. Los estudiantes también aprenderán cómo los mineros compiten por encontrar el Nonce adecuado para recibir recompensas. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

3.3 Reto III: Simulación de la Cadena de Bloques y Análisis de Cambios en los Hashes | Arquitectos de Blockchain

Es hora de poner en práctica tus conocimientos sobre cómo los bloques en una cadena de bloques están conectados entre sí a través de hashes. Ya has visto lo que es un hash, y cómo se utiliza para garantizar la integridad de un bloque en una blockchain. Ahora, en este reto, aprenderás cómo estos bloques se relacionan mediante el hash del bloque anterior, y cómo cualquier cambio en un bloque afecta toda la cadena.

Propósito de aprendizaje: El propósito de este reto es que los estudiantes comprendan la importancia de los hashes en la conexión de bloques dentro de una blockchain, así como la implicación de la modificación de cualquier bloque en la cadena. Además, se busca que los estudiantes practiquen con simuladores de blockchain para experimentar de primera mano cómo los bloques se minan y cómo cualquier cambio en los datos de un bloque rompe la cadena. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

3.4 Reto IV. Simulación de Blockchain distribuido | Arquitectos de Blockchain

En este reto, exploraremos cómo funciona una red de Blockchain distribuida, compuesta por múltiples nodos (Peers) que almacenan una copia exacta de la cadena de bloques. Verás cómo cualquier modificación en los datos de un bloque puede afectar la sincronización de la cadena y cómo los mecanismos de consenso detectan y rechazan estas modificaciones, asegurando la integridad de la red.

Utilizando el simulador de Blockchain distribuida, comprobarás de manera práctica cómo los bloques están conectados por sus hashes y cómo cualquier cambio en un nodo afecta la estructura completa de la cadena.

Propósito de aprendizaje: El objetivo de este reto es que los estudiantes comprendan cómo funciona una red de Blockchain distribuida, y cómo los cambios en los bloques afectan la sincronización y validez de la cadena en diferentes nodos. Además, aprenderán a identificar cómo los mecanismos de consenso previenen la aceptación de cadenas alteradas en la red. Instrucciones completas para los estudiantes están en el aula virtual (Capítulo 8).

Capítulo 8

Implementación del aula virtual

En este proceso se ponen en práctica los planes y estrategias desarrollados durante los capítulos anteriores. La implementación del aula virtual abarca la ejecución real del servidor, la configuración de moodle y las actividades a realizar por los estudiantes para asegurar que el proyecto se complete de acuerdo con los objetivos establecidos.

8.1. Herramientas de software

En este sección se mostrarán las herramientas de software implementadas en este proyecto de tesis.

8.1.1. Linux Xubuntu

Xubuntu es un sistema operativo elegante y fácil de usar. Utiliza Xfce [1] y su interfaz gráfica da un aspecto moderno obteniendo funcionalidades suficientes y eficientes para el día a día. Xubuntu es ideal incluso para máquinas antiguas.

La primera versión del núcleo de linux fue creada en 1991 por el estudiante finlandés Linus Torvalds y constituye el núcleo central de Xubuntu. El núcleo es crucial en cualquier sistema operativo, ya que facilita la comunicación entre el hardware y el software. La *X* en Xubuntu proviene de Xfce, el entorno de escritorio utilizado. Además, el nombre *ubuntu* refleja la dependencia del núcleo de Ubuntu, que a su vez encarna los principios filosóficos del sistema operativo. Una traducción aproximada de ubuntu es *humanidad hacia los demás*. (Xubuntu.org, 2024)

8.1.2. Python

Python es un lenguaje de programación multiplataforma, consistente y estructurado. Es empleado para desarrollo de aplicaciones web, inteligencia artificial, programación de sistemas, programación orientada a objetos, juegos y multimedia, etc.

Este lenguaje está disponible para los principales sistemas operativos como Windows, Mac y se incluye de manera automática en todas las distribuciones de Linux (Buttu, 2016).

Algunos de los beneficios de Python se muestran a continuación, cabe mencionar que fue por esta razón que se optó por este lenguaje para este proyecto de tésis:

- Es más fácil de aprender
- Se puede ejecutar en diversas plataformas

[1] Xfce es un entorno de escritorio estable, ligero y altamente configurable utilizado por Xubuntu. Está diseñado para ser rápido y consumir pocos recursos del sistema, mientras ofrece una interfaz visual atractiva y de fácil manejo. Xfce tiene la filosofía tradicional de UNIX en cuanto a modularidad y reutilización.

- Requiere menos líneas de código, permitiendo más productividad a los programadores.
- Contiene una gran biblioteca estándar con códigos reutilizables.
- Cuenta con muchos recursos en internet como tutoriales, documentación, guías etcétera.

Figura 8.1: Logo de Python.

8.1.3. Google Colaboratory

Google Colab es una herramienta desarrollada por Google para proveer el acceso gratuito a GPU (Unidad de Procesamiento Gráfico) Y TPU (Unidad de Procesamiento Tensorial) a cualquier persona en cualquier lugar. Esta herramienta está diseñada específicamente para el desarrollo de aplicaciones de IA y Análisis de datos. Se puede considerar una versión avanzada de Jupyter Notebook.

Jupyter Notebook por otro lado, es un bloc de notas online. Es decir, es una aplicación web que, a través del navegador o un entorno de desarrollo integrado (IDE) deja que los usuarios puedan editar y ejecutar documentos con extensión de bloc de notas. En este tipo de editores se pueden crear todo tipo de programas, desde desarrollo web, hasta aplicaciones para Inteligencia Artificial, etc. (Canle, 2022)

8.1.4. LAMP

LAMP es un acrónimo que representa cuatro tecnologías fundamentales que impulsan numerosas aplicaciones web. Este conjunto de tecnologías, conocido como stack LAMP, es ampliamente utilizado en la actualidad y todas ellas son de código abierto (Lozano, 2020). Sus principales componentes son:

- **Linux** Sistema operativo de código abierto que cuenta con numerosas distribuciones, cada una con distintos paquetes de software instalados.
- **Apache** El servidor web más utilizado que se encargará de ejecutar las herramientas del paquete y también nos mostrará la interfaz gráfica.
- **MySQL** Es la incorporación del sistema que gestiona la base de datos. Otra alternativa completamente compatible es MariaDB (se mantiene al margen de Oracle).
- **PHP** Al ser de código abierto, es un lenguaje de programación ampliamente utilizado para interactuar con bases de datos. Incluye muchas de las bibliotecas más populares para el desarrollo.

8.1.5. VirtualBox

Oracle VM VirtualBox es un software de virtualización [2] multiplataforma de código abierto que se utiliza para virtualizar sistemas operativos dentro de un solo equipo físico.

Una máquina virtual se define como un sistema aislado que contiene un sistema propio de hardware con su propia CPU, memoria, interfaz de red y almacenamiento. Esta separación de recursos informáticos se realiza mediante un sofware llamado hipervisor, el objetivo de este sofware es aislar la máquina física del sistema operativo de la máquina virtual para su gestión de manera independiente.

[2] Es una tecnología que permite crear entornos simulados desde un solo equipo o sistema de hardware físico

Esto permite que el usuario final pueda emular el sofware de una máquina virtual de una manera casi identica al de una máquina física. Para más información sobre este tema se puede ingresar al sitio: $https://www.redhat.com/es/topics/virtualization/what-is-a-virtual-machine$.

Figura 8.2: Logo de VirtualBox.

8.2. Topología de red de laboratorio de LACECI

Para la elaboración de este proyecto se asignó la dirección IP fija *172.17.133.252* al servidor de Moodle, tomando en cuenta las siguientes características de la red del laboratorio de LACECI:

Configuración	Dirección IP	Máscara de red
Segmento de red	172.17.133.x	255.255.255.0
Gateway	172.17.133.254	255.255.255.0
Broadcast	172.17.133.255	255.255.255.0

Cuadro 8.1: Configuración de red de LACECI.

Server	Dirección IP	Máscara de red
DNS1	172.18.17.14	255.255.255.0
DNS2	172.18.102.14	255.255.255.0
DHCP	172.17.133.1	255.255.255.0
Moodle	172.17.133.252	255.255.255.0

Cuadro 8.2: Servidores configuradas de LACECI.

A continuación, se muestra la configuración de las direcciones IP asignadas a los equipos de cómputo con ayuda con la herramienta nmap, y de acuerdo con los datos anteriormente mencionados, se muestra la siguiente topología de la red del laboratorio de LACECI:

```
root@fedora:/home/lacecil1# nmap -sn 172.17.133.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-14 17:13 PDT
Nmap scan report for 172.17.133.1
Host is up (0.00087s latency).
MAC Address: 1C:66:6D:8E:9F:26 (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.5
Host is up (0.00036s latency).
MAC Address: 1C:66:6D:91:0C:35 (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.12
Host is up (0.00049s latency).
MAC Address: 1C:66:6D:91:0C:29 (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.13
Host is up (0.00048s latency).
MAC Address: 1C:66:6D:91:0C:2D (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.14
Host is up (0.00068s latency).
MAC Address: 1C:66:6D:91:16:AD (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.30
Host is up (0.00034s latency).
MAC Address: 1C:66:6D:8E:A0:34 (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.32
Host is up (0.00043s latency).
MAC Address: 1C:66:6D:8E:A5:1D (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.33
Host is up (0.00044s latency).
MAC Address: 1C:66:6D:91:0C:37 (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.34
Host is up (0.00036s latency).
MAC Address: 1C:66:6D:91:0C:1F (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.36
Host is up (0.00067s latency).
MAC Address: 1C:66:6D:8E:A5:DE (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.38
Host is up (0.00044s latency).
MAC Address: 1C:66:6D:8E:A0:06 (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.40
Host is up (0.00046s latency).
MAC Address: 1C:66:6D:8E:E6:83 (Hon Hai Precision Ind.)
Nmap scan report for 172.17.133.101
Host is up (0.00043s latency).
MAC Address: 54:AF:97:1F:F1:05 (Unknown)
Nmap scan report for 172.17.133.110
Host is up (0.00040s latency).
MAC Address: FC:AA:14:98:C8:F8 (Giga-byte Technology)
Nmap scan report for _gateway (172.17.133.254)
Host is up (0.0012s latency).
MAC Address: DE:23:3B:86:F4:00 (Unknown)
Nmap scan report for fedora (172.17.133.11)
Host is up.
Nmap done: 256 IP addresses (16 hosts up) scanned in 3.07 seconds
```

Figura 8.3: Direcciones IP asignadas a los equiupos de LACECI.

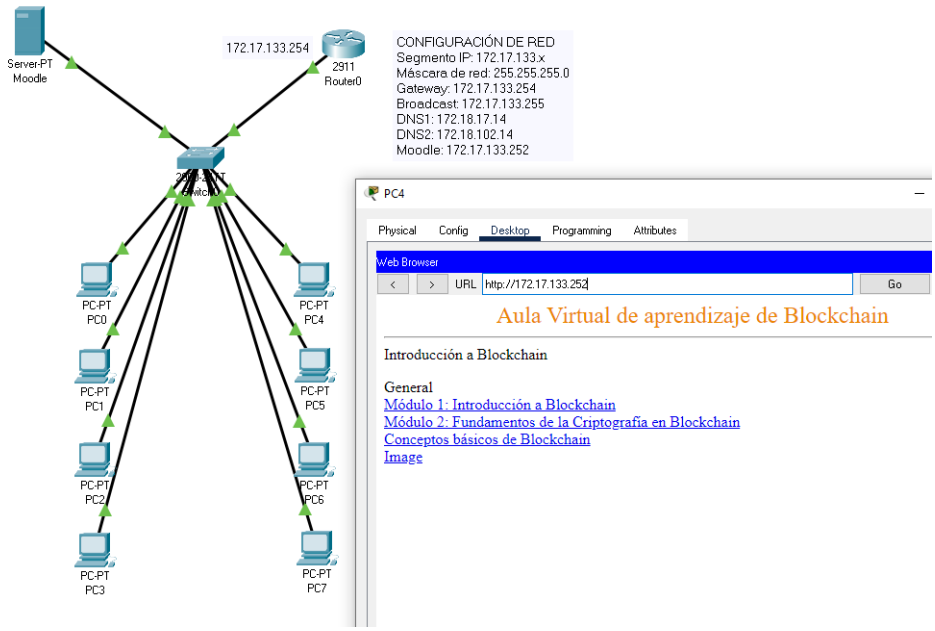


Figura 8.4: Topología de red de laboratoio LACECI en Cisco Packet Tracer.

En la figura anterior se puede observar la comunicación de forma exitosa hacia la IP *172.17.133.252*

que corresponde a nuestro servidor de Moodle.

Figura 8.5: Laboratorio de LACECI.

8.3. Instalación y configuración del servidor

Para este proyecto de tesis se instaló una máquina virtual (Virtual Box) con un sistema operativo Linux Xubuntu versión LTS 20.04 sobre otra distribución Linux Fedora 24.

Después de tener nuestra máquina virtual configurada se procedió a la instalación del servidor Moodle a la versión más actual, que es la *4.4.3+*. Si se desea saber a detalle el proceso de instalación se puede ir al apéndice B. Al tener nuestro servidor configurado se verá lo siguiente:

Figura 8.6: Vista del curso Blockchain.

8.3.1. Configuración de los usuarios

Para el acceso correcto se crearon las cuentas correspondientes de los siguientes usuarios:

Nombre	Matrícula	Carrera	Correo institucional
Alan Bernardo Garcia Escobar	16-003-0163	Ingeniería de Software	alan.garcia.escobar@estudiante.uacm.edu.mx
Angeles Aguilar Ramirez	14-003-0883	Ingeniería de Software	angeles.aguilar@estudiante.uacm.edu.mx
Manuel Antonio Salas Chavez	18-003-1125	Modelación Matemática	manuel.salas@estudiante.uacm.edu.mx
María del Carmen Alvarez Herrera	22-003-0873	Modelación Matemática	maria.alvarez.herrera@alumnos.uacm.edu.mx
José Luis Mata Ledezma	22-003-1012	Modelación Matemática	jose.mata.ledezma@alumnos.uacm.edu.mx
Israel Hernández Gonzalez	21-011-0903	Modelación Matemática	israel.hernandez@alumnos.uacm.edu.mx
Lorena Irann Rivas Lopez	16-003-0461	Ingeniería de Software	irann.rivas@estudiante.uacm.edu.mx

Cuadro 8.3: Estudiantes inscritos en el aula virtual.

8.4. Módulo 1: Introducción a Blockchain

En esta sección se mostrarán algunos de los temas explicados en el primer módulo junto con la actividad y las rúbricas de evaluación, cabe mencionar que la información utilizada forma parte del marco teórico de esta tésis.

8.4.1. Capítulos del módulo 1: Introducción a Blockchain. Crononautas del Blockchain

1. ¿Qué es Blockchain? Definición

   1.1 Reto I. Cuestionario de opción múltiple | Crononautas del Blockchain

2. Origen de la tecnología Blockchain

   2.1 Reto II. Creación de una línea de tiempo | Crononautas del Blockchain

3. Atributos clave de la tecnología Blockchain

   3.1 Foro de discusión y opinión personal | Crononautas del Blockchain

4. Evolución hasta la actualidad

   4.1 Reto IV. La evolución de Blockchain | Crononautas del Blockchain

Figura 8.7: Vista del primer módulo.

Figura 8.8: Vista de actividades (retos) del primer módulo.

A continuación, se muestran los recursos que contiene el primer módulo, los cuales contienen los capítulos, actividades y recursos de este.

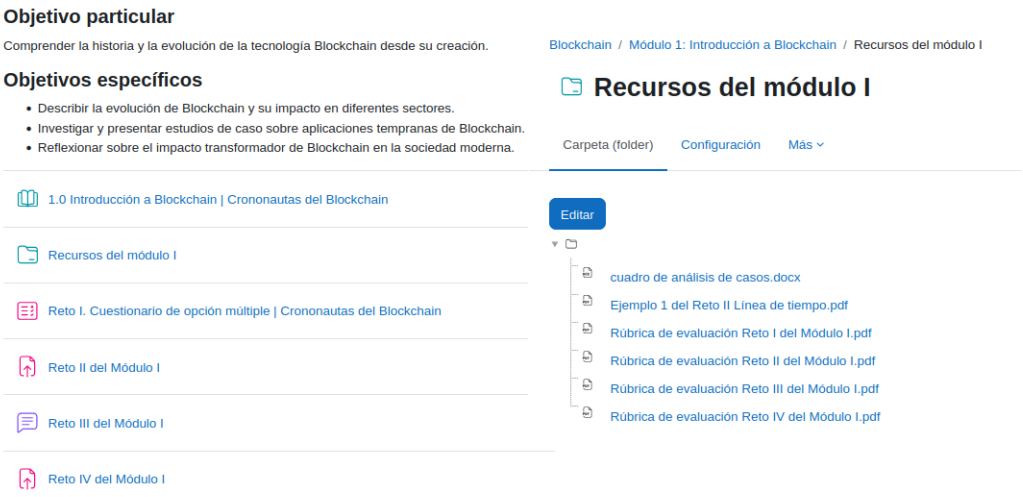
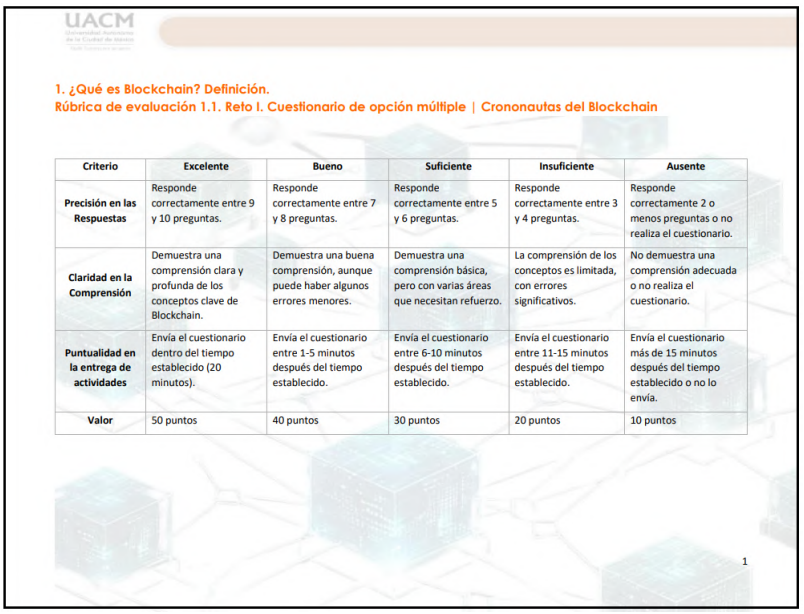


Figura 8.9: Recursos del primer módulo.

8.4.2. Rúbricas de evaluación del primer módulo

En esta sección se muestran las rúbricas de evaluación correspondientes a los cuatro retos del primer módulo. Estas rúbricas están diseñadas para evaluar de manera estructurada y justa el desempeño de los estudiantes en cada reto.



1. ¿Qué es Blockchain? Definición.
Rúbrica de evaluación 1.1. Reto I. Cuestionario de opción múltiple | Crononautas del Blockchain

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Precisión en las Respuestas	Responde correctamente entre 9 y 10 preguntas.	Responde correctamente entre 7 y 8 preguntas.	Responde correctamente entre 5 y 6 preguntas.	Responde correctamente entre 3 y 4 preguntas.	Responde correctamente 2 o menos preguntas o no realiza el cuestionario.
Claridad en la Comprensión	Demuestra una comprensión clara y profunda de los conceptos clave de Blockchain.	Demuestra una buena comprensión, aunque puede haber algunos errores menores.	Demuestra una comprensión básica, pero con varias áreas que necesitan refuerzo.	La comprensión de los conceptos es limitada, con errores significativos.	No demuestra una comprensión adecuada o no realiza el cuestionario.
Puntualidad en la entrega de actividades	Envía el cuestionario dentro del tiempo establecido (20 minutos).	Envía el cuestionario entre 1-5 minutos después del tiempo establecido.	Envía el cuestionario entre 6-10 minutos después del tiempo establecido.	Envía el cuestionario entre 11-15 minutos después del tiempo establecido.	Envía el cuestionario más de 15 minutos después del tiempo establecido o no lo envía.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

1

Figura 8.10: Rúbrica de evaluación del reto I del primer módulo.

Puntaje Total:

- **Precisión en las Respuestas:** 50 puntos
- **Claridad en la Comprensión:** 50 puntos
- **Puntualidad en la entrega de actividades:** 50 puntos

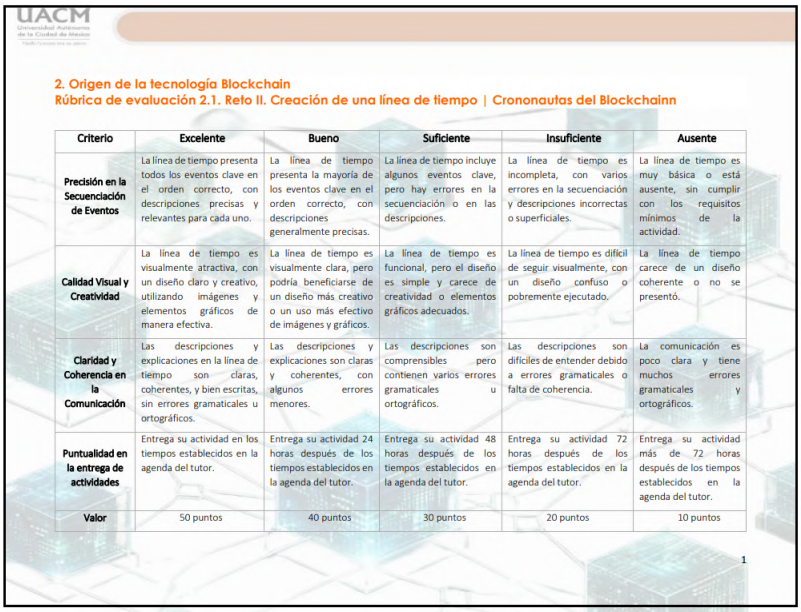
Total posible: 150 puntos

Interpretación de Resultados:

- **Excelente (135-150 puntos):** El estudiante ha demostrado un entendimiento sobresaliente de los conceptos clave de Blockchain, respondiendo correctamente la mayoría de las preguntas y entregando puntualmente.
- **Bueno (105-134 puntos):** El estudiante tiene una buena comprensión de los conceptos, aunque puede haber áreas menores que necesiten refuerzo.
- **Suficiente (75-104 puntos):** El estudiante ha demostrado una comprensión básica de los conceptos, pero con varias áreas que necesitan mejora significativa.
- **Insuficiente (50-74 puntos):** El estudiante tuvo dificultades importantes para comprender los conceptos y responder correctamente al cuestionario.
- **Ausente (10-49 puntos):** El estudiante no demostró una comprensión adecuada o no completó el cuestionario.

2

Figura 8.11: Interpretación de resultados del reto I del primer módulo.

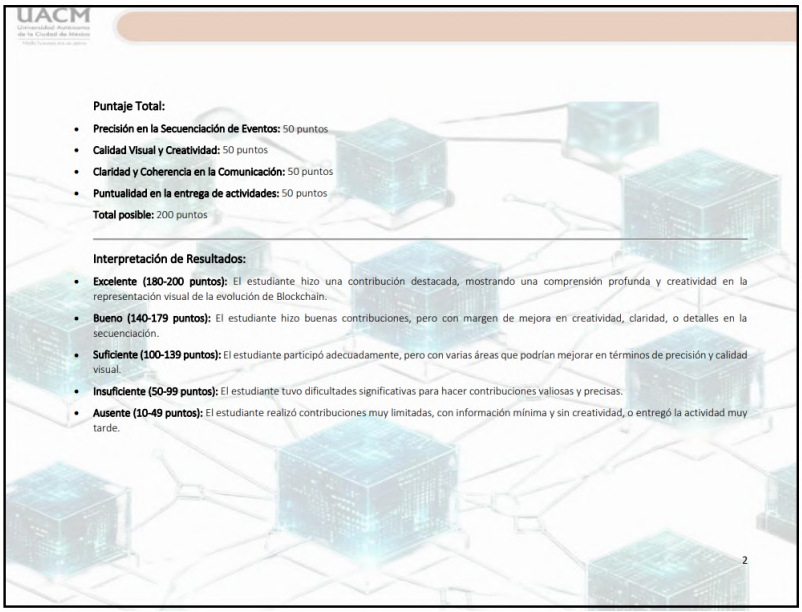


2. Origen de la tecnología Blockchain
Rúbrica de evaluación 2.1. Reto II. Creación de una línea de tiempo | Crononautas del Blockchainn

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Precisión en la Secuenciación de Eventos	La línea de tiempo presenta todos los eventos clave en el orden correcto, con descripciones precisas y relevantes para cada uno.	La línea de tiempo presenta la mayoría de los eventos clave en el orden correcto, con descripciones generalmente precisas.	La línea de tiempo incluye algunos eventos clave, pero hay errores en la secuenciación o en las descripciones.	La línea de tiempo es incompleta, con varios errores en la secuenciación y descripciones incorrectas o superficiales.	La línea de tiempo es muy básica o está ausente, sin cumplir con los requisitos mínimos de la actividad.
Calidad Visual y Creatividad	La línea de tiempo es visualmente atractiva, con un diseño claro y creativo, utilizando imágenes y elementos gráficos de manera efectiva.	La línea de tiempo es visualmente clara, pero podría beneficiarse de un diseño más creativo o un uso más efectivo de imágenes y gráficos.	La línea de tiempo es funcional, pero el diseño es simple y carece de creatividad o elementos gráficos adecuados.	La línea de tiempo es difícil de seguir visualmente, con un diseño confuso o pobremente ejecutado.	La línea de tiempo carece de un diseño coherente o no se presentó.
Claridad y Coherencia en la Comunicación	Las descripciones y explicaciones en la línea de tiempo son claras, coherentes, y bien escritas, sin errores gramaticales u ortográficos.	Las descripciones y explicaciones son claras y coherentes, con algunos errores menores.	Las descripciones son comprensibles pero contienen varios errores gramaticales u ortográficos.	Las descripciones son difíciles de entender debido a errores gramaticales o falta de coherencia.	La comunicación es poco clara y tiene muchos errores gramaticales y ortográficos.
Puntualidad en la entrega de actividades	Entrega su actividad en los tiempos establecidos en la agenda del tutor.	Entrega su actividad 24 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 48 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 72 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad más de 72 horas después de los tiempos establecidos en la agenda del tutor.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

1

Figura 8.12: Rúbrica de evaluación del reto II del primer módulo.



Puntaje Total:

- **Precisión en la Secuenciación de Eventos:** 50 puntos
- **Calidad Visual y Creatividad:** 50 puntos
- **Claridad y Coherencia en la Comunicación:** 50 puntos
- **Puntualidad en la entrega de actividades:** 50 puntos

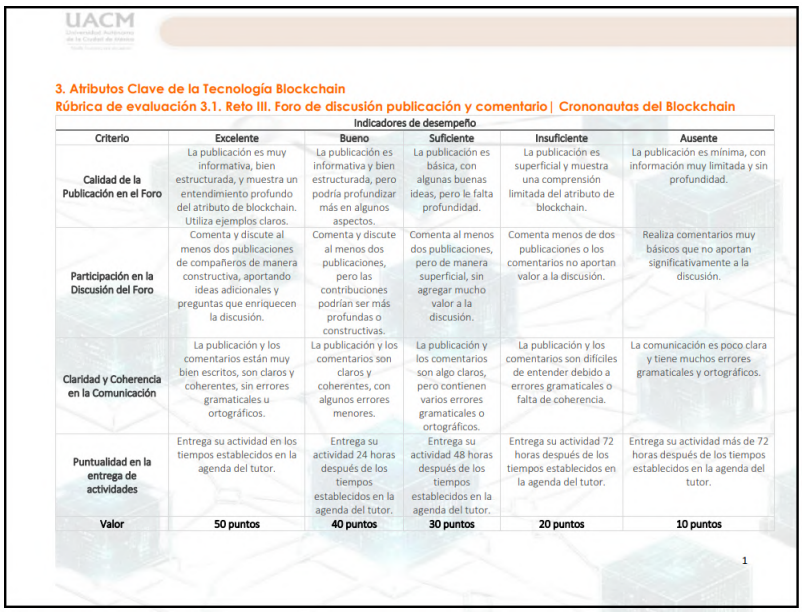
Total posible: 200 puntos

Interpretación de Resultados:

- **Excelente (180-200 puntos):** El estudiante hizo una contribución destacada, mostrando una comprensión profunda y creatividad en la representación visual de la evolución de Blockchain.
- **Bueno (140-179 puntos):** El estudiante hizo buenas contribuciones, pero con margen de mejora en creatividad, claridad, o detalles en la secuenciación.
- **Suficiente (100-139 puntos):** El estudiante participó adecuadamente, pero con varias áreas que podrían mejorar en términos de precisión y calidad visual.
- **Insuficiente (50-99 puntos):** El estudiante tuvo dificultades significativas para hacer contribuciones valiosas y precisas.
- **Ausente (10-49 puntos):** El estudiante realizó contribuciones muy limitadas, con información mínima y sin creatividad, o entregó la actividad muy tarde.

2

Figura 8.13: Interpretación de resultados del reto II del primer módulo.



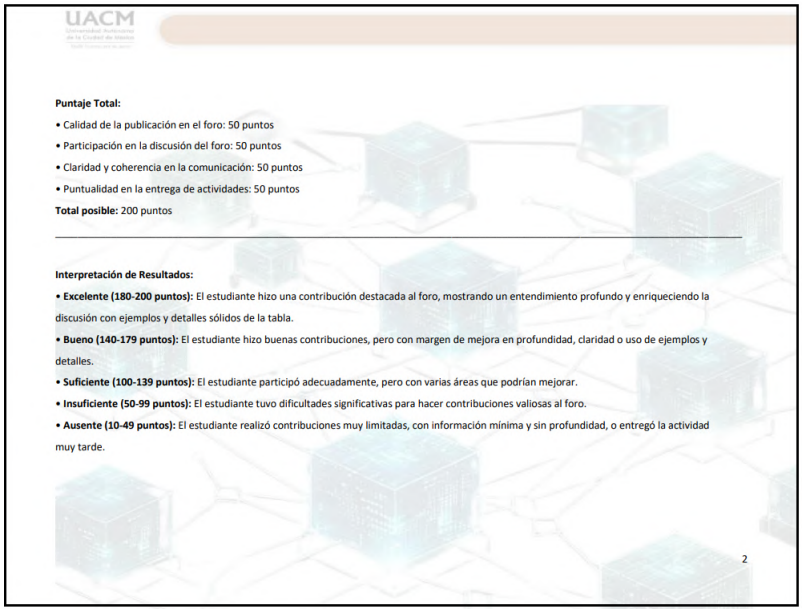
3. Atributos Clave de la Tecnología Blockchain

Rúbrica de evaluación 3.1. Reto III. Foro de discusión publicación y comentario | Crononautas del Blockchain

	Indicadores de desempeño				
Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Calidad de la Publicación en el Foro	La publicación es muy informativa, bien estructurada, y muestra un entendimiento profundo del atributo de blockchain. Utiliza ejemplos claros.	La publicación es informativa y bien estructurada, pero podría profundizar más en algunos aspectos.	La publicación es básica, con algunas buenas ideas, pero le falta profundidad.	La publicación es superficial y muestra una comprensión limitada del atributo de blockchain.	La publicación es mínima, con información muy limitada y sin profundidad.
Participación en la Discusión del Foro	Comenta y discute al menos dos publicaciones de compañeros de manera constructiva, aportando ideas adicionales y preguntas que enriquecen la discusión.	Comenta y discute al menos dos publicaciones, pero las contribuciones podrían ser más profundas o constructivas.	Comenta al menos dos publicaciones, pero de manera superficial, sin agregar mucho valor a la discusión.	Comenta menos de dos publicaciones o los comentarios no aportan valor a la discusión.	Realiza comentarios muy básicos que no aportan significativamente a la discusión.
Claridad y Coherencia en la Comunicación	La publicación y los comentarios están muy bien escritos, son claros y coherentes, sin errores gramaticales u ortográficos.	La publicación y los comentarios son claros y coherentes, con algunos errores menores.	La publicación y los comentarios son algo claros, pero contienen varios errores gramaticales o ortográficos.	La publicación y los comentarios son difíciles de entender debido a errores gramaticales o falta de coherencia.	La comunicación es poco clara y tiene muchos errores gramaticales y ortográficos.
Puntualidad en la entrega de actividades	Entrega su actividad en los tiempos establecidos en la agenda del tutor.	Entrega su actividad 24 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 48 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 72 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad más de 72 horas después de los tiempos establecidos en la agenda del tutor.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

1

Figura 8.14: Rúbrica de evaluación del reto III del primer módulo.



Puntaje Total:

- Calidad de la publicación en el foro: 50 puntos
- Participación en la discusión del foro: 50 puntos
- Claridad y coherencia en la comunicación: 50 puntos
- Puntualidad en la entrega de actividades: 50 puntos

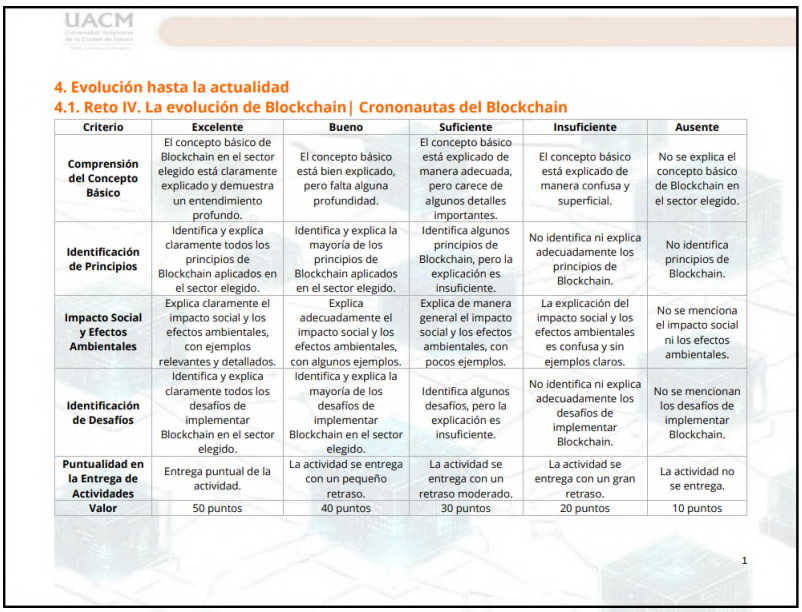
Total posible: 200 puntos

Interpretación de Resultados:

- **Excelente (180-200 puntos):** El estudiante hizo una contribución destacada al foro, mostrando un entendimiento profundo y enriqueciendo la discusión con ejemplos y detalles sólidos de la tabla.
- **Bueno (140-179 puntos):** El estudiante hizo buenas contribuciones, pero con margen de mejora en profundidad, claridad o uso de ejemplos y detalles.
- **Suficiente (100-139 puntos):** El estudiante participó adecuadamente, pero con varias áreas que podrían mejorar.
- **Insuficiente (50-99 puntos):** El estudiante tuvo dificultades significativas para hacer contribuciones valiosas al foro.
- **Ausente (10-49 puntos):** El estudiante realizó contribuciones muy limitadas, con información mínima y sin profundidad, o entregó la actividad muy tarde.

2

Figura 8.15: Interpretación de resultados del reto III del primer módulo.



UACM

4. Evolución hasta la actualidad

4.1. Reto IV. La evolución de Blockchain| Crononautas del Blockchain

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Comprensión del Concepto Básico	El concepto básico de Blockchain en el sector elegido está claramente explicado y demuestra un entendimiento profundo.	El concepto básico está bien explicado, pero falta alguna profundidad.	El concepto básico está explicado de manera adecuada, pero carece de algunos detalles importantes.	El concepto básico está explicado de manera confusa y superficial.	No se explica el concepto básico de Blockchain en el sector elegido.
Identificación de Principios	Identifica y explica claramente todos los principios de Blockchain aplicados en el sector elegido.	Identifica y explica la mayoría de los principios de Blockchain aplicados en el sector elegido.	Identifica algunos principios de Blockchain, pero la explicación es insuficiente.	No identifica ni explica adecuadamente los principios de Blockchain.	No identifica principios de Blockchain.
Impacto Social y Efectos Ambientales	Explica claramente el impacto social y los efectos ambientales, con ejemplos relevantes y detallados.	Explica adecuadamente el impacto social y los efectos ambientales, con algunos ejemplos.	Explica de manera general el impacto social y los efectos ambientales, con pocos ejemplos.	La explicación del impacto social y los efectos ambientales es confusa y sin ejemplos claros.	No se menciona el impacto social ni los efectos ambientales.
Identificación de Desafíos	Identifica y explica claramente todos los desafíos de implementar Blockchain en el sector elegido.	Identifica y explica la mayoría de los desafíos de implementar Blockchain en el sector elegido.	Identifica algunos desafíos, pero la explicación es insuficiente.	No identifica ni explica adecuadamente los desafíos de implementar Blockchain.	No se mencionan los desafíos de implementar Blockchain.
Puntualidad en la Entrega de Actividades	Entrega puntual de la actividad.	La actividad se entrega con un pequeño retraso.	La actividad se entrega con un retraso moderado.	La actividad se entrega con un gran retraso.	La actividad no se entrega.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

1

Figura 8.16: Rúbrica de evaluación del reto IV del primer módulo.

UACM

Puntaje Total

- **Comprensión del Concepto Básico:** 50 puntos
- **Identificación de Principios:** 50 puntos
- **Impacto Social y Efectos Ambientales:** 50 puntos
- **Identificación de Desafíos:** 50 puntos
- **Puntualidad en la Entrega de Actividades:** 50 puntos

Total posible: 250 puntos

Interpretación de Resultados

- **Excelente (235-250 puntos):** El estudiante demostró una comprensión profunda de la evolución de Blockchain, proporcionando análisis detallados y ejemplos relevantes.
- **Bueno (205-234 puntos):** El estudiante mostró un buen entendimiento con algunos detalles y ejemplos faltantes.
- **Suficiente (175-204 puntos):** El estudiante demostró una comprensión adecuada, pero necesita mejorar en varias áreas.
- **Insuficiente (145-174 puntos):** El estudiante tuvo dificultades significativas para entender y explicar los conceptos de Blockchain.
- **Ausente (110-144 puntos):** El estudiante realizó contribuciones muy limitadas, con información mínima y sin profundidad, o entregó la actividad muy tarde.

2

Figura 8.17: Interpretación de resultados del reto IV del primer módulo.

8.5. Módulo 2: Fundamentos de la Criptografía en Blockchain

En esta sección se mostrarán algunos de los temas explicados en el segundo módulo junto con la actividad y las rúbricas de evaluación, cabe mencionar que la información utilizada forma parte del marco teórico de esta tésis.

8.5.1. Capítulos del módulo 1: Introducción a Blockchain. Crononautas del Blockchain

1. Acontecimientos históricos de la Criptografía
   - 1.1 Reto I. Foro de discusión fundamentos de la Criptografía | Guardianes de la Criptografía
2. Conceptos básicos de Criptografía
   - 2.1 Reto II: Aplicación de conceptos básicos de Criptografía | Guardianes de la Criptografía
3. Criptosistemas: Simétricos y Asimétricos
   - 3.1 Reto III: Comparación de criptosistemas simétricos y asimétricos | Guardianes de la Criptografía
4. Funciones Hash y algoritmo SHA
   - 4.1 Reto IV: Funciones Hash y algoritmo SHA | Guardianes de la Criptografía

Figura 8.18: Vista del primer módulo.

Figura 8.19: Vista de actividades (retos) del primer módulo.

A continuación, se muestran los recursos que contiene el primer módulo, los cuales contienen los capítulos, actividades y recursos de este.

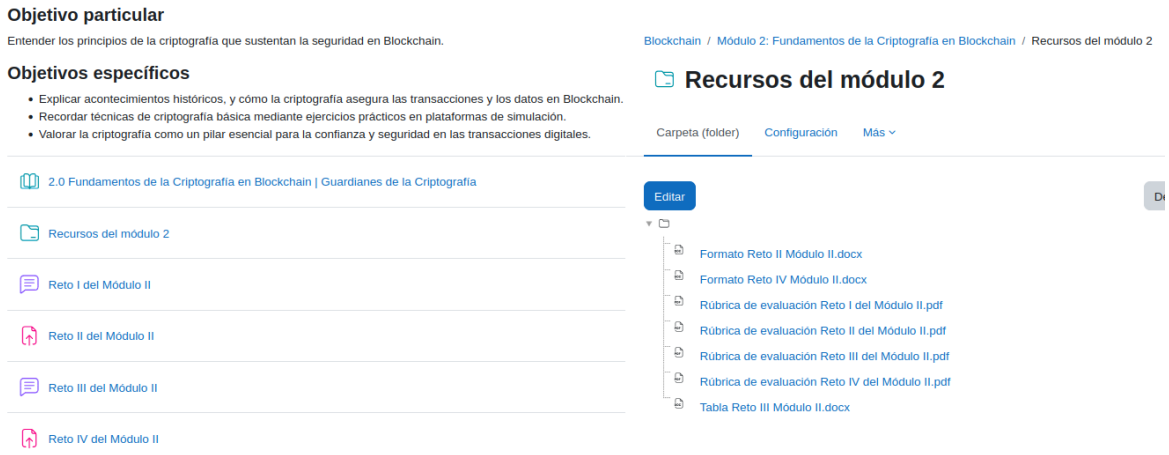


Figura 8.20: Recursos del primer módulo.

8.5.2. Rúbricas de evaluación del primer módulo

En esta sección se muestran las rúbricas de evaluación correspondientes a los cuatro retos del segundo módulo. Estas rúbricas están diseñadas para evaluar de manera estructurada y justa el desempeño de los estudiantes en cada reto.

UACM

1. Acontecimientos históricos de la Criptografía

Rúbrica de evaluación Reto I. Foro de discusión Fundamentos de la Criptografía | Guardianes de la Criptografía

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Análisis del hito histórico seleccionado	El análisis es completo, bien detallado y demuestra una comprensión profunda del hito histórico seleccionado.	El análisis es claro, pero podría profundizar más en algunos aspectos del hito histórico seleccionado.	El análisis es básico, cubre los puntos clave de manera limitada y superficial.	El análisis es superficial y no refleja una comprensión clara del hito histórico seleccionado.	El análisis no se presenta o es muy limitado.
Relación con la criptografía moderna	Establece una relación clara y bien fundamentada entre el hito histórico y su influencia en la criptografía moderna.	La relación es clara, pero no está completamente fundamentada o desarrollada.	Se menciona la relación, pero falta profundidad o claridad en cómo influyó en la criptografía moderna.	La relación con la criptografía moderna es vaga o está ausente.	No se menciona la relación con la criptografía moderna.
Participación en la discusión	Comenta de manera constructiva y crítica en al menos una publicación de un compañero, añadiendo ideas o reflexiones útiles.	Comenta en la publicación de un compañero, pero su aportación podría ser más profunda o relevante.	Comenta de manera superficial en la publicación de un compañero, con aportaciones mínimas.	Comenta de manera insuficiente o no aporta valor a la discusión.	No comenta ni participa en la discusión.
Claridad y coherencia en la comunicación	La publicación y los comentarios están bien escritos, son claros y coherentes, sin errores gramaticales u ortográficos.	La publicación y los comentarios son claros, con algunos errores menores de gramática u ortografía.	La publicación y los comentarios son comprensibles, pero tienen errores que afectan la claridad.	La publicación y los comentarios son difíciles de entender debido a errores gramaticales.	La comunicación es poco clara y tiene muchos errores.
Puntualidad en la entrega de actividades	Entrega su actividad en los tiempos establecidos en la agenda del tutor.	Entrega su actividad 24 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 48 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 72 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad más de 72 horas después de los tiempos establecidos en la agenda del tutor.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

1

Figura 8.21: Rúbrica de evaluación del reto I del segundo módulo.

Puntaje Total:

- **Análisis del hito histórico seleccionado:** 50 puntos
- **Relación con la criptografía moderna:** 50 puntos
- **Participación en la discusión:** 50 puntos
- **Claridad y coherencia en la comunicación:** 50 puntos
- **Puntualidad en la entrega de actividades:** 50 puntos

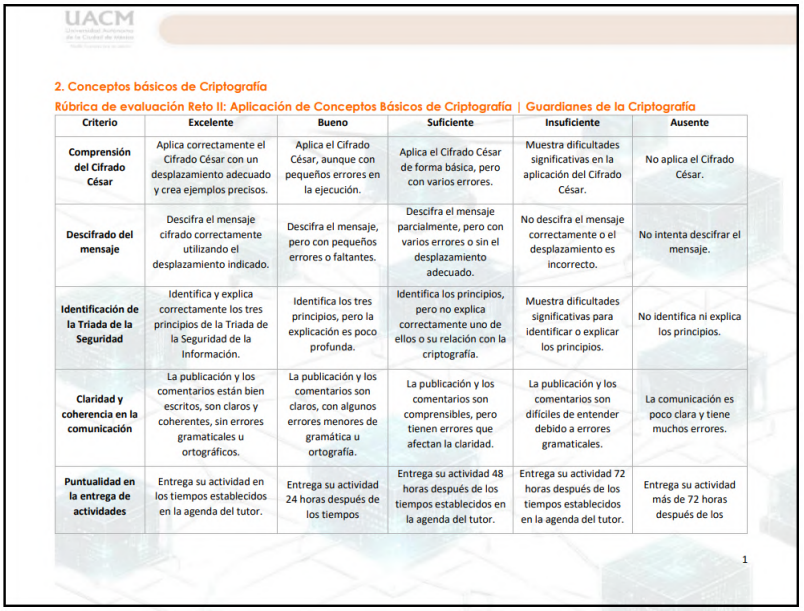
Total posible: 250 puntos

Interpretación de Resultados:

- **Excelente (225-250 puntos):** El estudiante ha realizado un análisis profundo y preciso, estableciendo conexiones claras entre la historia y la criptografía moderna.
- **Bueno (175-224 puntos):** El análisis es sólido, aunque algunos aspectos podrían desarrollarse más o con mayor claridad.
- **Suficiente (125-174 puntos):** El estudiante ha cubierto los puntos principales, pero de forma limitada o superficial.
- **Insuficiente (75-124 puntos):** El estudiante ha tenido dificultades para realizar un análisis adecuado y establecer las relaciones pertinentes.
- **Ausente (10-74 puntos):** El estudiante no ha entregado la actividad o lo ha hecho de manera muy incompleta.

2

Figura 8.22: Interpretación de resultados del reto I del segundo módulo.



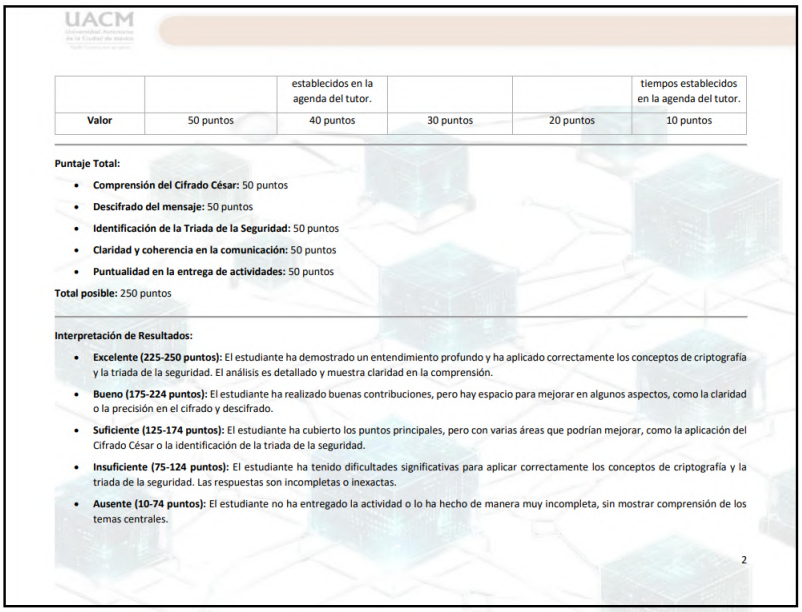
2. Conceptos básicos de Criptografía

Rúbrica de evaluación Reto II: Aplicación de Conceptos Básicos de Criptografía | Guardianes de la Criptografía

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Comprensión del Cifrado César	Aplica correctamente el Cifrado César con un desplazamiento adecuado y crea ejemplos precisos.	Aplica el Cifrado César, aunque con pequeños errores en la ejecución.	Aplica el Cifrado César de forma básica, pero con varios errores.	Muestra dificultades significativas en la aplicación del Cifrado César.	No aplica el Cifrado César.
Descifrado del mensaje	Descifra el mensaje cifrado correctamente utilizando el desplazamiento indicado.	Descifra el mensaje, pero con pequeños errores o faltantes.	Descifra el mensaje parcialmente, pero con varios errores o sin el desplazamiento adecuado.	No descifra el mensaje correctamente o el desplazamiento es incorrecto.	No intenta descifrar el mensaje.
Identificación de la Triada de la Seguridad	Identifica y explica correctamente los tres principios de la Triada de la Seguridad de la Información.	Identifica los tres principios, pero la explicación es poco profunda.	Identifica los principios, pero no explica correctamente uno de ellos o su relación con la criptografía.	Muestra dificultades significativas para identificar o explicar los principios.	No identifica ni explica los principios.
Claridad y coherencia en la comunicación	La publicación y los comentarios están bien escritos, son claros y coherentes, sin errores gramaticales u ortográficos.	La publicación y los comentarios son claros, con algunos errores menores de gramática u ortografía.	La publicación y los comentarios son comprensibles, pero tienen errores que afectan la claridad.	La publicación y los comentarios son difíciles de entender debido a errores gramaticales.	La comunicación es poco clara y tiene muchos errores.
Puntualidad en la entrega de actividades	Entrega su actividad en los tiempos establecidos en la agenda del tutor.	Entrega su actividad 24 horas después de los tiempos	Entrega su actividad 48 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 72 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad más de 72 horas después de los

1

Figura 8.23: Rúbrica de evaluación del reto II del segundo módulo.



		establecidos en la agenda del tutor.			tiempos establecidos en la agenda del tutor.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

Puntaje Total:

- **Comprensión del Cifrado César:** 50 puntos
- **Descifrado del mensaje:** 50 puntos
- **Identificación de la Triada de la Seguridad:** 50 puntos
- **Claridad y coherencia en la comunicación:** 50 puntos
- **Puntualidad en la entrega de actividades:** 50 puntos

Total posible: 250 puntos

Interpretación de Resultados:

- **Excelente (225-250 puntos):** El estudiante ha demostrado un entendimiento profundo y ha aplicado correctamente los conceptos de criptografía y la triada de la seguridad. El análisis es detallado y muestra claridad en la comprensión.
- **Bueno (175-224 puntos):** El estudiante ha realizado buenas contribuciones, pero hay espacio para mejorar en algunos aspectos, como la claridad o la precisión en el cifrado y descifrado.
- **Suficiente (125-174 puntos):** El estudiante ha cubierto los puntos principales, pero con varias áreas que podrían mejorar, como la aplicación del Cifrado César o la identificación de la triada de la seguridad.
- **Insuficiente (75-124 puntos):** El estudiante ha tenido dificultades significativas para aplicar correctamente los conceptos de criptografía y la triada de la seguridad. Las respuestas son incompletas o inexactas.
- **Ausente (10-74 puntos):** El estudiante no ha entregado la actividad o lo ha hecho de manera muy incompleta, sin mostrar comprensión de los temas centrales.

2

Figura 8.24: Interpretación de resultados del reto II del segundo módulo.

3. Criptosistemas: Simétricos y Asimétricos

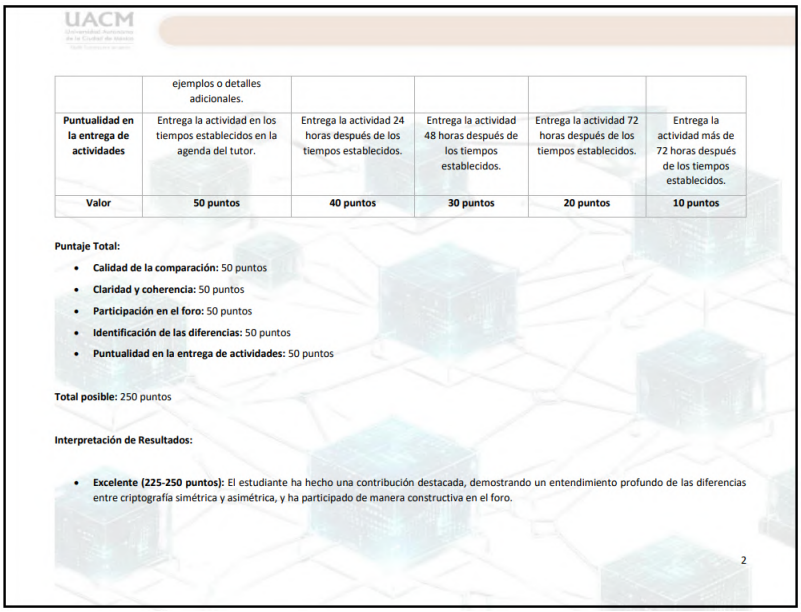
Rúbrica de evaluación Reto III: Comparación de Criptosistemas Simétricos y Asimétricos

| Guardianes de la Criptografía

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Calidad de la comparación	La comparación es clara y bien estructurada. Identifica y explica de manera precisa al menos cinco diferencias clave entre criptografía simétrica y asimétrica.	La comparación es clara, pero algunas diferencias no están completamente desarrolladas o explicadas.	La comparación identifica las diferencias, pero con explicaciones limitadas o inexactas.	La comparación es superficial y no logra identificar adecuadamente las diferencias clave.	No realiza la comparación o las diferencias son incorrectas o ausentes.
Claridad y coherencia	La explicación está muy bien escrita, con claridad y coherencia. No presenta errores gramaticales u ortográficos.	La explicación es clara, pero presenta algunos errores menores que no afectan la comprensión.	La explicación es comprensible, pero con varios errores que afectan la claridad general.	La explicación tiene errores que dificultan la comprensión o coherencia del mensaje.	La explicación es confusa o está incompleta, con múltiples errores.
Participación en el foro	Comenta al menos dos publicaciones de compañeros, aportando ideas adicionales, preguntas o críticas constructivas.	Comenta al menos dos publicaciones, pero sus aportaciones podrían ser más profundas o constructivas.	Comenta dos publicaciones, pero de manera superficial, sin agregar mucho valor a la discusión.	Comenta menos de dos publicaciones o los comentarios no aportan valor a la discusión.	No participa en el foro o los comentarios no son significativos.
Identificación de las diferencias	Identifica claramente las diferencias clave entre criptografía simétrica y asimétrica, proporcionando	Identifica las diferencias, pero algunas podrían estar mejor desarrolladas o más detalladas.	Identifica diferencias, pero de manera básica o con algunos errores.	Las diferencias no están claramente explicadas o son incorrectas.	No identifica las diferencias o lo hace de forma incorrecta.

1

Figura 8.25: Rúbrica de evaluación del reto III del segundo módulo.



	ejemplos o detalles adicionales.				
Puntualidad en la entrega de actividades	Entrega la actividad en los tiempos establecidos en la agenda del tutor.	Entrega la actividad 24 horas después de los tiempos establecidos.	Entrega la actividad 48 horas después de los tiempos establecidos.	Entrega la actividad 72 horas después de los tiempos establecidos.	Entrega la actividad más de 72 horas después de los tiempos establecidos.
Valor	**50 puntos**	**40 puntos**	**30 puntos**	**20 puntos**	**10 puntos**

Puntaje Total:

- **Calidad de la comparación:** 50 puntos
- **Claridad y coherencia:** 50 puntos
- **Participación en el foro:** 50 puntos
- **Identificación de las diferencias:** 50 puntos
- **Puntualidad en la entrega de actividades:** 50 puntos

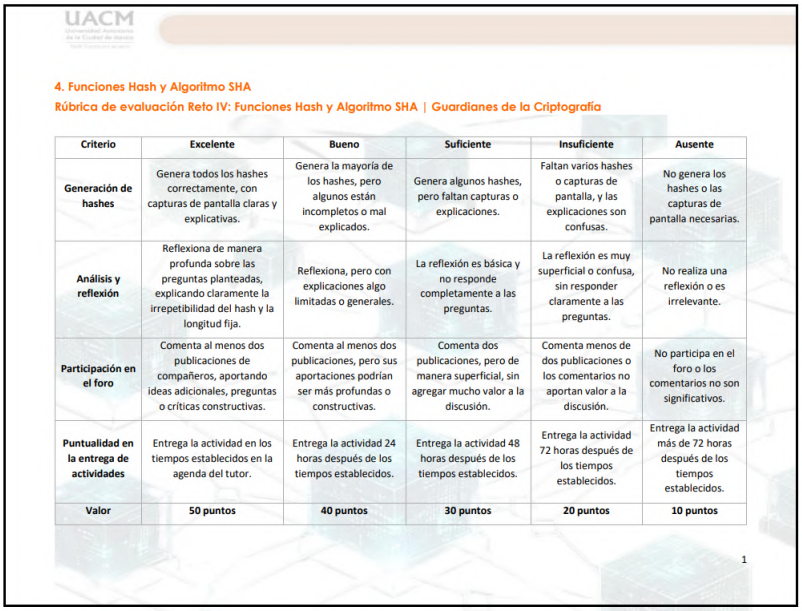
Total posible: 250 puntos

Interpretación de Resultados:

- **Excelente (225-250 puntos):** El estudiante ha hecho una contribución destacada, demostrando un entendimiento profundo de las diferencias entre criptografía simétrica y asimétrica, y ha participado de manera constructiva en el foro.

2

Figura 8.26: Interpretación de resultados del reto III del segundo módulo.



4. Funciones Hash y Algoritmo SHA

Rúbrica de evaluación Reto IV: Funciones Hash y Algoritmo SHA | Guardianes de la Criptografía

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Generación de hashes	Genera todos los hashes correctamente, con capturas de pantalla claras y explicativas.	Genera la mayoría de los hashes, pero algunos están incompletos o mal explicados.	Genera algunos hashes, pero faltan capturas o explicaciones.	Faltan varios hashes o capturas de pantalla, y las explicaciones son confusas.	No genera los hashes o las capturas de pantalla necesarias.
Análisis y reflexión	Reflexiona de manera profunda sobre las preguntas planteadas, explicando claramente la irrepetibilidad del hash y la longitud fija.	Reflexiona, pero con explicaciones algo limitadas o generales.	La reflexión es básica y no responde completamente a las preguntas.	La reflexión es muy superficial o confusa, sin responder claramente a las preguntas.	No realiza una reflexión o es irrelevante.
Participación en el foro	Comenta al menos dos publicaciones de compañeros, aportando ideas adicionales, preguntas o críticas constructivas.	Comenta al menos dos publicaciones, pero sus aportaciones podrían ser más profundas o constructivas.	Comenta dos publicaciones, pero de manera superficial, sin agregar mucho valor a la discusión.	Comenta menos de dos publicaciones o los comentarios no aportan valor a la discusión.	No participa en el foro o los comentarios no son significativos.
Puntualidad en la entrega de actividades	Entrega la actividad en los tiempos establecidos en la agenda del tutor.	Entrega la actividad 24 horas después de los tiempos establecidos.	Entrega la actividad 48 horas después de los tiempos establecidos.	Entrega la actividad 72 horas después de los tiempos establecidos.	Entrega la actividad más de 72 horas después de los tiempos establecidos.
Valor	**50 puntos**	**40 puntos**	**30 puntos**	**20 puntos**	**10 puntos**

1

Figura 8.27: Rúbrica de evaluación del reto IV del segundo módulo.

Figura 8.28: Interpretación de resultados del reto IV del segundo módulo.

8.6. Módulo 3: Conceptos básicos de Blockchain

En esta sección se mostrarán algunos de los temas explicados en el tercer módulo junto con la actividad y las rúbricas de evaluación, cabe mencionar que la información utilizada forma parte del marco teórico de esta tésis.

8.6.1. Capítulos del módulo 1: Introducción a Blockchain. Crononautas del Blockchain

1. Árbol de Merkle
   - 1.1 Reto I del Módulo III: Foro árbol de Merkle | Arquitectos de Blockchain
2. Elementos de un bloque y el proceso de minado
   - 2.1 Reto II del Módulo III: Comprender los Elementos de un Bloque y el Proceso de Minado | Arquitectos de Blockchain
3. Cadena de bloques
   - 3.1 Reto III del Módulo III: Simulación de la cadena de bloques y análisis de cambios en los hashes | Arquitectos de Blockchain
4. Cadena de bloques distribuida y consensos
   - 4.1 Reto IV del Módulo III: Simulación de Blockchain distribuido | Arquitectos de Blockchain
   - 4.2 Rúbrica de evaluación: La evolución de Blockchain | Crononautas del Blockchain
5. Primeros pasos con Python y Google Colaboratory

Figura 8.29: Vista del primer módulo.

Figura 8.30: Vista de actividades (retos) del primer módulo.

A continuación, se muestran los recursos que contiene el primer módulo, los cuales contienen los capítulos, actividades y recursos de este.

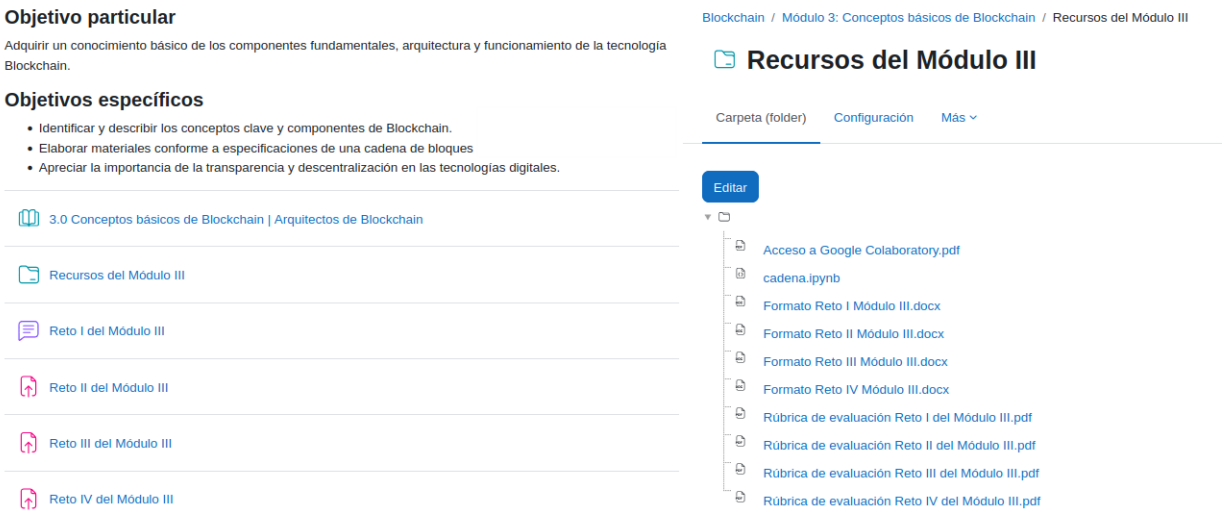


Figura 8.31: Recursos del primer módulo.

8.6.2. Rúbricas de evaluación del tercer módulo

En esta sección se muestran las rúbricas de evaluación correspondientes a los cuatro retos del tercer módulo. Estas rúbricas están diseñadas para evaluar de manera estructurada y justa el desempeño de los estudiantes en cada reto.

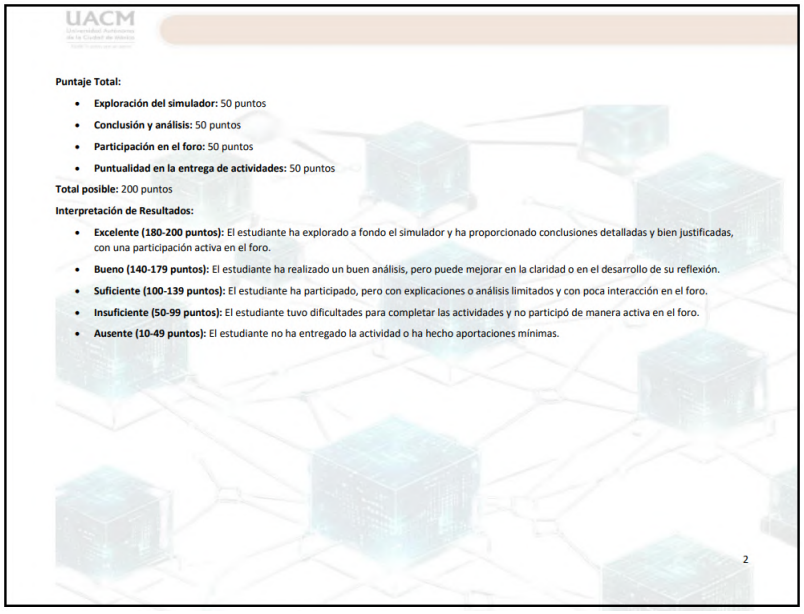
1. Árbol de Merkle

Rúbrica de evaluación Reto I del Módulo III: Foro Árbol de Merkle | Arquitectos de Blockchain

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Exploración del simulador	Explora el simulador de forma exhaustiva, realizando múltiples modificaciones en los nodos y generando capturas detalladas.	Explora el simulador, pero algunas capturas no son claras o faltan detalles sobre las modificaciones.	Explora el simulador de manera limitada, con capturas incompletas o poco detalladas.	Explora el simulador, pero las capturas de pantalla son mínimas y faltan explicaciones detalladas.	No explora el simulador o no presenta capturas de pantalla adecuadas.
Conclusión y análisis	La conclusión muestra un análisis profundo sobre el impacto de las modificaciones en el Root Hash y la integridad de los datos.	La conclusión es clara, pero algunas ideas no están completamente desarrolladas o faltan detalles.	La conclusión es básica, con algunas observaciones generales pero sin mucho detalle.	La conclusión es muy superficial o confusa, sin responder completamente a las preguntas.	No presenta una conclusión o esta es irrelevante.
Participación en el foro	Comenta al menos dos publicaciones de compañeros, aportando ideas adicionales, preguntas o críticas constructivas.	Comenta al menos dos publicaciones, pero sus aportaciones podrían ser más profundas o constructivas.	Comenta dos publicaciones, pero de manera superficial, sin agregar mucho valor a la discusión.	Comenta menos de dos publicaciones o los comentarios no aportan valor a la discusión.	No participa en el foro o los comentarios no son significativos.
Puntualidad en la entrega de actividades	Entrega la actividad en los tiempos establecidos en la agenda del tutor.	Entrega la actividad 24 horas después de los tiempos establecidos.	Entrega la actividad 48 horas después de los tiempos establecidos.	Entrega la actividad 72 horas después de los tiempos establecidos.	Entrega la actividad más de 72 horas después de los tiempos establecidos.
Valor	**50 puntos**	**40 puntos**	**30 puntos**	**20 puntos**	**10 puntos**

1

Figura 8.32: Rúbrica de evaluación del reto I del tercer módulo.



Puntaje Total:

- **Exploración del simulador:** 50 puntos
- **Conclusión y análisis:** 50 puntos
- **Participación en el foro:** 50 puntos
- **Puntualidad en la entrega de actividades:** 50 puntos

Total posible: 200 puntos

Interpretación de Resultados:

- **Excelente (180-200 puntos):** El estudiante ha explorado a fondo el simulador y ha proporcionado conclusiones detalladas y bien justificadas, con una participación activa en el foro.
- **Bueno (140-179 puntos):** El estudiante ha realizado un buen análisis, pero puede mejorar en la claridad o en el desarrollo de su reflexión.
- **Suficiente (100-139 puntos):** El estudiante ha participado, pero con explicaciones o análisis limitados y con poca interacción en el foro.
- **Insuficiente (50-99 puntos):** El estudiante tuvo dificultades para completar las actividades y no participó de manera activa en el foro.
- **Ausente (10-49 puntos):** El estudiante no ha entregado la actividad o ha hecho aportaciones mínimas.

2

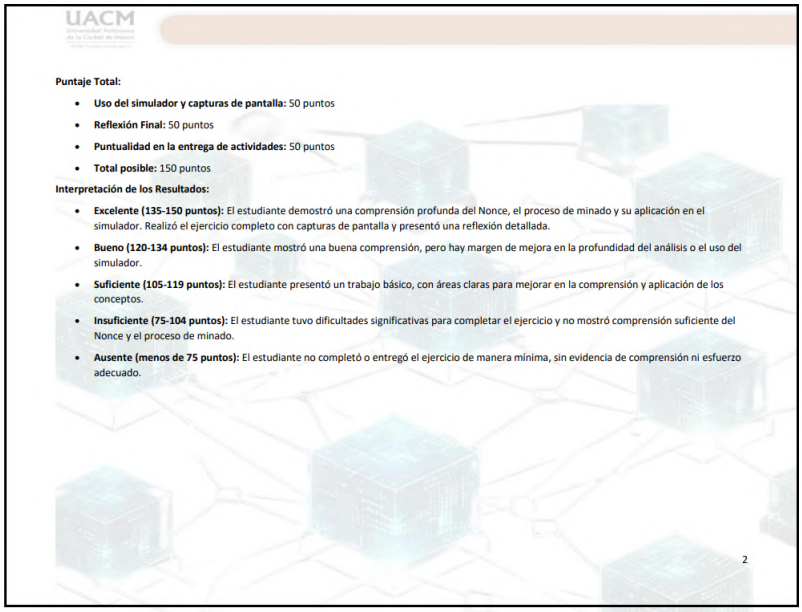
Figura 8.33: Interpretación de resultados del reto I del tercer módulo.

2. Elementos de un Bloque y el Proceso de MinadoRúbrica de evaluación Reto II del Módulo III: Comprender los Elementos de un Bloque y el Proceso de Minado | Arquitectos de Blockchain

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Uso del Simulador y Capturas de Pantalla	Realiza correctamente el ejercicio en el simulador, presentando capturas de pantalla que muestran claramente los cambios en el Nonce, datos y hash antes y después de minar.	Realiza correctamente el ejercicio en el simulador, presentando capturas de pantalla, pero con claridad suficiente para ilustrar los cambios en el Nonce, datos y hash.	Utiliza el simulador, pero las capturas de pantalla no son suficientes o no muestran claramente los cambios en el Nonce, datos y hash.	Utiliza el simulador de forma incorrecta o no proporciona capturas de pantalla suficientes ni claras para mostrar los resultados del ejercicio.	No utiliza el simulador o no proporciona capturas de pantalla.
Reflexión Final	La reflexión muestra un análisis profundo de la relación entre el Nonce, los datos y el hash, explicando claramente cómo el proceso de minado asegura la validación del bloque. Aporta ideas nuevas o perspectivas interesantes.	La reflexión explica correctamente la relación entre el Nonce, los datos y el hash, pero con un análisis que podría ser más profundo. No se incluyen perspectivas adicionales.	La reflexión es superficial, mencionando la relación entre el Nonce, los datos y el hash, pero sin un análisis detallado.	La reflexión es confusa o no muestra una comprensión clara de la relación entre el Nonce, los datos y el hash, o cómo el proceso de minado asegura la validación del bloque.	No se presenta reflexión o la reflexión no está relacionada con el tema.
Puntualidad en la Entrega de Actividades	Entrega su actividad en los tiempos establecidos en la agenda del tutor.	Entrega su actividad 24 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 48 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad 72 horas después de los tiempos establecidos en la agenda del tutor.	Entrega su actividad más de 72 horas después de los tiempos establecidos en la agenda del tutor.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

1

Figura 8.34: Rúbrica de evaluación del reto II del tercer módulo.



Puntaje Total:

- **Uso del simulador y capturas de pantalla:** 50 puntos
- **Reflexión Final:** 50 puntos
- **Puntualidad en la entrega de actividades:** 50 puntos
- **Total posible:** 150 puntos

Interpretación de los Resultados:

- **Excelente (135-150 puntos):** El estudiante demostró una comprensión profunda del Nonce, el proceso de minado y su aplicación en el simulador. Realizó el ejercicio completo con capturas de pantalla y presentó una reflexión detallada.
- **Bueno (120-134 puntos):** El estudiante mostró una buena comprensión, pero hay margen de mejora en la profundidad del análisis o el uso del simulador.
- **Suficiente (105-119 puntos):** El estudiante presentó un trabajo básico, con áreas claras para mejorar en la comprensión y aplicación de los conceptos.
- **Insuficiente (75-104 puntos):** El estudiante tuvo dificultades significativas para completar el ejercicio y no mostró comprensión suficiente del Nonce y el proceso de minado.
- **Ausente (menos de 75 puntos):** El estudiante no completó o entregó el ejercicio de manera mínima, sin evidencia de comprensión ni esfuerzo adecuado.

2

Figura 8.35: Interpretación de resultados del reto II del tercer módulo.

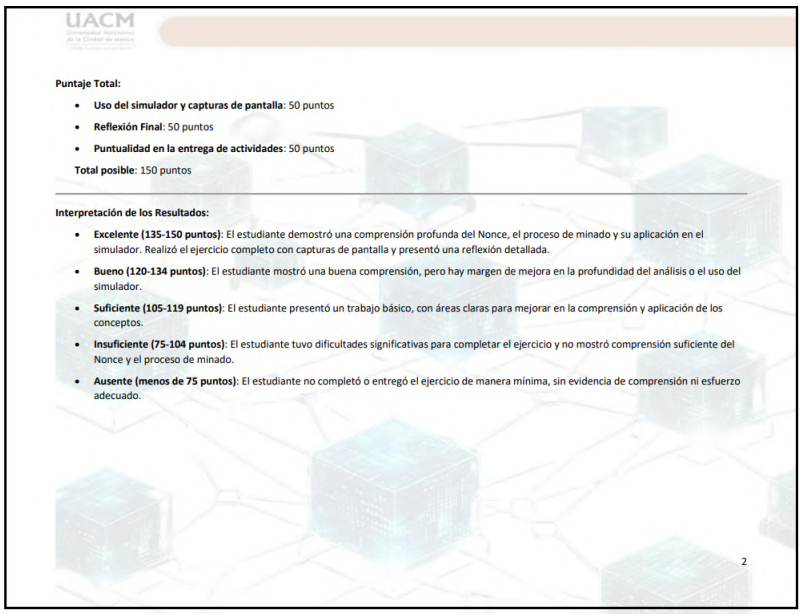
3. Cadena de Bloques

Reto III del Módulo III: Simulación de la Cadena de Bloques y Análisis de Cambios en los Hashes | Arquitectos de Blockchain

Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Uso del Simulador y Capturas de Pantalla	Realiza correctamente el ejercicio en el simulador, presentando al menos cinco capturas de pantalla claras que muestran los cambios antes y después de minar.	Realiza el ejercicio con menos de cinco capturas, pero las capturas son claras.	Utiliza el simulador, pero las capturas no son claras o son insuficientes.	Utiliza el simulador de manera incorrecta, y las capturas no muestran el proceso correctamente.	No utiliza el simulador o no proporciona capturas.
Reflexión Final	La reflexión muestra un análisis profundo y bien estructurado sobre el impacto de los cambios en los bloques y la importancia del hash.	La reflexión explica correctamente los puntos clave, pero podría ser más profunda.	La reflexión es superficial y carece de detalles.	La reflexión no demuestra comprensión clara del tema.	No se presenta reflexión o no está relacionada con el tema.
Puntualidad en la Entrega de Actividades	Entrega su actividad en los tiempos establecidos en la agenda del tutor.	Entrega su actividad 24 horas después de los tiempos establecidos.	Entrega su actividad 48 horas después de los tiempos establecidos.	Entrega su actividad 72 horas después de los tiempos establecidos.	Entrega su actividad más de 72 horas después de los tiempos establecidos.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

1

Figura 8.36: Rúbrica de evaluación del reto III del tercer módulo.



Puntaje Total:

- **Uso del simulador y capturas de pantalla**: 50 puntos
- **Reflexión Final**: 50 puntos
- **Puntualidad en la entrega de actividades**: 50 puntos

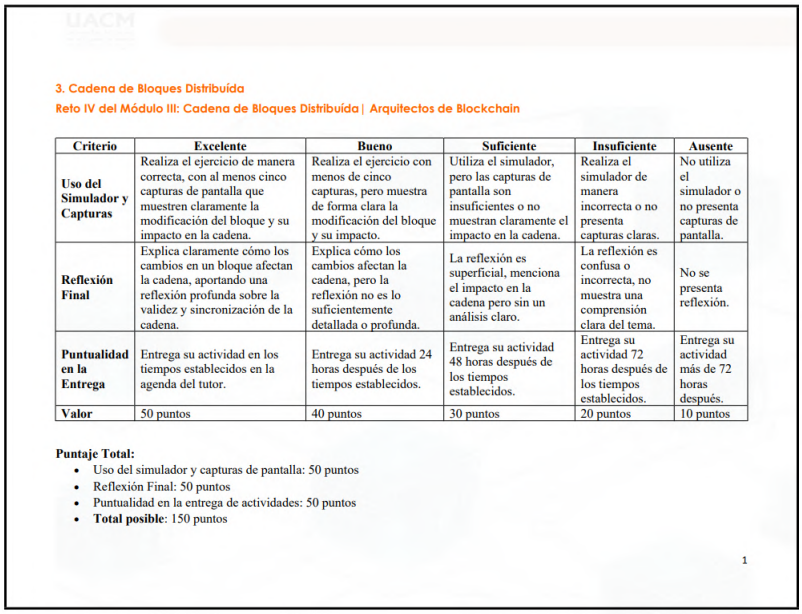
Total posible: 150 puntos

Interpretación de los Resultados:

- **Excelente (135-150 puntos)**: El estudiante demostró una comprensión profunda del Nonce, el proceso de minado y su aplicación en el simulador. Realizó el ejercicio completo con capturas de pantalla y presentó una reflexión detallada.
- **Bueno (120-134 puntos)**: El estudiante mostró una buena comprensión, pero hay margen de mejora en la profundidad del análisis o el uso del simulador.
- **Suficiente (105-119 puntos)**: El estudiante presentó un trabajo básico, con áreas claras para mejorar en la comprensión y aplicación de los conceptos.
- **Insuficiente (75-104 puntos)**: El estudiante tuvo dificultades significativas para completar el ejercicio y no mostró comprensión suficiente del Nonce y el proceso de minado.
- **Ausente (menos de 75 puntos)**: El estudiante no completó o entregó el ejercicio de manera mínima, sin evidencia de comprensión ni esfuerzo adecuado.

2

Figura 8.37: Interpretación de resultados del reto III del tercer módulo.



3. Cadena de Bloques Distribuída

Reto IV del Módulo III: Cadena de Bloques Distribuída | Arquitectos de Blockchain

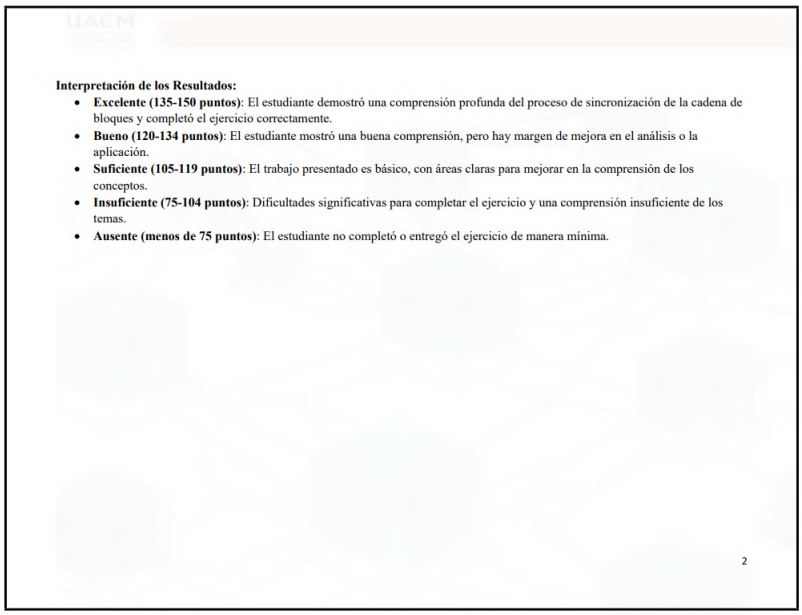
Criterio	Excelente	Bueno	Suficiente	Insuficiente	Ausente
Uso del Simulador y Capturas	Realiza el ejercicio de manera correcta, con al menos cinco capturas de pantalla que muestren claramente la modificación del bloque y su impacto en la cadena.	Realiza el ejercicio con menos de cinco capturas, pero muestra de forma clara la modificación del bloque y su impacto.	Utiliza el simulador, pero las capturas de pantalla son insuficientes o no muestran claramente el impacto en la cadena.	Realiza el simulador de manera incorrecta o no presenta capturas claras.	No utiliza el simulador o no presenta capturas de pantalla.
Reflexión Final	Explica claramente cómo los cambios en un bloque afectan la cadena, aportando una reflexión profunda sobre la validez y sincronización de la cadena.	Explica cómo los cambios afectan la cadena, pero la reflexión no es lo suficientemente detallada o profunda.	La reflexión es superficial, menciona el impacto en la cadena pero sin un análisis claro.	La reflexión es confusa o incorrecta, no muestra una comprensión clara del tema.	No se presenta reflexión.
Puntualidad en la Entrega	Entrega su actividad en los tiempos establecidos en la agenda del tutor.	Entrega su actividad 24 horas después de los tiempos establecidos.	Entrega su actividad 48 horas después de los tiempos establecidos.	Entrega su actividad 72 horas después de los tiempos establecidos.	Entrega su actividad más de 72 horas después.
Valor	50 puntos	40 puntos	30 puntos	20 puntos	10 puntos

Puntaje Total:

- Uso del simulador y capturas de pantalla: 50 puntos
- Reflexión Final: 50 puntos
- Puntualidad en la entrega de actividades: 50 puntos
- **Total posible**: 150 puntos

1

Figura 8.38: Rúbrica de evaluación del reto IV del tercer módulo.



Interpretación de los Resultados:

- **Excelente (135-150 puntos)**: El estudiante demostró una comprensión profunda del proceso de sincronización de la cadena de bloques y completó el ejercicio correctamente.
- **Bueno (120-134 puntos)**: El estudiante mostró una buena comprensión, pero hay margen de mejora en el análisis o la aplicación.
- **Suficiente (105-119 puntos)**: El trabajo presentado es básico, con áreas claras para mejorar en la comprensión de los conceptos.
- **Insuficiente (75-104 puntos)**: Dificultades significativas para completar el ejercicio y una comprensión insuficiente de los temas.
- **Ausente (menos de 75 puntos)**: El estudiante no completó o entregó el ejercicio de manera mínima.

2

Figura 8.39: Interpretación de resultados del reto IV del tercer módulo.

8.6.3. Primeros pasos con Python y Google Colaboratory

Para la etapa final del curso se creó una sección en donde los estudiantes tendrán la oportunidad de estudiar los diferentes componentes de blokchain con Python. Esta actividad será realizada mediante Google Colaboratory, por lo que no será nacesaria la instalación de ningún software, además se les comparte un breve manual de cómo configurar dicha herramienta.

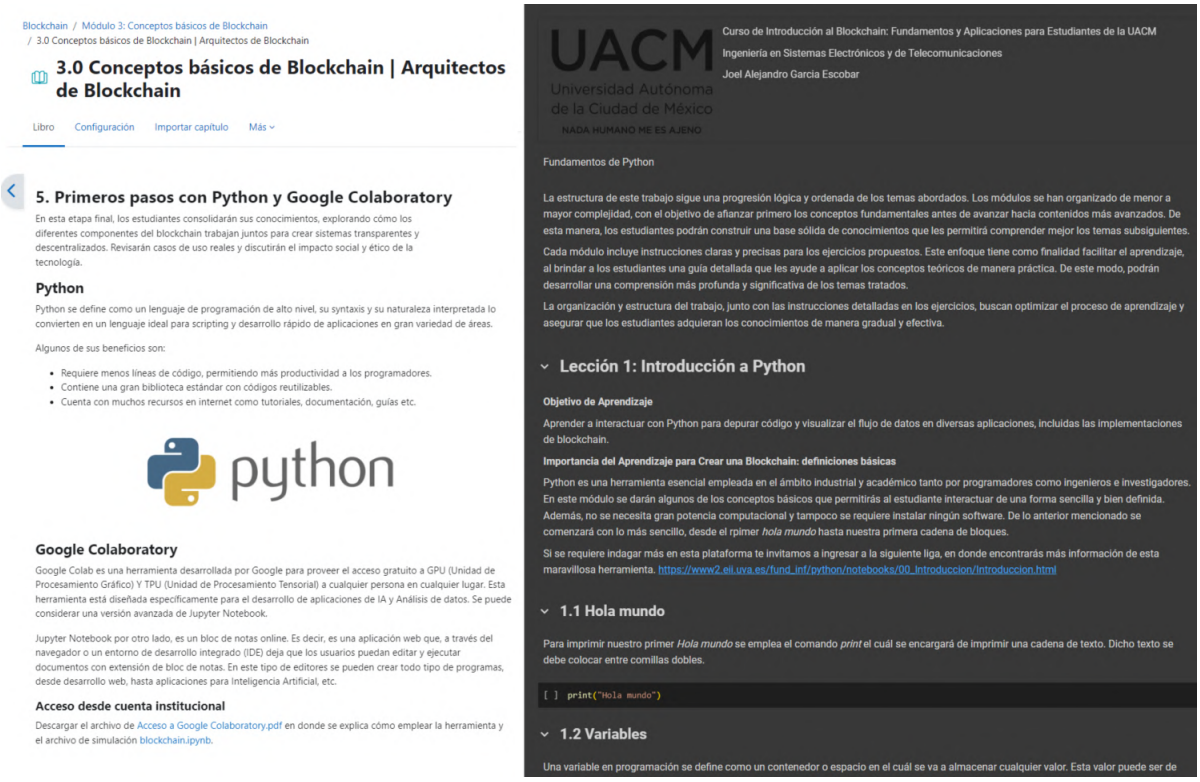


Figura 8.40: Actividad primeros pasos con Python.

En esta actividad se presentan conceptos básicos para programar en Python, con el fin de que los estudiantes puedan comprender el código relacionado con la cadena de bloques. Es importante señalar que esta tesis no tiene como objetivo enseñar Python de manera exhaustiva. Por ello, la actividad no incluye una rúbrica de evaluación y se considera exclusivamente informativa, permitiendo a los estudiantes llevarse el contenido a casa para su estudio.

```
[ ] from hashlib import sha256

    transactions1 = ["Dani le envia 5 a Luis",
                     "Luis le envia 3 a Aida",
                     "Dani le envia 1 a Mauro"]

    transactions2 = ["Juan le envia 5 a Marta",
                     "Mauro le envia 3 a Aida",
                     "Luis le envia 2 a Javier"]

    class Block:
      def __init__(self,previous_hash_block,data):
        self.previous_hash_block = previous_hash_block
        self.data = data
        self.nonce = 0

      def hash(self):
        info = " | ".join(self.data) + self.previous_hash_block + str(self.nonce)
        return sha256(info.encode()).hexdigest()


    class Blockchain:
      difficulty = 3

      def __init__(self):
        self.chain = []

      def add(self,block):
        self.chain.append(block)

      def mine(self,block):
        while True:
          if block.hash()[:self.difficulty] == "0"*self.difficulty:
            self.add(block)
            break
          else:
            block.nonce += 1

    block_chain = Blockchain()

    b1 = Block("0"*64,transactions1)
    #print("Hash bloque 1: ", b1.hash())
    block_chain.mine(b1)
    print("Hash minado bloque 1: ",block_chain.chain[0].hash())
    print("Valor del nonce: ",block_chain.chain[0].nonce)
    print("_____________________________________________________________________________")

    b2 = Block(block_chain.chain[-1].hash(),transactions2)
    #print("Hash bloque 2: ", b2.hash())
    block_chain.mine(b2)
    print("Hash minado bloque 2: ",block_chain.chain[1].hash())
    print("Valor del nonce: ",block_chain.chain[1].nonce)
    print("_____________________________________________________________________________")

    Hash minado bloque 1:  0004b3b3128d3eb262aadf80cfe40c8b9b9d75af3090cd876810632fd1e84475
    Valor del nonce:  2362
    _____________________________________________________________________________
    Hash minado bloque 2:  000ee365115eed02d3fd646d5710d059f476a2d8e611345f7711e08200cca858
    Valor del nonce:  8982
    _____________________________________________________________________________
```

Figura 8.41: Impresión de una cadena de bloques mediante Python.

Capítulo 9

Resultados

En esta sección se documentan las actividades de los estudiantes, acompañado de sus respectivas evidencias. Cabe mencionar que por cuestiones de tiempo algunos de los retos no fueron llevados a cabo, así mismo, algunos estudiantes presentaron inconvenientes con la disponibilidad por lo que no todos realizaron las mismas actividades.

9.1. Evaluación dignostica y foro de bienvenida

Antes de comenzar con el curso, se les pidió participar en un foro de bienvenida compartiendo sus comentarios de lo que saben o creen que es Blockchain.

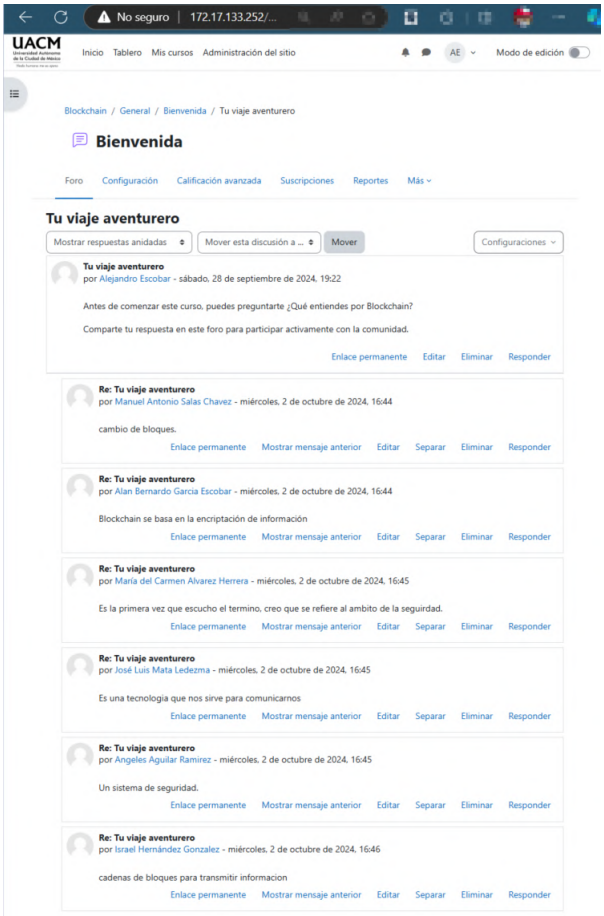


Figura 9.1: Resultados del foro Tu viaje aventurero.

A continuación se comparten los datos de la evaluación diagnóstica:

	Nombre / Apellido(s)	Dirección Email	Estado	Iniciado	Finalizado	Duración	Calificación/10.00	Q. 1 /1.25	Q. 2 /1.25	Q. 3 /1.25	Q. 4 /1.25	Q. 5 /1.25	Q. 6 /1.25	Q. 7 /1.25	Q. 8 /1.25
IH	Israel Hernández Gonzalez Revisión del intento	israel.hernandez@alumnos.uacm.edu.mx	Terminados	2 de octubre de 2024 16:44	2 de octubre de 2024 16:51	6 mins 29 segundos	6.25	✓ 1.25	✗ 0.00	✗ 0.00	✓ 1.25	✓ 1.25	✗ 0.00	✓ 1.25	✓ 1.25
MS	Manuel Antonio Salas Chavez Revisión del intento	manuel.salas@estudiante.uacm.edu.mx	Terminados	2 de octubre de 2024 16:48	2 de octubre de 2024 16:52	3 mins 56 segundos	3.75	✗ 0.00	✓ 1.25	✓ 1.25	✗ 0.00	✓ 1.25	✗ 0.00	✗ 0.00	✗ 0.00
AG	Alan Bernardo Garcia Escobar Revisión del intento	alan.garcia.escobar@estudiante.uacm.edu.mx	Terminados	2 de octubre de 2024 16:48	2 de octubre de 2024 16:51	2 mins 31 segundos	5.00	✓ 1.25	✓ 1.25	✗ 0.00	✗ 0.00	✓ 1.25	✗ 0.00	✓ 1.25	✗ 0.00
MA	María del Carmen Alvarez Herrera Revisión del intento	maria.alvarez.herrera@alumnos.uacm.edu.mx	Terminados	2 de octubre de 2024 16:48	2 de octubre de 2024 16:50	2 mins 6 segundos	2.50	✗ 0.00	✗ 0.00	✗ 0.00	✓ 1.25	✗ 0.00	✗ 0.00	✓ 1.25	✗ 0.00
AA	Angeles Aguilar Ramirez Revisión del intento	angeles.aguilar@estudiante.uacm.edu.mx	Terminados	2 de octubre de 2024 16:49	2 de octubre de 2024 16:51	2 mins 21 segundos	7.50	✗ 0.00	✓ 1.25	✓ 1.25	✗ 0.00	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25
JM	José Luis Mata Ledezma Revisión del intento	jose.mata.ledezma@alumnos.uacm.edu.mx	Terminados	2 de octubre de 2024 16:49	2 de octubre de 2024 16:51	2 mins 16 segundos	5.00	✗ 0.00	✗ 0.00	✗ 0.00	✗ 0.00	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25
	Promedio general						5.00 (6)	0.42 (6)	0.63 (6)	0.42 (6)	0.42 (6)	1.04 (6)	0.42 (6)	1.04 (6)	0.63 (6)

Volver a calificar los intentos seleccionados | Eliminar los intentos seleccionados

Figura 9.2: Resultados de la evaluación diagnostica.

De acuerdo con la evidencia anterior, se observa que las preguntas con menor promedio de respuestas correctas (0.42) fueron:

- Blockchain es un sistema centralizado donde una entidad controla toda la información. La respuesta correcta es: Falso
- ¿Qué atributo garantiza la inmutabilidad en Blockchain? La respuesta correcta es: El hash de los bloques
- El concepto de Blockchain fue introducido por Bitcoin en 1991. La respuesta apropiada es 'Falso
- El minado en Blockchain consume grandes cantidades de energía. La respuesta apropiada es 'Verdadero

Por el contrario, las preguntas con mayor promedio de respuestas correctas (1.04) fueron:

- ¿Cuál es la función principal de los mineros en Blockchain? La respuesta correcta es: Validar transacciones y agregar bloques a la cadena
- Blockchain solo puede utilizarse en el sector financiero. La respuesta apropiada es 'Falso

A continuación se adjunta una gráfica mostrando los rangos de calificación:

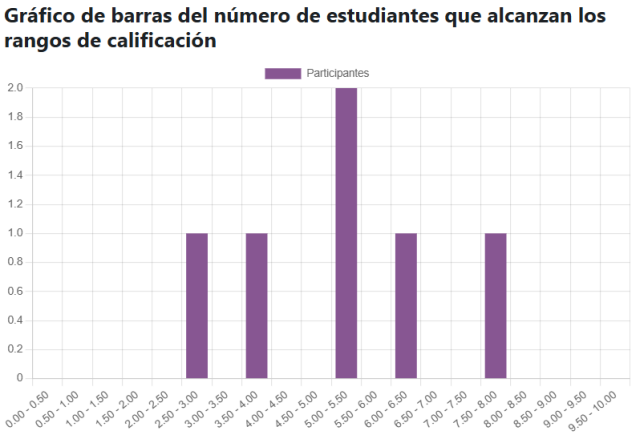
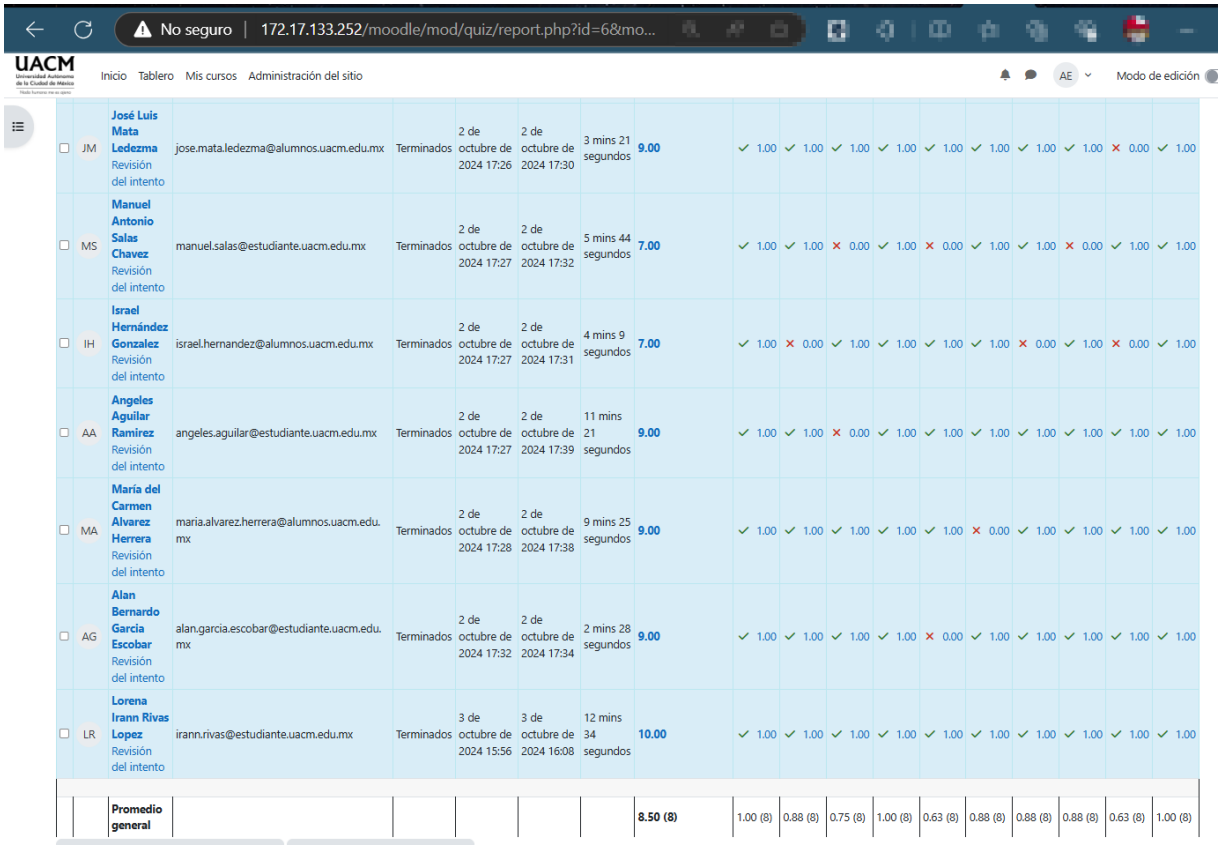


Figura 9.3: Gráfico de barras de los rangos de calificación de la evaluación diagnostica

9.2. Actividades realizadas en el módulo 1: Introducción a Blockchain

A continuación se comparte la evidencia de los estudiantes del primer reto:



	JM	José Luis Mata Ledezma Revisión del intento	jose.mata.ledezma@alumnos.uacm.edu.mx	Terminados	2 de octubre de 2024 17:26	2 de octubre de 2024 17:30	3 mins 21 segundos	9.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00
	MS	Manuel Antonio Salas Chavez Revisión del intento	manuel.salas@estudiante.uacm.edu.mx	Terminados	2 de octubre de 2024 17:27	2 de octubre de 2024 17:32	5 mins 44 segundos	7.00	✓ 1.00	✓ 1.00	✗ 0.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00
	IH	Israel Hernández Gonzalez Revisión del intento	israel.hernandez@alumnos.uacm.edu.mx	Terminados	2 de octubre de 2024 17:27	2 de octubre de 2024 17:31	4 mins 9 segundos	7.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✗ 0.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00
	AA	Angeles Aguilar Ramirez Revisión del intento	angeles.aguilar@estudiante.uacm.edu.mx	Terminados	2 de octubre de 2024 17:27	2 de octubre de 2024 17:39	11 mins 21 segundos	9.00	✓ 1.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00
	MA	María del Carmen Alvarez Herrera Revisión del intento	maria.alvarez.herrera@alumnos.uacm.edu.mx	Terminados	2 de octubre de 2024 17:28	2 de octubre de 2024 17:38	9 mins 25 segundos	9.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00
	AG	Alan Bernardo Garcia Escobar Revisión del intento	alan.garcia.escobar@estudiante.uacm.edu.mx	Terminados	2 de octubre de 2024 17:32	2 de octubre de 2024 17:34	2 mins 28 segundos	9.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✗ 0.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00
	LR	Lorena Irann Rivas Lopez Revisión del intento	irann.rivas@estudiante.uacm.edu.mx	Terminados	3 de octubre de 2024 15:56	3 de octubre de 2024 16:08	12 mins 34 segundos	10.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00	✓ 1.00
		Promedio general						8.50 (8)	1.00 (8)	0.88 (8)	0.75 (8)	1.00 (8)	0.63 (8)	0.88 (8)	0.88 (8)	0.88 (8)	0.63 (8)	1.00 (8)									

Figura 9.4: Resultados de la evaluación del reto 1 primer módulo.

De acuerdo con la evidencia anterior, se observa que las preguntas con menor promedio de respuestas correctas (0.63) fueron:

- ¿Qué sucede cada vez que se realiza una transacción en Blockchain? La respuesta correcta es: El registro se actualiza automáticamente en todos los nodos.

- ¿Qué significa que una transacción sea verificada? La respuesta correcta es: Que la transacción puede involucrar criptomoneda y otras señales digitales.

Por el contrario, las preguntas con mayor promedio de respuestas correctas (1.00) fueron:

- ¿Qué es Blockchain? La respuesta correcta es: Una tecnología de registro distribuido
- ¿Cómo se describe la base de datos de Blockchain? La respuesta correcta es: Una base de datos distribuida y segura criptográficamente.
- ¿Qué ocurre después de que un nuevo bloque es verificado? La respuesta correcta es: El bloque se combina con otras transacciones para crear un nuevo bloque de datos.

A continuación se adjunta una gráfica mostrando los rangos de calificación:

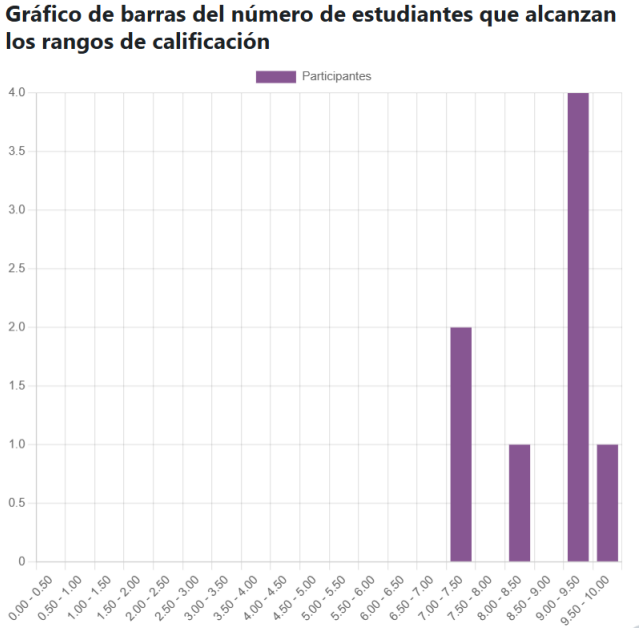


Figura 9.5: Gráfico de barras de los rangos de calificación de la evaluación del reto 1 primer módulo

A continuación se comparte la evidencia de los estudiantes del segundo y tercer reto:

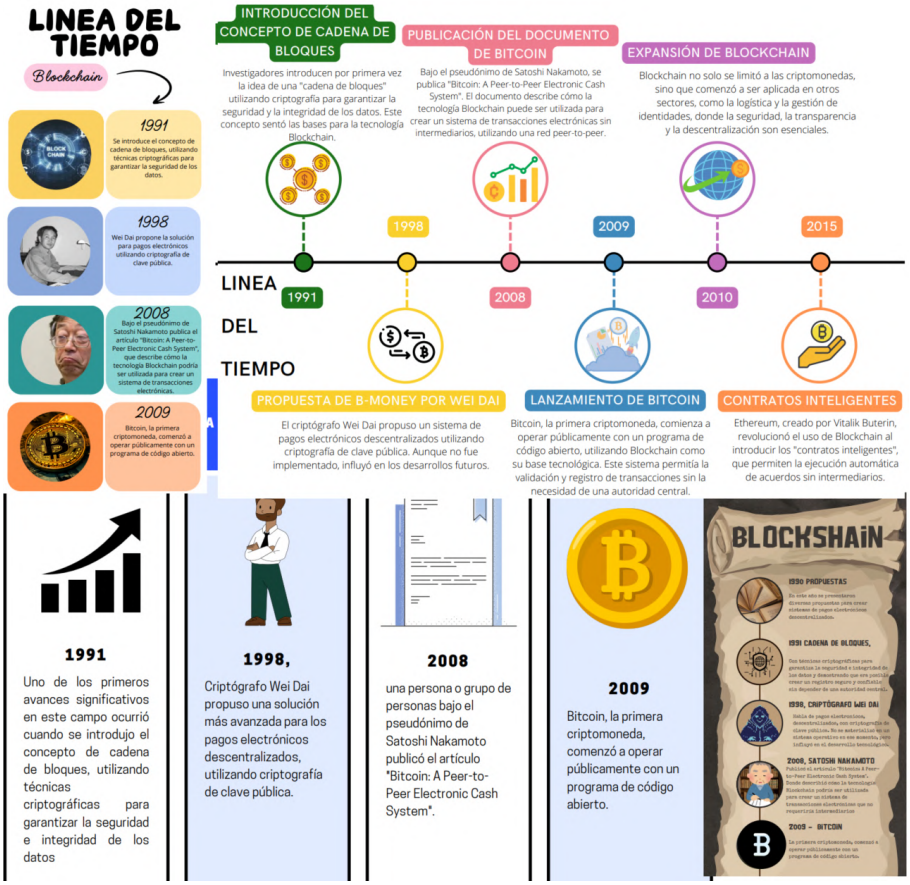


Figura 9.6: Líneas del tiempo del reto 2 primer módulo.

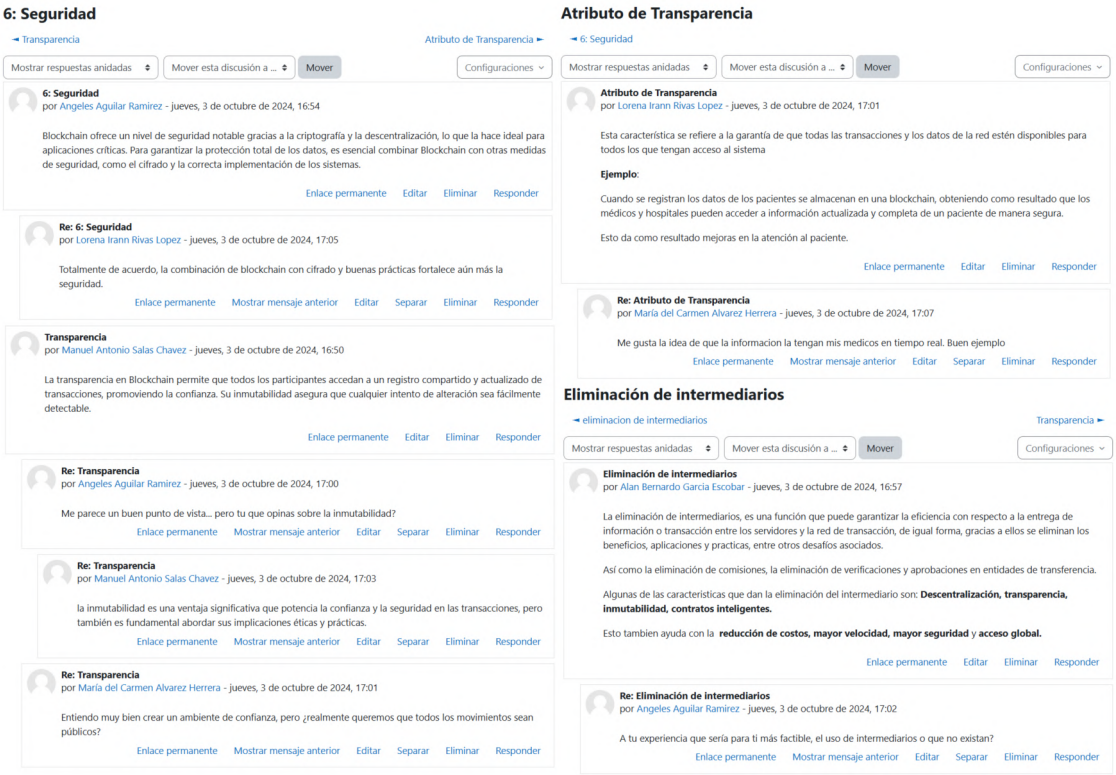


Figura 9.7: Publicaciones y comentarios del foro de discusión y opinión personal.

9.3. Actividades realizadas en el módulo 2: Fundamentos de la Criptografía en Blockchain

A continuación se comparten los datos de la evaluación del primer reto:

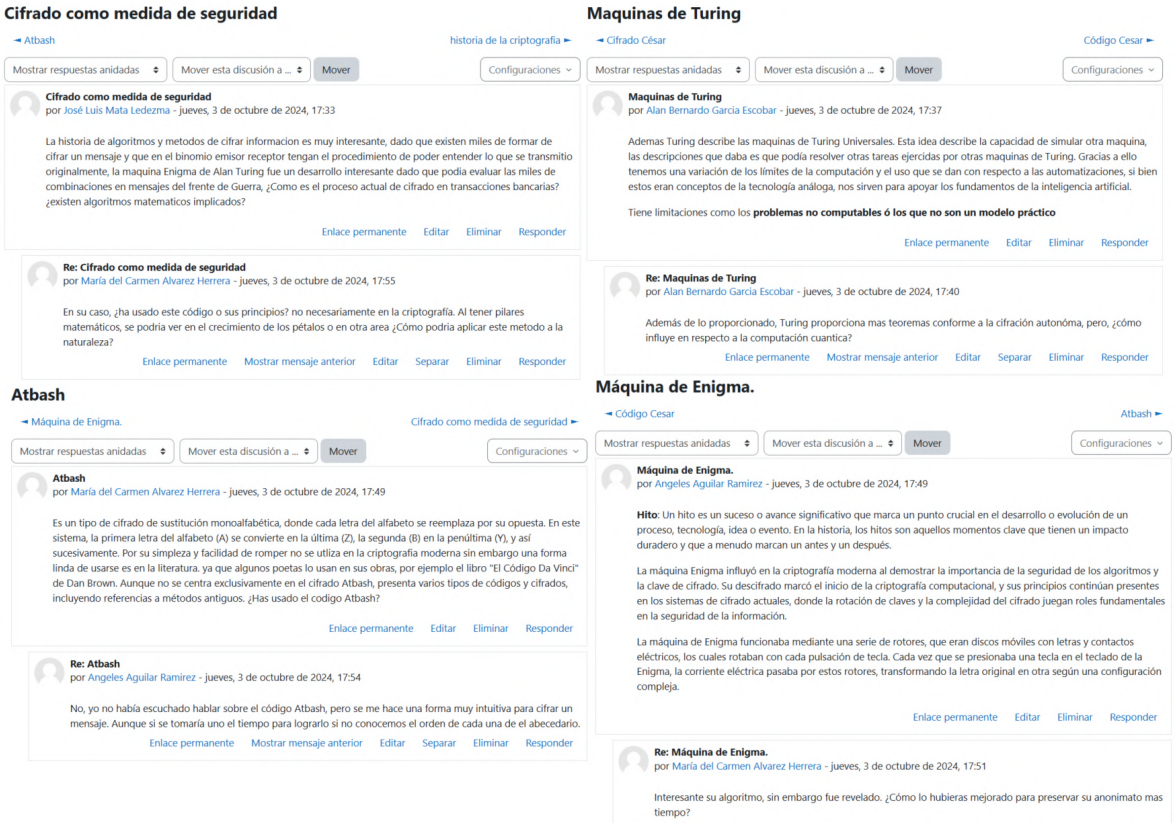


Figura 9.8: Publicaciones y comentarios del foro de discusión fundamentos de la criptografía.

A continuación se comparten los datos de la evaluación del segundo reto:

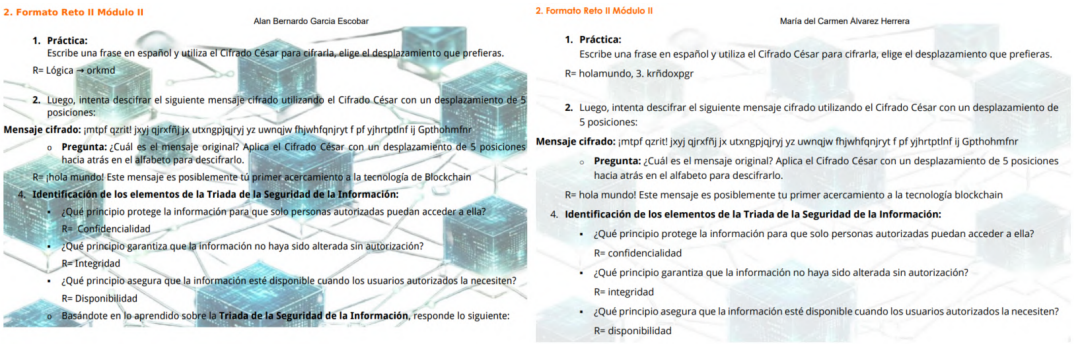
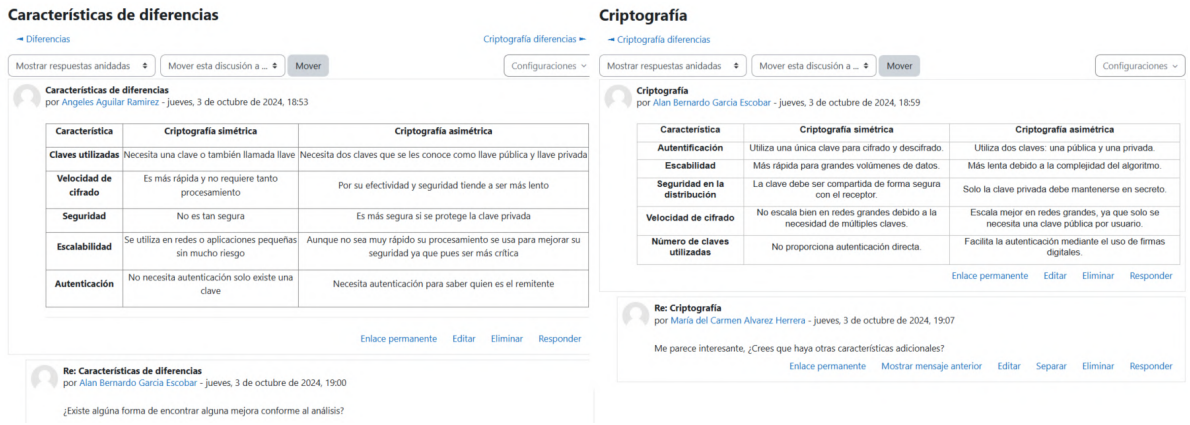


Figura 9.9: Evidencias de la actividad aplicación de conceptos básicos de criptografía.

A continuación se comparten los datos de la evaluación del tercer reto:



Características de diferencias

→ Diferencias

Criptografía diferencias ►

Mostrar respuestas anidadas | Mover esta discusión a ... | Mover | Configuraciones

Características de diferencias
por Angeles Aguilar Ramirez - jueves, 3 de octubre de 2024, 18:53

Característica	Criptografía simétrica	Criptografía asimétrica
Claves utilizadas	Necesita una clave o también llamada llave	Necesita dos claves que se les conoce como llave pública y llave privada
Velocidad de cifrado	Es más rápida y no requiere tanto procesamiento	Por su efectividad y seguridad tiende a ser más lento
Seguridad	No es tan segura	Es más segura si se protege la clave privada
Escalabilidad	Se utiliza en redes o aplicaciones pequeñas sin mucho riesgo	Aunque no sea muy rápido su procesamiento se usa para mejorar su seguridad ya que pues ser más crítica
Autenticación	No necesita autenticación solo existe una clave	Necesita autenticación para saber quien es el remitente

Enlace permanente Editar Eliminar Responder

Re: Características de diferencias
por Alan Bernardo Garcia Escobar - jueves, 3 de octubre de 2024, 19:00

¿Existe algúna forma de encontrar alguna mejora conforme al análisis?

Criptografía

→ Criptografía diferencias

Mostrar respuestas anidadas | Mover esta discusión a ... | Mover | Configuraciones

Criptografía
por Alan Bernardo Garcia Escobar - jueves, 3 de octubre de 2024, 18:59

Característica	Criptografía simétrica	Criptografía asimétrica
Autentificación	Utiliza una única clave para cifrado y descifrado.	Utiliza dos claves: una pública y una privada.
Escabilidad	Más rápida para grandes volúmenes de datos.	Más lenta debido a la complejidad del algoritmo.
Seguridad en la distribución	La clave debe ser compartida de forma segura con el receptor.	Solo la clave privada debe mantenerse en secreto.
Velocidad de cifrado	No escala bien en redes grandes debido a la necesidad de múltiples claves.	Escala mejor en redes grandes, ya que solo se necesita una clave pública por usuario.
Número de claves utilizadas	No proporciona autenticación directa.	Facilita la autenticación mediante el uso de firmas digitales.

Enlace permanente Editar Eliminar Responder

Re: Criptografía
por María del Carmen Alvarez Herrera - jueves, 3 de octubre de 2024, 19:07

Me parece interesante, ¿Crees que haya otras características adicionales?

Enlace permanente Mostrar mensaje anterior Editar Separar Eliminar Responder

Figura 9.10: Publicaciones y comentarios del foro de comparación de criptosistemas simétricos y asimétricos.

9.4. Actividades realizadas en el módulo 3: Conceptos básicos de Blockchain

A continuación se comparten los datos de la evaluación del segundo, tercer y cuarto reto:

Reflexión: Los **hashes** juegan un papel fundamental en el funcionamiento de la cadena de bloques, ya que son la herramienta clave para garantizar la **integridad de los datos**. Un hash es una función criptográfica que transforma cualquier bloque de información en una cadena de caracteres de longitud fija. Lo más importante es que cualquier pequeño cambio en los datos originales genera un hash completamente diferente, lo que permite detectar incluso la más mínima alteración.

Angeles Aguilar Ramirez

Bloque

Bloque

Bloque

Bloque

Manuel Antonio Salas Chavez

Bloque : 1

Nonce antes de minar : 72608

Nonce después de minar : 136155

Datos : Hello, My name is Antonio, My nickname is Antoni

Hash después de minar : 0000161e893217a1ca5293143f359daec3362088c2c3977eae86340712c

Hash antes de minar : 0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e

El análisis de blockchain experimental muestra su potencial para transformar interacciones y transacciones mediante registros transparentes e inmutables, fomentando la confianza en entornos inciertos. Su verdadero valor radica en empoderar a las personas y democratizar el acceso a la información.

Ejemplo de Actividad Completada:

Número del Bloque:

- Bloque #1

Nonce:

- Nonce antes de minar: 72608
- Nonce después de minar: 83452

Datos:

- Datos ingresados: "Ejemplo de transacción"
- Hash antes de minar: 4f2b8d123...
- Hash después de minar: 0000babc54...

Reflexión Final:

- Me sorprendió ver cómo el proceso de minado requiere probar muchos Nonces diferentes para encontrar uno que genere un hash válido. Esto me ayudó a entender la importancia del Nonce en la validación de un bloque, y cómo los mineros compiten para ser los primeros en encontrar el valor correcto. Además, cualquier cambio en los datos altera completamente el hash, lo que asegura que los datos en el bloque no puedan ser modificados sin invalidar el bloque completo.

UACM

Elaboró: Alan García Escobar

Bloque

Figura 9.11: Evidencia de la actividad comprender los elementos de un bloque y el proceso de minado.

Figura 9.12: Evidencia de la actividad simulación de la cadena de bloques y análisis de cambios en los hashes.

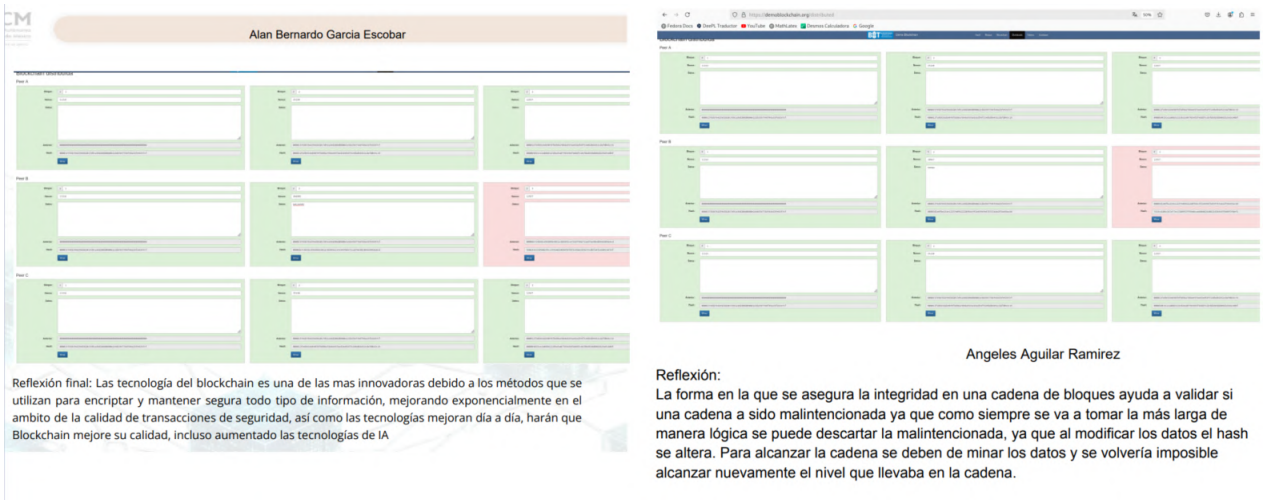


Figura 9.13: Evidencia de la actividad simulación de Blockchain distribuido.

9.5. Calificaciones obtenidas por los estudiantes

En esta sección se presentan las calificaciones de los estudiantes en los tres módulos, las cuales se basaron en las rúbricas de evaluación. Es importante mencionar que, debido a limitaciones de tiempo, no fue posible completar todos los retos. Además, al contar con estudiantes de diversas carreras, surgieron problemas de disponibilidad, ya que algunos tenían clases en el mismo horario del curso. Por ello, se implementaron y evaluaron tres retos por módulo, cada uno con un valor del 33 % en la evaluación final. A pesar de que la participación de los estudiantes fue variable, se identificaron características interesantes en su desempeño.

9.5.1. Calificaciones del módulo 1

Las calificaciones obtenidas en este módulo se muestran en la siguiente tabla:

Módulo 1				
Estudiantes	**Reto I**	**Reto II**	**Reto III**	**Promedio**
Aguilar Ramirez Angeles	150	200	200	9.9
Alvarez Herrera María del Carmen	150	200	200	9.9
Garcia Escobar Alan Bernardo	150	190	140	8.7
Hernández Gonzalez Israel	120	N/A	120	4.6
Mata Ledezma José Luis	150	N/A	160	6.0
Rivas Lopez Lorena Irann	150	170	200	9.4
Salas Chavez Manuel Antonio	120	N/A	190	5.7

Cuadro 9.1: Calificaciones pertenecientes al primer módulo

De acuerdo con las rúbricas de evaluación se evaluó a los estudiantes con un máximo de 150 puntos en el reto 1 y sobre 200 en los retos II y III.

Durante la evaluación se tuvieron las siguientes observaciones:

- Las líneas del tiempo tuvieron buena precisión en la secuenciación de los eventos de Blockchain, creatividad y claridad sobre el tema.
- Se tiene buena calidad en la discusión y comentarios del foro, se observó buena participación de algunos estudiantes realizando preguntas y dando puntos de vista sobre los atributos clave de Blockchain.
- Algunos estudiantes deben mejorar su redacción para interactuar.

9.5.2. Calificaciones del módulo 2

Las calificaciones obtenidas en este módulo se muestran en la siguiente tabla:

Módulo 2				
Estudiantes	**Reto I**	**Reto II**	**Reto III**	**Promedio**
Aguilar Ramirez Angeles	250	240	220	9.4
Alvarez Herrera María del Carmen	250	240	210	9.2
Garcia Escobar Alan Bernardo	240	250	240	9.6
Hernández Gonzalez Israel	100	N/A	N/A	1.3
Mata Ledezma José Luis	180	N/A	N/A	2.4
Rivas Lopez Lorena Irann	190	250	200	8.4
Salas Chavez Manuel Antonio	220	N/A	N/A	2.9

Cuadro 9.2: Calificaciones pertenecientes al segundo módulo

De acuerdo con las rúbricas de evaluación se evaluó a los estudiantes con un máximo de 250 puntos en los retos I, II y III.

Durante la evaluación se tuvieron las siguientes observaciones:

- En el foro fundamentos de la criptografía se realizaron buenos análisis del hito seleccionado y se relacionó de manera correcta a la criptografía moderna. Sin embargo, se observó la falta de participación en la discusión por algunos estudiantes.
- Se observa una buena comprensión en el cifrado de César y la triada de la seguridad.
- En el foro de comparación de criptografía simétrica y asimétrica se identifica claridad y coherencia, sin embargo se notó un poco de ausencia en la participación del foro.

9.5.3. Calificaciones del módulo 3

En esta sección se muestran las calificaciones de los estudiantes en el tercer módulo las cuales se basaron en las rúbricas de evaluación. De los cuatro retos planteados se evaluaron los tres últimos.

Módulo 3				
Estudiantes	**Reto II**	**Reto III**	**Reto IV**	**Promedio**
Aguilar Ramirez Angeles	140	100	150	8.6
Alvarez Herrera María del Carmen	110	110	110	7.3
Garcia Escobar Alan Bernardo	150	150	150	9.9
Hernández Gonzalez Israel	N/A	N/A	N/A	N/A
Mata Ledezma José Luis	N/A	N/A	N/A	N/A
Rivas Lopez Lorena Irann	N/A	N/A	N/A	N/A
Salas Chavez Manuel Antonio	90	130	130	7.7

Cuadro 9.3: Calificaciones pertenecientes al tercer módulo

De acuerdo con las rúbricas de evaluación se evaluó a los estudiantes con un máximo de 150 puntos en los retos II, III y IV.

Durante la evaluación se tuvieron las siguientes observaciones:

- Para las tres actividades se encontraron reflexiones interesantes por parte de algunos estudiantes. Demostrando su completa comprensión y conocimiento de los temas; elemento de un bloque y minería, simulación cadena de bloques y análisis de cambio en hashes, así como en la simulación de Blockchain distribuida.
- Se recomienda mejorar la presentación respecto a las evidencias ya que no se tenía un orden en sus documentos, y algunos casos dejaron la evidencia incompleta.

9.6. Evaluación final

A continuación se comparten los datos de la evaluación final:

		Nombre / Apellido(s)	Dirección Email	Estado	Iniciado	Finalizado	Duración	Calificación/10.00	Q. 1 /1.25	Q. 2 /1.25	Q. 3 /1.25	Q. 4 /1.25	Q. 5 /1.25	Q. 6 /1.25	Q. 7 /1.25	Q. 8 /1.25
☐	AA	**Angeles Aguilar Ramirez** Revisión del intento	angeles.aguilar@estudiante.uacm.edu.mx	Terminados	4 de octubre de 2024 17:57	4 de octubre de 2024 18:00	2 mins 17 segundos	**10.00**	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25
☐	MS	**Manuel Antonio Salas Chavez** Revisión del intento	manuel.salas@estudiante.uacm.edu.mx	Terminados	4 de octubre de 2024 17:59	4 de octubre de 2024 18:04	4 mins 47 segundos	**7.50**	✓ 1.25	✓ 1.25	✓ 1.25	✗ 0.00	✓ 1.25	✓ 1.25	✓ 1.25	✗ 0.00
☐	MA	**María del Carmen Alvarez Herrera** Revisión del intento	maria.alvarez.herrera@alumnos.uacm.edu.mx	Terminados	4 de octubre de 2024 18:01	4 de octubre de 2024 18:02	1 min 54 segundos	**8.75**	✓ 1.25	✓ 1.25	✗ 0.00	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25
☐	AG	**Alan Bernardo Garcia Escobar** Revisión del intento	alan.garcia.escobar@estudiante.uacm.edu.mx	Terminados	4 de octubre de 2024 18:13	4 de octubre de 2024 18:14	1 min 15 segundos	**10.00**	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25	✓ 1.25
		Promedio general						**9.06 (4)**	1.25 (4)	1.25 (4)	0.94 (4)	0.94 (4)	1.25 (4)	1.25 (4)	1.25 (4)	0.94 (4)

Figura 9.14: Resultados de la evaluación final.

De acuerdo con la evidencia anterior, se observa que las preguntas con menor promedio de respuestas correctas (0.94) fueron:

- ¿Qué asegura la integridad de los datos en Blockchain? La respuesta correcta es: Funciones hash
- El concepto de Blockchain fue introducido por Bitcoin en 1991. La respuesta apropiada es 'Falso'.
- El proceso de hashing es reversible en Blockchain. La respuesta apropiada es 'Falso'.

Por el contrario, las preguntas con mayor promedio de respuestas correctas (1.25) fueron:

- Blockchain es un sistema centralizado donde una entidad controla toda la información. La respuesta apropiada es 'Falso'.
- ¿Qué atributo garantiza la inmutabilidad en Blockchain? La respuesta correcta es: El hash de los bloques.
- ¿Cuál es la función principal de los mineros en Blockchain? La respuesta correcta es: Validar transacciones y agregar bloques a la cadena.
- El minado en Blockchain consume grandes cantidades de energía. La respuesta apropiada es 'Verdadero'.
- Blockchain solo puede utilizarse en el sector financiero. La respuesta apropiada es 'Falso'.

A continuación se adjunta una gráfica mostrando los rangos de calificación:

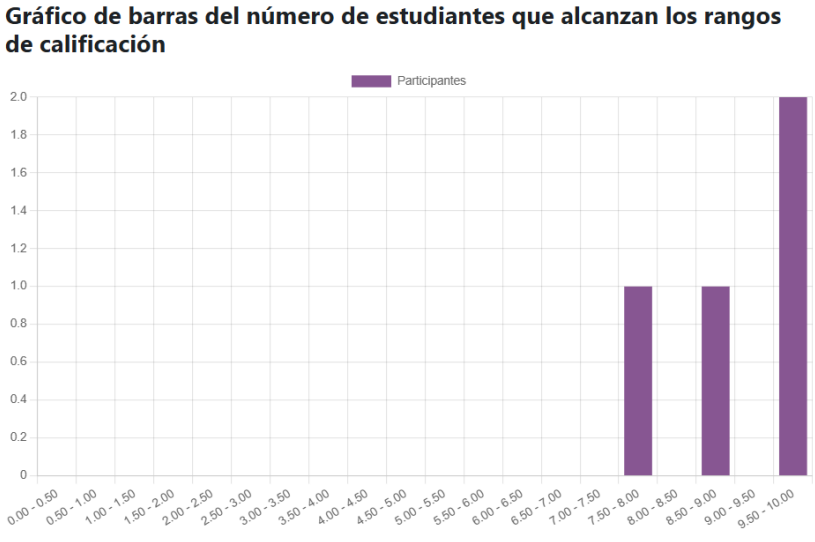


Figura 9.15: Gráfico de barras de los rangos de calificación de la evaluación final

9.7. Retroalimentación de los estudiantes

A continuación, se adjunta evidencia de la retroalimentación recibida por los estudiantes al finalizar el curso:

Respuesta número	¿Cómo calificarías tu experiencia en general?	¿Cual es tu opinión sobre explicarle a los estudiantes el método de la evaluación mediante Rúbricas?	En un rango del 1 al 10 ¿Cuánto consideras que aprendiste en este curso?	¿Cuál es el módulo que te pareció más interesante?	¿Qué mejoras sugerirías para optimizar nuestro curso?	El curso me pareció ...	¿Te gustaría ver más opciones o características de Blockchain en el futuro?	¿Cómo calificarías la disponibilidad y efectividad del instructor para resolver dudas?
1	Excelente	Excelente, solo se más expresivo :p	10	Módulo 2: Fundamentos de la Criptografía en Blockchain	NO des mucho tiempo para los ejerecicios	Regular	Sii	Excelente
2	Buena	Me resulto secilla, sin embargo hay terminos que deconocia. Por lo cual preguntab y me senti en la libertad de seguir haciendolo cuando mis preguntas erna validadas y no ignoradas	7	Módulo 2: Fundamentos de la Criptografía en Blockchain	Ejercicios practicos es decir algo que pueda usar yendome despues de la clase.	Fácil	Si me gustaria, en un nivel que comprandamos mas personas como personas mayores o con discapacidades	Excelente
3	Buena	Perfecta pero puede mejorar	8	Módulo 1: Introducción a Blockchain		Regular	Estaría	Excelente
4	Buena	Tiene buen manejo de la información y tiene claros los conceptos.	9	Módulo 3: Conceptos básicos de Blockchain	El tiempo fué muy poco y necesitaría más ejercicios y prácticas para tener mejor dominio del tema	Regular	Sería interesante.	Excelente

Figura 9.16: Retroalimentación final por parte de los estudiantes.

A lo largo de la impartición del curso se presentaron diversas dudas sobre el tema de Blockchain, las cuales se abordaron y aclararon. Se explicó a detalle cada capítulo y se dejaron claras los objetivos y las actividades. Se explicaron los componentes fundamentales y funcionamiento de la tecnología Blockchain. Se elaboraron materiales conforme a especificaciones de una cadena de bloques donde se comprendió la transparencia y descentralización en las tecnologías digitales.

Uno de los inconvenientes que se presentaron a lo largo del curso fue la falta de tiempo. Algunos compañeros tenían clases que les impedían continuar con el curso, y otros se presentaron un día después, lo que dificultó su evaluación en comparación con el resto del grupo. Cabe destacar que, entre las actividades que no se pudieron llevar a cabo, se encontraba la programación en Python; por ello, se compartió el código y un manual con los estudiantes interesados. De lo anterior mencionado, es fundamental establecer un horario y un espacio fijo que permitan a los estudiantes interactuar de manera efectiva en el curso, en donde se plantee un horario y tiempo específico para cada módulo. Asimismo, se tendrán en cuenta sus opiniones y comentarios como retroalimentación final para la mejora del curso. Este enfoque reflexivo no solo enriquece la investigación, sino que también contribuye al desarrollo de un entorno educativo más robusto y adaptable a las necesidades de los estudiantes.

Conclusiones

El objetivo de esta tesis fue implementar un aula virtual de aprendizaje sobre Blockchain para los estudiantes de la Universidad Autónoma de la Ciudad de México (UACM). En este contexto, se definieron aspectos fundamentales sobre cómo funciona esta tecnología, sus características, tipos y diversas implementaciones. Para alcanzar este objetivo, fue necesario llevar a cabo una extensa investigación teórica que abarcó los conceptos básicos de Blockchain, su funcionamiento, y su aplicación en la criptografía a través de diferentes sectores tecnológicos. La información fue recopilada de diversas fuentes, empleando una amplia variedad de autores reconocidos en el campo.

Este proceso de investigación nos permitió adaptar y desarrollar los conceptos clave necesarios para la implementación del aula virtual. Gracias a este enfoque, se logró cumplir con los objetivos específicos de la tesis, que incluyeron la comprensión de la historia y la evolución de la tecnología Blockchain desde su creación, así como su impacto en diversos sectores. Se profundizó en los principios de la criptografía que sustentan la seguridad en Blockchain, reconociéndola como un pilar esencial para generar confianza y asegurar la integridad de la información. Asimismo, se discutieron acontecimientos históricos relevantes y se exploraron técnicas a través de ejercicios prácticos en plataformas de simulación.

Durante el proceso de implementación, se optó por utilizar tecnologías de software libre, lo que no solo garantizó el acceso a herramientas robustas y eficientes para las aulas virtuales, sino que también promovió la flexibilidad y la personalización de los entornos de aprendizaje. El software libre ofrece una serie de ventajas significativas: en primer lugar, su naturaleza abierta permite a los educadores y administradores adaptar las plataformas a las necesidades específicas de sus estudiantes, facilitando la creación de un entorno de aprendizaje más inclusivo y accesible. Además, al no estar sujetos a costos de licencias, las instituciones pueden invertir recursos en otras áreas críticas, como la capacitación docente y la mejora de infraestructuras. Asimismo, el uso de software libre fomenta una comunidad activa de usuarios y desarrolladores, lo que se traduce en actualizaciones constantes, soporte colaborativo y una variedad de recursos educativos disponibles. En otras palabras, la implementación de tecnologías de software libre en las aulas virtuales no solo contribuyó a la creación de entornos educativos robustos, sino que también promovió un enfoque más colaborativo y sostenible en la educación.

Aunque esta tesis se centró exclusivamente en los estudiantes de la UACM dentro del laboratorio LACECI, no se descarta la posibilidad de extender su implementación a toda la universidad o incluso trabajar de manera colaborativa a través de la nube. Durante la implementación del aula virtual, se observó un notable interés por parte de varios estudiantes, lo que indica una buena receptividad hacia el contenido. Además, el aula se estructuró de acuerdo con el estándar EC 217.01, lo que podría facilitar el desarrollo de futuros proyectos similares dentro de la universidad. Se espera que esta tesis no solo sirva como una herramienta útil, sino que también contribuya a la implementación de proyectos relacionados con Blockchain y aulas virtuales. Con ediciones futuras, se espera poder abordar dudas y realizar un seguimiento efectivo mediante el uso de Inteligencias Artificiales.

En la UACM, existe una oportunidad real para que Blockchain prospere y se aplique de manera innovadora. Por ejemplo, la universidad podría desarrollar un sistema en línea capaz de emitir certifica-

dos que sean inalterables y que no dependan de los procesos tradicionales. Esto no solo garantizaría la autenticidad de los documentos, sino que también reduciría el riesgo de fraude académico. Asimismo, el mismo enfoque podría aplicarse a la asignación de calificaciones y a las inscripciones semestrales de los estudiantes. Imaginemos un sistema donde las calificaciones se registren de manera transparente y segura, permitiendo a los estudiantes y docentes acceder a la información en tiempo real y con total confianza. Las posibilidades son inmensas, abriendo la puerta a una administración más eficiente y a un aprendizaje más accesible. Todo esto dependerá del potencial y la imaginación de las siguientes generaciones.

Esta tesis representa solo el comienzo de una serie de iniciativas que pueden ser adoptadas en diversas instituciones educativas. Blockchain, al igual que cualquier otra tecnología emergente, puede parecer disruptiva o incluso amenazante en sus inicios; sin embargo, con el tiempo tiene el potencial de impulsar el desarrollo de un ecosistema vasto que integre tanto innovaciones nuevas como las ya establecidas. Aún quedan interrogantes relevantes que deben ser consideradas: ¿Podría Blockchain dar lugar al surgimiento de nuevos gigantes tecnológicos, al igual que lo hicieron Google o Microsoft? ¿Cómo abordarán los gobiernos estas transformaciones? ¿Será imprescindible integrar conocimientos sobre Blockchain en los planes de estudio de las universidades? Estas preguntas son complejas y difíciles de responder, pero es innegable que el futuro de la educación y la administración académica podría verse transformado por esta tecnología. Lamentablemente, existe la posibilidad de que los gobiernos en todo el mundo se sientan amenazados si la tecnología continúa prosperando, lo que podría llevarles a implementar medidas que dificulten su crecimiento. Sin embargo, todo esto se encuentra en el ámbito de la especulación. Lo cierto es que Blockchain ya ha dejado una marca indeleble en la historia de la tecnología, y su evolución futura seguirá siendo un tema de interés y debate.

Para concluir, quiero enfatizar el mensaje central de esta tesis: es crucial que los futuros líderes y educadores reconozcan las herramientas a su disposición y comprendan cómo utilizarlas para fomentar un entorno educativo más dinámico y resiliente. La integración de Blockchain y Aulas Virtuales basadas en software libre no es simplemente una opción, sino una necesidad imperante que podría definir el futuro de las instituciones académicas. Al adoptar estas tecnologías, se abre la puerta a una educación más accesible, transparente y adaptable a las necesidades de las nuevas generaciones.

Apéndice A

Modelo teórico matemático para la generación de hash de 256 bits.

En este apartado se mostrará mediante un diagrama de flujo cómo se genera un hash de tipo SHA256 a partir de una palabra cualquiera. Cabe aclarar que los pasos son demasiado extensos por lo que se tratará de ser lo más breve posible. Para dar comienzo a este concepto se van a dar algunos conceptos clave que serán de mucha importancia para la comprensión del tema que se aborda en esta tésis.

A.1. Funciones y operaciones básicas

A.1.1. Tablas de verdad

Lo primero que se va a definir serán las siguientes tablas de verdad, las cuales nos permiten determinar cuando una proposición compuesta es verdadera, falsa o variada. algunas de estas tablas se muestran a continuación:

p	$\neg$ p
0	1
1	0

Cuadro A.1: Operador NOT $\neg$.

p	q	q Λ q
0	0	0
0	1	0
1	0	0
1	1	1

Cuadro A.2: Operador AND Λ .

p	q	q $\oplus$ q
0	0	0
0	1	1
1	0	1
1	1	0

Cuadro A.3: Operador XOR $\oplus$.

A.1.2. Números enteros de 32 bits

Un hash de 256 bits, está compuesto por 64 caracteres hexadecimales, lo que se divide en 8 valores decimales concatenados.

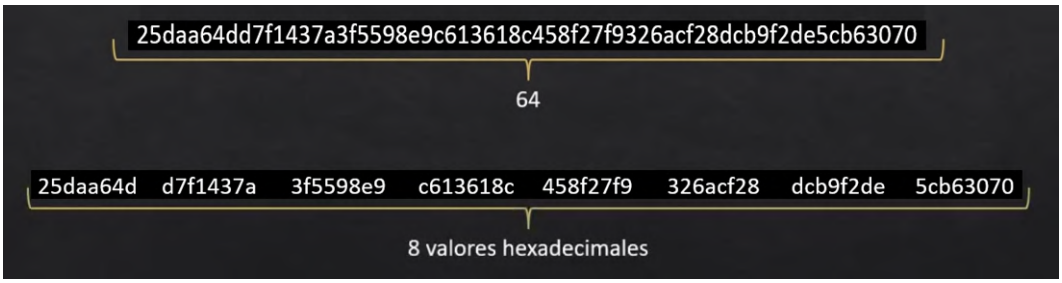


Figura A.1: Valores hexadecimales de un SHA-256.

Como sabemos que cada hash tiene 8 valores hexadecimales, se define que la concatenación de los valores binarios de 32 bits da como resultado una salida de 256 bits, tal y como se muestra en la siguiente figura:

Hexadecimal	Entero	Binario	Bits
25daa64d	635086413	00100101110110101010011001001101	32
d7f1437a	3622912890	11010111111100010100001101111010	32
3f5598e9	1062574313	00111111010101011001100011101001	32
c613618c	3323158924	11000110000100110110000110001100	32
458f27f9	1167009785	01000101100011110010011111111001	32
326acf28	845860648	00110010011010101100111100101000	32
dcb9f2de	3703173854	11011100101110011111001011011110	32
5cb63070	1555443824	01011100101101100011000001110000	32

Figura A.2: Concatenación de valores de un SHA-256.

Para esta parte, se va a definir el rango de valores decimales que abarcan los 32 bits en binario. Por lo tanto, vamos a definir a un número entero sin signo como un dato de 32 bits que codifica un entero no negativo en el rango de [0 a $2^{32} - 1 = 4,294,967,295$]. Dicho rango se expresa a detalle en la siguiente figura:

Hexadecimal	Entero	Binario	Bits
0	0	00000000000000000000000000000000	32
FFFFFFFF	4294967295	11111111111111111111111111111111	32

Figura A.3: Entero sin signo de 32 bits.

En otras palabras, un número entero que representa 32 bits se define como aquellos números enteros que se encuentran entre el 0 y el resultado de $2^{32} - 1$. Cabe destacar que este valor -1 es muy importante, ya que de no realizar la resta, se estaría superando el número de bits, resultando en un valor de 33 bits.

A.1.3. Operación módulo

La operación módulo no es más que el residuo r de la divisón de dos números enteros, llamése A el dividendo y B el divisor. Obteniendo la siguiente expresión matemática:

$$r = A \bmod B$$

Por ejemplo, si quiseramos calcular el módulo con los valores $A = 35$ y $B = 8$ se tendría lo siguiente:

$$r = 35 \bmod 8 = 3$$

$$\begin{array}{r} 4 \\ 8\overline{)35} \\ \underline{32} \\ 3 \end{array}$$

Operador suma MOD 2^{32}

Ahora que se ha definido la operación módulo, vamos a definir una operación que será muy importante para la realización de un hash, Esta operación se encarga de añadir todos los elementos de un vector expresión que contiene una variable de rango. La fórmula resultante sería:

$$Operador\ (A+B)\ mod\ 2^{32}$$

Ejemplo, si se requiere sumar A= 2456913771 y B= 1948165048 el resultado sería;

$$(A + B)\ MOD\ 2^{32} = (2456913771 + 1948165048)\ MOD\ 2^{32}$$
$$(A + B)\ MOD\ 2^{32} = 4405078819\ MOD\ 2^{32}$$
$$(A + B)\ MOD\ 2^{32} = 4405078819\ MOD\ 4294967296 = 110111523$$

Una vez obtenido el resultado se convierte a binario, obteniendo lo siguiente:

$$110111523 \rightarrow 11010010000001010110010011$$

Cómo se requiere que el resultado sea de 32 bits se añaden ceros a la izquiera del primer bit obteniendo:

$$00000110100100000010101100100011$$

A.1.4. Funciones de desplazamiento

Función Right Rotate: $RotR(x, n)$

Esta función permite un desplazamiento desde un arreglo de 32 bits llámese x, y un número de desplazamientos n hacia la derecha. Cuando se desplace el último bit, este pasará a ser el primero en la siguiente rotación. Por ejemplo:

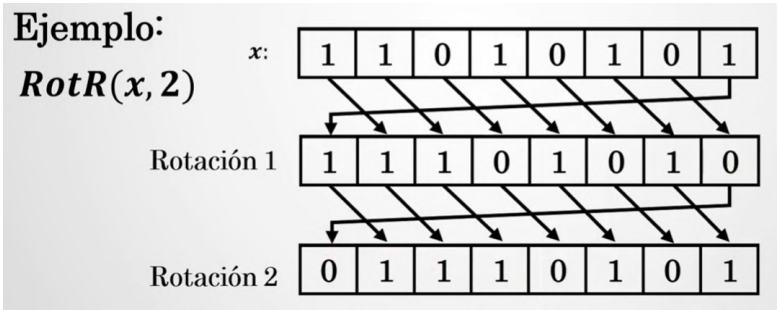


Figura A.4: Función Right Rotate con 2 desplazamientos.

Función Right Shift: $ShR(x, n)$

Esta función permite un desplazamiento desde un arreglo de 32 bits llámese x, y un número de desplazamientos n hacia la derecha. Sin embargo, el último bit desplazado será reemplazado por un cero. Por ejemplo:

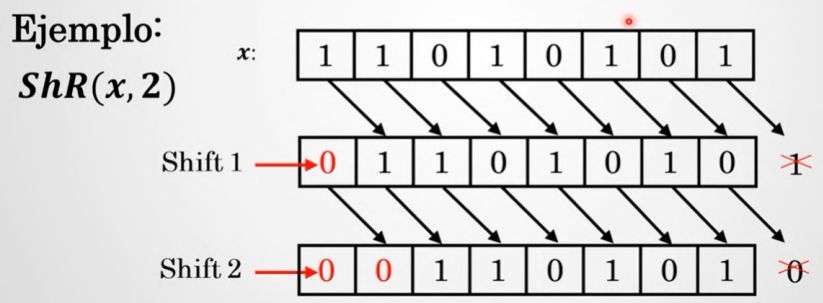


Figura A.5: Función Right Shift con 2 desplazamientos.

Ahora que se entiende cómo se emplean estas funciones se define el siguiente paso donde se emplean fórmular que emplean los conceptos básicos que ya se han definido.

Funciones para las palabras y la compresión.
En este apartado se definirán las funciones que serán utilizadas para la compresión de las palabras.

Función Choose:

$$Ch(x, y, z) = (x\Lambda y) \oplus (\neg x\Lambda z) \tag{A.1}$$

Función Majority:

$$Maj(x, y, z) = (x\Lambda y) \oplus (x\Lambda z) \oplus (y\Lambda z) \tag{A.2}$$

Función sigma $\sigma 0(x)$:

$$\sigma 0(x) = RotR(x, 7) \oplus RotR(x, 18) \oplus ShR(x, 3) \tag{A.3}$$

Función sigma $\sigma 1(x)$:

$$\sigma 1(x) = RotR(x, 17) \oplus RotR(x, 19) \oplus ShR(x, 10) \tag{A.4}$$

Función sumatoria $\sum 0(x)$:

$$\sum 0(x) = RotR(x, 2) \oplus RotR(x, 13) \oplus RotR(x, 22) \tag{A.5}$$

Función sumatoria $\sum 1(x)$:

$$\sum 1(x) = RotR(x, 6) \oplus RotR(x, 11) \oplus RotR(x, 25) \tag{A.6}$$

A.2. Algoritmo de implementación.

A continuación, se procederá a explicar a detalle cómo funciona el algoritmo de la implementación hash 256.

Hay algunas consideraciones que se deben tomar en cuenta antes de comenzar con esta etapa, y entre ellas está que cada caracter utilizado debe tener forzosamente 8 bits al representarse en código binario. Si se llegaran a utilizar caractéres que utilicen menos bits estos deben completarse añadiendo ceros a la izquiera. Otra consideración es que todos los caractéres deben ser considerados como tipo ”string”, incluyendo los números.

Por ejemplo, si se requiere convertir el número 13 a binario, se tendría: 00110001 00110011 ya que se consideran los valores como caracteres. Una buena herramienta que se puede utilizar para estas conversiones está en la liga: $https://es.convertbinary.com/texto-a-binario/$.

Por último, hay que evitar utilizar letras con acentos o tildes ya que algunos algoritmos no los consideran como caracteres.

A.2.1. Etapa de relleno

Ahora que se han definido las consideraciones se explicará paso a paso la primera etapa de este algoritmo, llamada etapa de relleno. La siguiente figura muestra el diagrama del flujo de dicha etapa:

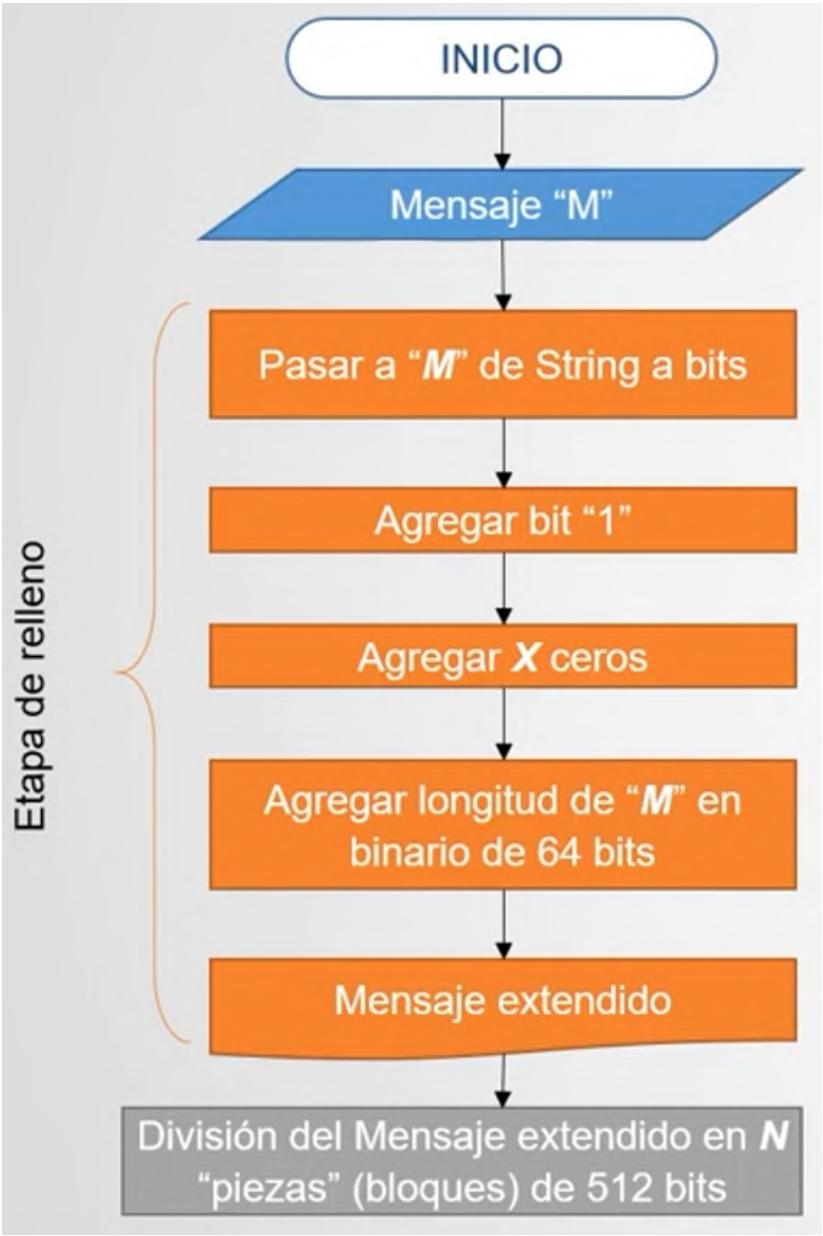


Figura A.6: Etapa de relleno.

En esta primera parte, lo que se debe hacer es convertir cada letra del mensaje original a código binario, siguiendo las recomendaciones anteriores.

Por ejemplo, para este seguimiento se va a calcular el hash de la palabra $hola\ Blockchain$. Lo primero que se debe hacer es validar el número de carcateres del texto inicial considerando los espacios, en este caso se van a convertir 15 caracteres a código binario, el resultado sería:

01101000 01101111 01101100 01100001 00100000 01000010 01101100 01101111 01100011 01101011 01100011 01101000 01100001 01101001 01101110

De acuerdo al dato anterior se tiene un total de 15 bytes que corresponden a cada caracter definido,

por lo tanto se cuenta con una longitud total de 120 bits.

El siguiente paso será añadir un bit 1 al final de los obtenidos 120 bits anteriores obteniendo:

01101000 01101111 01101100 01100001 00100000 01000010 01101100 01101111 01100011 01101011 01100011 01101000 01100001 01101001 01101110 1

Para agregar *x* cantidad de ceros se empleará la siguiente fórmula, donde *l* es la longitud del mensaje en bits:

$$x = (448 - l - 1) \bmod 512$$

Al sustituir los valores se tendrá lo siguiente:

$$x = (448 - 120 - 1) \bmod 512 = 327 \bmod 512 = 327 \text{ ceros}$$

Esto significa que además de agregar 1 bit, se agregarán 327 ceros al final del código binario obteniendo un total de 448 bits.

Después se agrega la longitud del mensaje inicial en binario. En este caso se convirten los 120 bits a binario (en esta conversión si se consideran los valores cómo decimales):

$$120 = (1111000)_2$$

Debido a que sólo se cuentan con 7 bits, se añaden 57 ceros a la izquierda para completar los 64 bits.

$$0000000000000000000000000000000000000000000000000000000001111000$$

Los 64 bits serán agregados a los 448 bits anteriores dando un fragmento de 512 bits. Es importante que el valor total sea divisible entre 512 ya que esto nos será de utilidad para la división de piezas (bloques) en el siguiente paso. En este caso particular nos da un valor de:

$$N = \frac{totaldebits}{512} = \frac{512}{512} = 1$$

De acuerdo con la división anterior sólo se cuenta con un fragmento de una pieza. En caso de tener un valor N ≥ 2 será necesario ralizar una división de dicho fragmento entre N cadenas de 512 bits cada una.

A.2.2. Lazo principal

Una vez teniendo estos valores se realizará la siguiente etapa conocida como Lazo principal:

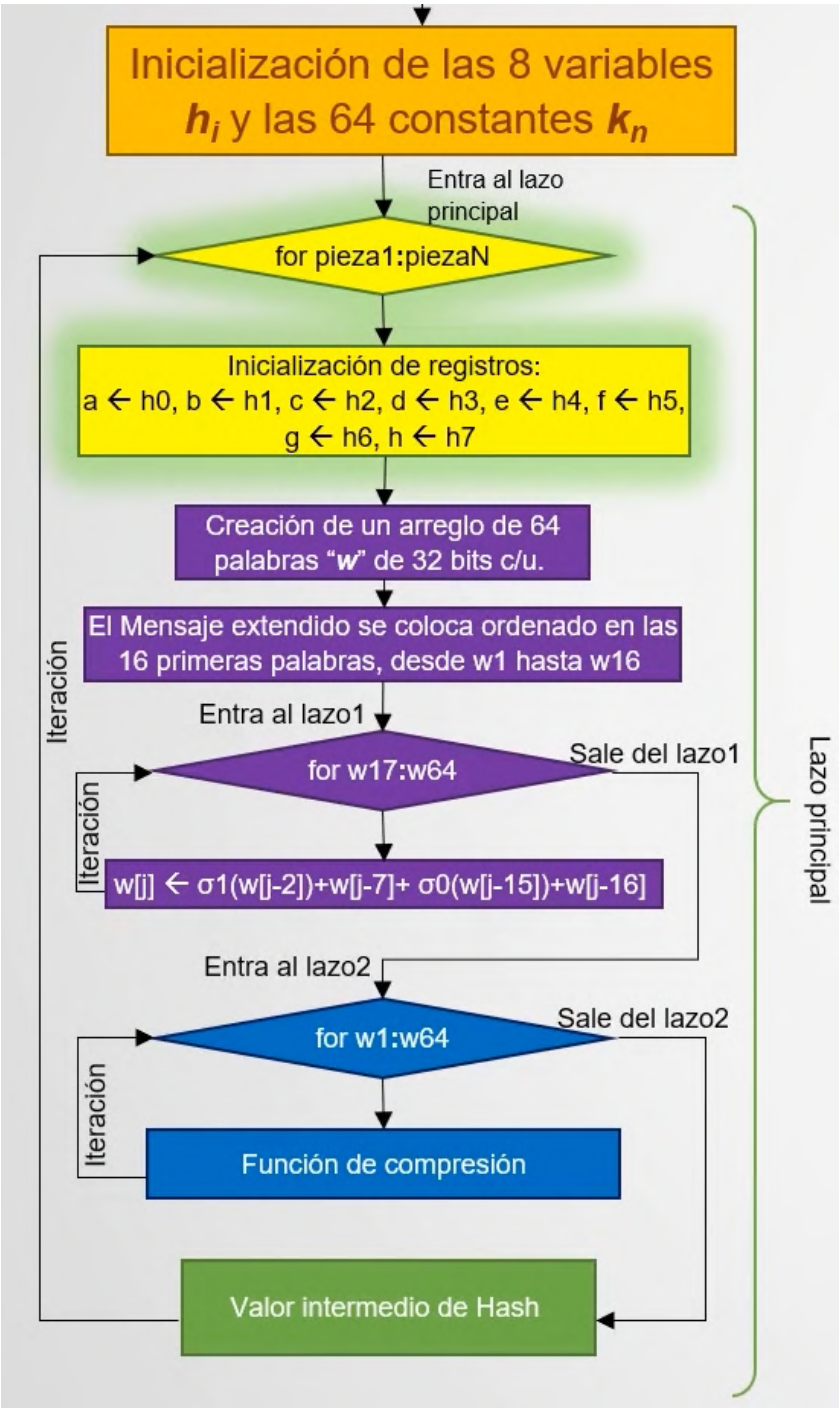


Figura A.7: Etapa de Lazo principal con sus respectivas iteraciones.

Es importante aclarar que dichos pasos se realizarán por piezas de 512 bits, de modo que, al finalizar cada pieza, los valores de las variables y las constantes de la figura A.7 serán guardados para utilizarse en la pieza siguiente. En este caso particular únicamente se cuenta con una pieza por lo que se realizará lo siguiente; se asignan los primeros hashes correspondientes a la figura A.8, registrando sus valores en las variables que se muestran a continuación:

$$a = h_0$$
$$b = h_1$$
$$c = h_2$$
$$d = h_3$$

$$e = h_4$$
$$f = h_5$$
$$g = h_6$$
$$h = h_7$$

Después de la asignación de registros se pasará a la creación de arreglos w de 64 palabras, donde cada palabra tendrá una longitud de 32 bits.

Para este paso, nuestra pieza de 512 será dividida en 16 partes iguales, al hacer la división se tendrá que cada parte equivale a 32 bits cada una. Lo que se hará después, será definir las primeras 16 palabras desde w_1 hasta w_{16} con las partes obtenidas en nuestra pieza de 512 bits.

Ahora que se tienen las primeras 16 palabras, se realizará el resto de las 48 iteraciones que abarcan las palabras w_{17} hasta la w_{64}. Este proceso se llevará a cabo con la siguiente ecuación:

$$w_n = \sigma 1(w_{n-2}) + w_{n-7} + \sigma 0(w_{n-15}) + w_{n-16} \tag{A.7}$$

Sustiuyendo los valores en cada iteración se tendría lo siguiente:

$$w_{17} = \sigma 1(w_{15}) + w_{10} + \sigma 0(w_2) + w_1$$
$$...$$
$$w_{64} = \sigma 1(w_{62}) + w_{57} + \sigma 0(w_{49}) + w_{48}$$

Incialización de variables

Antes de continuar con la siguente etapa del lazo principal, se procederá con la siguiente etapa del algoritmo que es la Inicialización de variables h_i y constantes k_n.

Para este paso se deben utilizar las variables h conocidas como hashes las cuales se calculan con la siguiente fórmula, definiendo a ρ como un número primo:

$$h_n = parte fraccionaria \sqrt[2]{\rho} * 2^{32} \tag{A.8}$$

Sustituyendo los valores para h_0 se tendría lo siguiente:

$$h_0 = \textit{parte fraccionaria } \sqrt[2]{2} * 2^{32}$$
$$h_0 = \textit{0.4142135623730951} * 2^{32} = \textit{1779033703}$$

Si convertimos ese valor a su versión binaria se obtendría lo siguiente:

$$\textit{1779033703} = (01101010000010011110011001100111)_2$$

A continuación, se muestra una tabla con los valores obtenidos de acuerdo a la fórmula anterior, proponiendo los primeros ocho números primos partiendo desde el 2.

	No. Primo	Raíz cuadrada	Fraccionario	* 2^{32}	Binario
h_0	2	1.414213562	0.414213562	1779033703	01101010000010011110011001100111
h_1	3	1.732050808	0.732050808	3144134277	10111011011001111010111010000101
h_2	5	2.236067977	0.236067977	1013904242	00111100011011011111001101110010
h_3	7	2.645751311	0.645751311	2773480762	10100101010011111111101010011 1010
h_4	11	3.31662479	0.31662479	1359893119	01010001000011100101001001111111
h_5	13	3.605551275	0.605551275	2600822924	10011011000001010110100010001100
h_6	17	4.123105626	0.123105626	528734635	00011111100000111101100110101011
h_7	19	4.358898944	0.358898944	1541459225	01011011111000001100110100011001

Figura A.8: Variables h_i.

Estas variables reciben ese nombre ya que su valor irá variando con cada iteración. Este proceso se definirá a detalle en la etapa de lazo principal.

Posteriormente, se tienen las constantes k las cuales mantienen un valor fijo de entrada que debe ser utilizado sin importar el texto de entrada que se tenga. Dichas constantes se definen de manera similar a las variables, siguiendo la siguiente fórmula:

$$k_n = parte fraccionaria \sqrt[3]{\rho} * 2^{32} \tag{A.9}$$

Sustituyendo los valores para k_1 se tendría lo siguiente:

$$k_1 = \textit{parte fraccionaria } \sqrt[2]{2} * 2^{32}$$
$$k_1 = \textit{0.2599210499} * 2^{32} = \textit{1116352408}$$

Si convertimos ese valor a su versión binaria se obtendría lo siguiente:

$$\textit{1116352408} = (01000010100001010001011111001100 0)_2$$

A diferencia de las constantes, aquí se deben calcular los 64 primeros valores desde k_1 hasta k_{64}, se muestra una tabla con los valores obtenidos de acuerdo a la fórmula anterior, proponiendo los primeros ocho números primos partiendo desde el 2.

	No. Primo	Raíz cúbica	Fraccionario	* 2^{32}	Binario
k_0	2	1.25992105	0.25992105	1116352408	01000010100001010001011111001100 0
k_1	3	1.44224957	0.44224957	1899447441	01110001001101110100010010010001
k_2	5	1.709975947	0.709975947	3049323471	10110101110000001111101111001111
k_3	7	1.912931183	0.912931183	3921009573	11101001101101011101101110100101
k_4	11	2.223980091	0.223980091	961987163	00111001010101101100001001011011
...	...	...	...	...	...
k_{63}	307	6.745996712	0.745996712	3204031479	10111110111110011010001111110111
k_{64}	311	6.775168952	0.775168952	3329325298	11000110011100010111100011110010

Figura A.9: Variables k_n.

Sustitución de registros

Después de definir cómo se calculan las 16 palabras y de contar con nuestras variables y constantes se irá al siguiente paso del algoritmo que se basa en la función de compresión de cada palabra. Significa que este proceso se aplicará a todas las palabras desde w_1 hasta la w_{64}. A continuación, se definen las sustituciones a realizar en los registros anteriormente mencionados:

$$T1 = h + \sum 1(e) + Ch(e, f, g) + k_n + w_n$$
$$T2 = \sum 0(a) + Maj(a, b, c)$$
$$h = g$$
$$g = f$$
$$f = e$$
$$e = d + T1$$
$$d = c$$
$$c = b$$
$$b = a$$
$$a = T1 + T2$$

Después de realizar las 64 iteraciones con cada palabra, se aplicará la siguiente suma con los valores h_i obtenidos en la última iteración, es decir en la número 64.

$$h_0 = a + h_0$$
$$h_1 = a + h_1$$
$$h_2 = a + h_2$$
$$h_3 = a + h_3$$
$$h_4 = a + h_4$$
$$h_5 = a + h_5$$
$$h_6 = a + h_6$$
$$h_7 = a + h_7$$

Nota: las sumas mostradas con anterioridad son sumas (A+B) MOD 2^{32}.

En este caso particular se terminan las iteraciones debido a que solo se contaba con una pieza de 512 bits. Sin embargo, en caso de contar con más piezas lo que se debe hacer es volver a empezar con las 64 palabras w_n, pero esta vez inicializando con los registros h_i resultantes de la primera pieza. Después de finalizar con todas las piezas y todas las iteraciones se contará con ocho hasehs finales h_i. Esos valores serán los que contengan el hash final.

Por lo tanto, se juntarán (concatenar) los últimos valores hash de la N-ésima pieza tal y como se muestra a continuación:

$$Hash = h_0h_1h_2h_3h_4h_5h_6h_7$$

Hash =

1101111111011111101111000001011100000000111100010011101010100100000011100110011110101101101111100111111010101001011011001111101000110110011111011100001110101111101000010111101110000001001110111111001010000111100001011100001010101101010011111001001011101110000000100111011111100101000011110000101110000101010110101001111100101101110110

Por último se hará la conversión a hexadecimal. Debido a que cada variable h_i es de 32 bits, al sconcatenar las 8 variables se tendrá un valor de 256 bits. Al convertirlo a hexadecimal se tendrá un valor de 64 digitos:

dfdfbc1701e275481ccf5b6f9faa5b3e8d9ee1d7d0bdc09df943c2e156a7cb76

Este valor obtenido será nuestro hash final.

Referencias: (Montenegro, 2021), (Rovira, 2021)

Apéndice B

Instalación de Aula Virtual

En este apéndice se explicará paso a pasó cómo se llevo a cabo la instalación de Moodle.

B.1. Instalación de la máquina virtual

Primero ingresamos al sitio web *virtualbox.org* y descargamos la última versión disponible, en este caso se descargó la versión *7.0* para Linux, ya que la máquina física a utilizar tiene un Sistema Operativo Linux Fedora 24:

Figura B.1: Descarga de VirtualBox en su sitio oficial.

Al tener instalado nuestro programa aparecerá la siguiente interfaz:

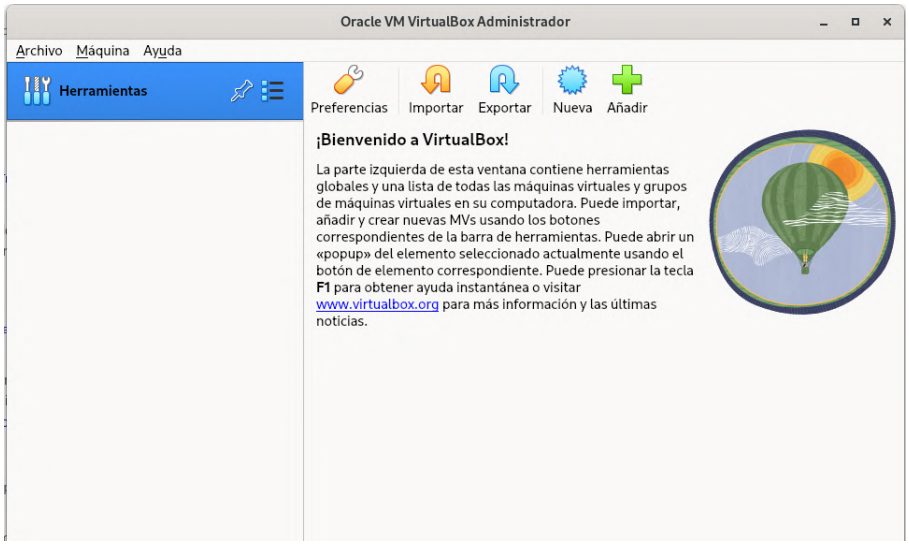


Figura B.2: Instalación de VirtualBox

Descargamos la versión más actual del sistema operativo (24.04 LTS) en el sitio oficial de Xubuntu.

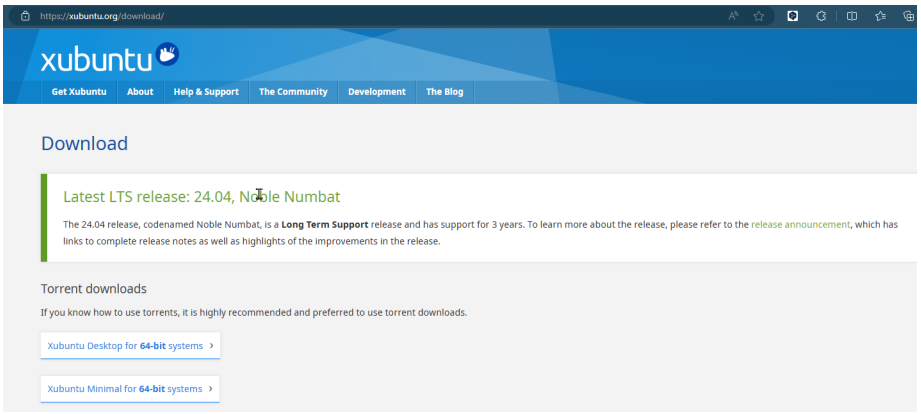


Figura B.3: Descarga del sistema operativo en el sitio oficial de Xubuntu.org.

Una vez descargado nuestro sistema operativo creamos una nueva máquina virtual a la cuál se le asignaron las siguientes características:

Figura B.4: Resumen de la configuración en la Máquina Virtual.

Algunas de las configuraciones realizadas son:

- Idioma: Español
- Conexión de red: Utilizar conexión por cable
- Tipo de instalación: Interactiva
- Aplicaciones: Xubuntu Desktop
- Configuración de disco: Borrar e instalar Xubuntu

Para la cuenta del usuario administrador asignamos los siguientes datos para crear el modo super usuario:

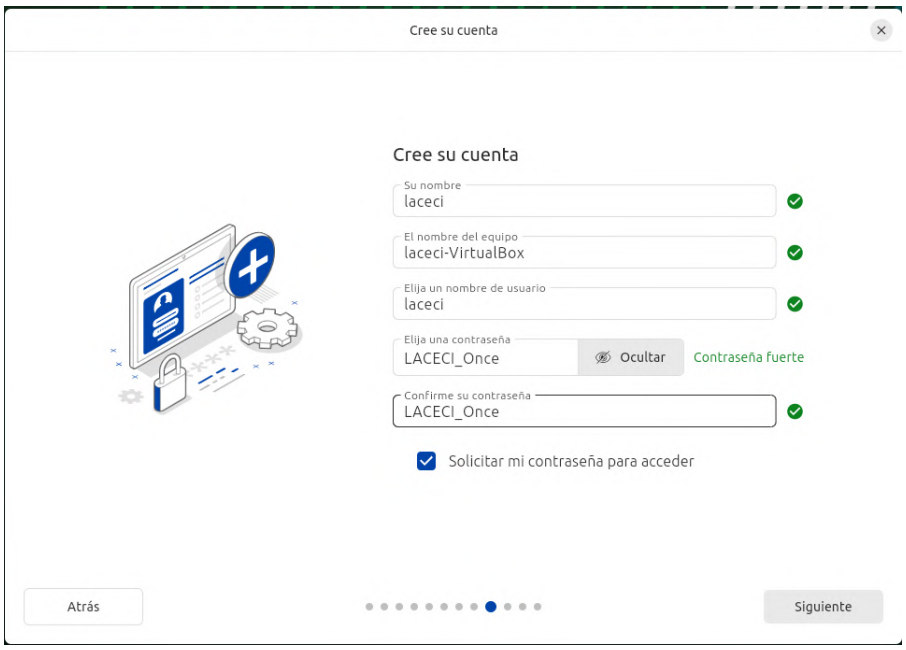


Figura B.5: Registro del super usuario de Linux.

Después de la configuración esperamos que termine de instalarse nuestra máquina virtual:

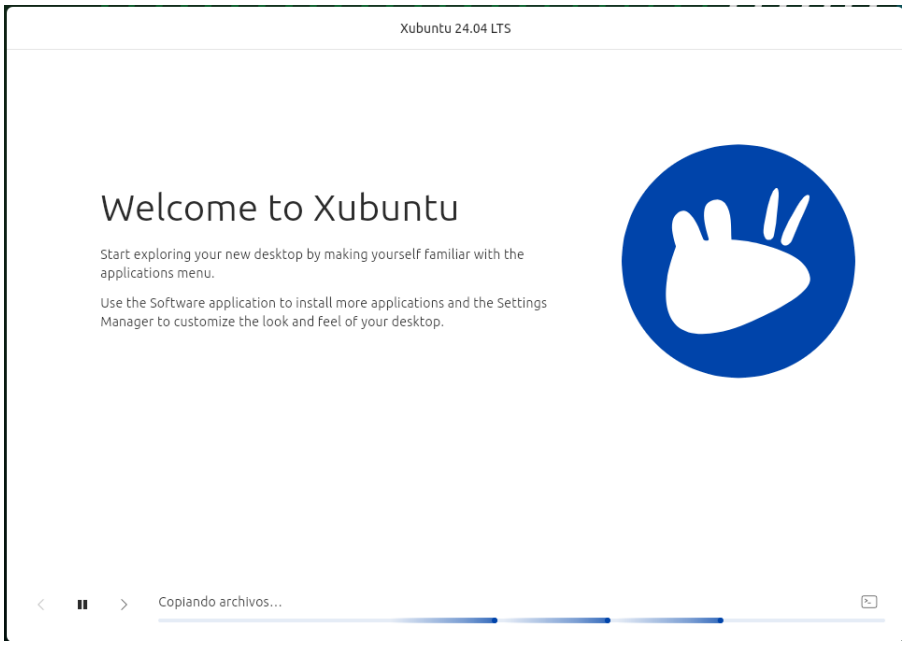


Figura B.6: Instalación de archivos de Xubuntu 24.04 LTS.

Después de que carguen todos los servicios reiniciamos el equipo. Una vez que haya cargado tendremos nuestra máquina virtual instalada

B.2. Instalación y configuración de Moodle

B.2.1. Instalación de LAMP

Ingresamos a nuestra máquina virtual y lo que haremos será instalar Apache, MariaDB y PHP en modo administrador:

```
apt install apache2
apt install mariadb-server
apt install php
```

```
root@laceci-VirtualBox:/home/laceci#
root@laceci-VirtualBox:/home/laceci# apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 1896 kB de archivos.
Se utilizarán 7452 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 libapr1t64 amd64 1.7.2-3.1build2 [107 kB]
```

Figura B.7: Instalación de apache2.

```
root@laceci-VirtualBox:/home/laceci#
root@laceci-VirtualBox:/home/laceci# apt install mariadb-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  galera-4 gawk libconfig-inifiles-perl libdaxctl1 libdbd-mysql-perl libdbi-perl libhtml-template-perl libmariadb3
  libmysqlclient21 libndctl6 libpmem1 libsigsegv2 mariadb-client mariadb-client-core mariadb-common
  mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
  mariadb-plugin-provider-snappy mariadb-server-core mysql-common pv socat
Paquetes sugeridos:
  gawk-doc libnet-daemon-perl libsql-statement-perl libipc-sharedcache-perl mailx mariadb-test
Se instalarán los siguientes paquetes NUEVOS:
  galera-4 gawk libconfig-inifiles-perl libdaxctl1 libdbd-mysql-perl libdbi-perl libhtml-template-perl libmariadb3
  libmysqlclient21 libndctl6 libpmem1 libsigsegv2 mariadb-client mariadb-client-core mariadb-common
  mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
  mariadb-plugin-provider-snappy mariadb-server mariadb-server-core mysql-common pv socat
0 actualizados, 25 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 18.9 MB de archivos.
Se utilizarán 198 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://mx.archive.ubuntu.com/ubuntu noble/universe amd64 galera-4 amd64 26.4.16-2build4 [736 kB]
```

Figura B.8: Instalación de mariadb.

```
root@laceci-VirtualBox:/home/laceci#
root@laceci-VirtualBox:/home/laceci# apt install php
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libapache2-mod-php8.3 php-common php8.3 php8.3-cli php8.3-common php8.3-opcache php8.3-readline
Paquetes sugeridos:
  php-pear
Se instalarán los siguientes paquetes NUEVOS:
  libapache2-mod-php8.3 php php-common php8.3 php8.3-cli php8.3-common php8.3-opcache php8.3-readline
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 4915 kB de archivos.
Se utilizarán 22.4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php-common all 2:93ubuntu2 [13.9 kB]
Des:2 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php8.3-common amd64 8.3.6-0maysync1 [738 kB]
Des:3 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php8.3-opcache amd64 8.3.6-0maysync1 [371 kB]
Des:4 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php8.3-readline amd64 8.3.6-0maysync1 [13.5 kB]
Des:5 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php8.3-cli amd64 8.3.6-0maysync1 [1915 kB]
Des:6 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 libapache2-mod-php8.3 amd64 8.3.6-0maysync1 [1849 kB]
```

Figura B.9: Instalación de php.

Al terminar de instalar revisamos cuál es la versión de php, en este caso se cuenta con la *8.3.6*

```
php -version
```

```
root@laceci-VirtualBox:/home/laceci# php -version
PHP 8.3.6 (cli) (built: Apr 15 2024 19:21:47) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.3.6, Copyright (c) Zend Technologies
    with Zend OPcache v8.3.6, Copyright (c), by Zend Technologies
root@laceci-VirtualBox:/home/laceci# cd /etc/php
root@laceci-VirtualBox:/etc/php# ls
8.3
root@laceci-VirtualBox:/etc/php#
```

Figura B.10: Versión de php.

Revisamos que apache funcione de manera correcta, para esto se empleará la instrucción:

```
service apache2 status
```

```
root@laceci-VirtualBox:/etc/php#
root@laceci-VirtualBox:/etc/php# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-06-18 17:02:44 CST; 2min 59s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 12358 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 12362 (apache2)
      Tasks: 6 (limit: 4615)
     Memory: 10.6M (peak: 11.2M)
        CPU: 67ms
     CGroup: /system.slice/apache2.service
             ├─12362 /usr/sbin/apache2 -k start
             ├─12365 /usr/sbin/apache2 -k start
             ├─12366 /usr/sbin/apache2 -k start
             ├─12367 /usr/sbin/apache2 -k start
             ├─12368 /usr/sbin/apache2 -k start
             └─12369 /usr/sbin/apache2 -k start

Jun 18 17:02:44 laceci-VirtualBox systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 18 17:02:44 laceci-VirtualBox apachectl[12361]: AH00558: apache2: Could not reliably determine the server's fully qualifi>
Jun 18 17:02:44 laceci-VirtualBox systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
```

Figura B.11: Servidor apache funcionando correctamente.

Para validarlo ingresamos a nuestro navegador y buscamos localhost:

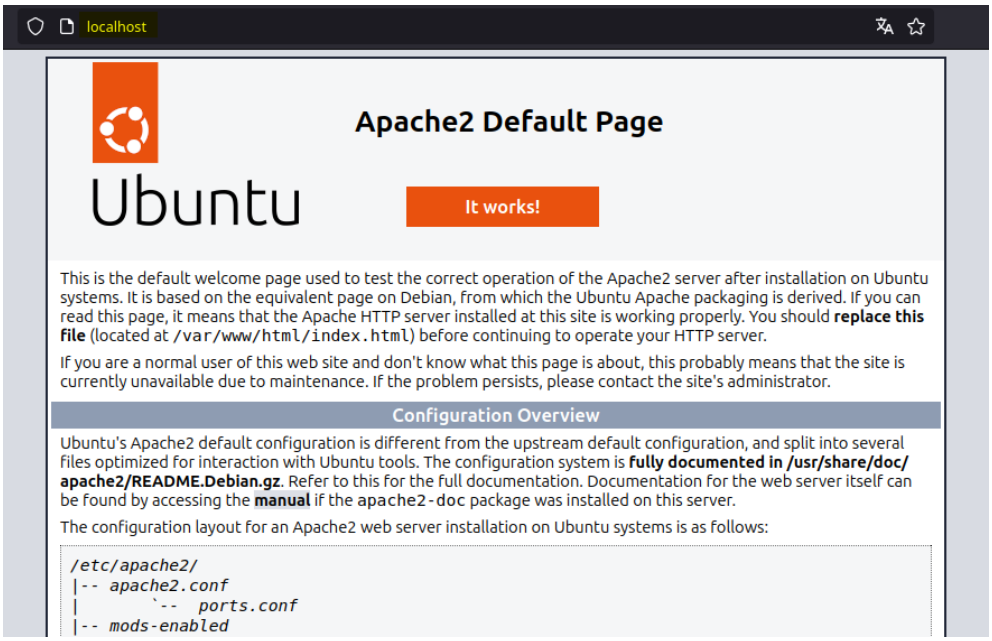


Figura B.12: Servidor desde nuestro navegador.

Como se puede observar en la figura anterior, nuestro servidor lamp ha sido instalado correctamente.

B.2.2. Instalación de moodle

Ingresamos al sitio de *moodle.org* y descargamos la última versión disponible, en este caso es la versión *4.4.1+*:

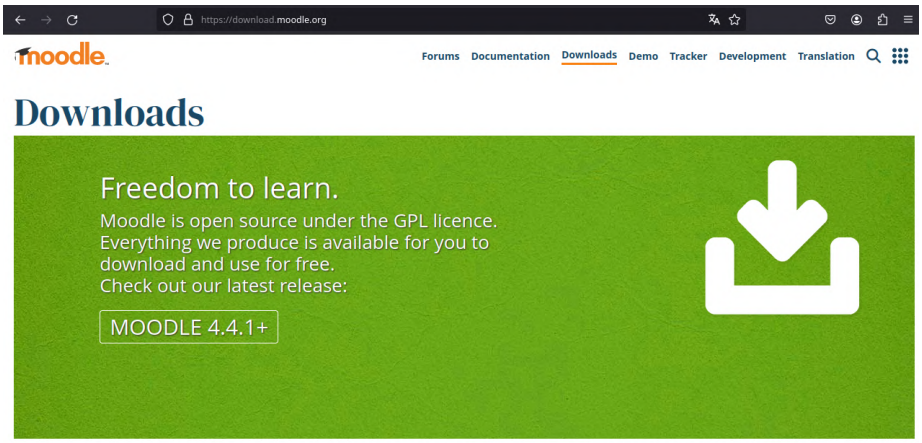


Figura B.13: Sitio oficial de descarga de moodle.

Después de esto descomprimimos el archivo y revisamos sus permisos, cabe mencionar que la carpeta se descomprime en la carpeta raíz de nuestro servidor apache

```
unzip moodle-latest-404.zip -d /var/www/html/
cd /var/www/html/
ls -la
```

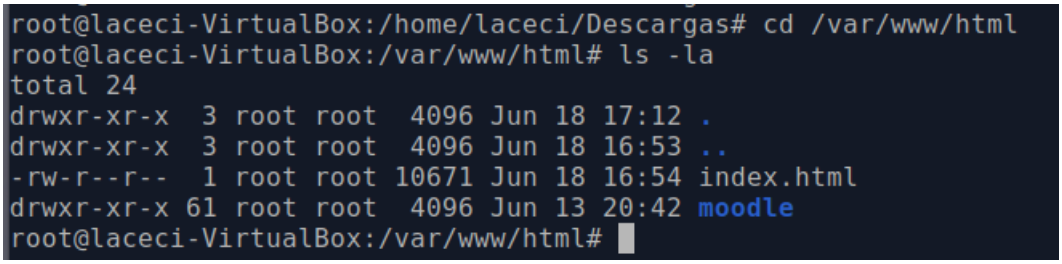


Figura B.14: Descarga y validación de permisos de moodle.

Como se puede observar el propietario de la carpeta *moodle* pertenece a *root* por lo que se realizará el cambio de modo que el propietario sea el navegador apache, para incluir los subdirectorios se añade *-R*:

```
chown -R www-data:www-data moodle/
ls -la
```

```
root@laceci-VirtualBox:/var/www/html#
root@laceci-VirtualBox:/var/www/html# chown -R www-data:www-data moodle/
root@laceci-VirtualBox:/var/www/html# ls -la
total 24
drwxr-xr-x  3 root     root      4096 Jun 18 17:12 .
drwxr-xr-x  3 root     root      4096 Jun 18 16:53 ..
-rw-r--r--  1 root     root     10671 Jun 18 16:54 index.html
drwxr-xr-x 61 www-data www-data  4096 Jun 13 20:42 moodle
root@laceci-VirtualBox:/var/www/html# cd moodle/
root@laceci-VirtualBox:/var/www/html/moodle# ls -la
total 1136
drwxr-xr-x 61 www-data www-data   4096 Jun 13 20:42 .
drwxr-xr-x  3 root     root       4096 Jun 18 17:12 ..
drwxr-xr-x 16 www-data www-data   4096 Jun 13 18:57 admin
drwxr-xr-x  5 www-data www-data   4096 Jun 13 18:57 analytics
drwxr-xr-x 16 www-data www-data   4096 Jun 13 18:57 auth
drwxr-xr-x  8 www-data www-data   4096 Jun 13 18:57 availability
drwxr-xr-x  8 www-data www-data   4096 Jun 13 18:57 backup
drwxr-xr-x  8 www-data www-data   4096 Jun 13 18:57 badges
-rw-r--r--  1 www-data www-data    311 Jun 13 18:57 behat.yml.dist
drwxr-xr-x 48 www-data www-data   4096 Jun 13 18:57 blocks
drwxr-xr-x  4 www-data www-data   4096 Jun 13 18:57 blog
-rw-r--r--  1 www-data www-data   1162 Jun 13 18:57 brokenfile.php
```

Figura B.15: Cambio de propietario para el directorio moodle.

Ahora creamos un directorio para almacenar nuestros datos, este directorio recibirá el nombre de *moodledata*:

```
sudo mkdir moodledata
ls -la
```

```
root@laceci-VirtualBox:/var/www/html/moodle#
root@laceci-VirtualBox:/var/www/html/moodle# cd /home
root@laceci-VirtualBox:/home# sudo mkdir moodledata
root@laceci-VirtualBox:/home# ls -la
total 16
drwxr-xr-x  4 root   root   4096 Jun 18 17:17 .
drwxr-xr-x 23 root   root   4096 Jun 18 15:51 ..
drwxr-x--- 15 laceci laceci 4096 Jun 18 16:17 laceci
drwxr-xr-x  2 root   root   4096 Jun 18 17:17 moodledata
root@laceci-VirtualBox:/home#
```

Figura B.16: Se crea directorio para almacenar la información de la base de datos.

Después de crearlo se le cambiará nuevamente el propietario:

```
chown -R www-data:www-data moodledata/
ls -la
```

```
root@laceci-VirtualBox:/home# chown -R www-data:www-data moodledata/
root@laceci-VirtualBox:/home# ls -la
total 16
drwxr-xr-x  4 root     root     4096 Jun 18 17:17 .
drwxr-xr-x 23 root     root     4096 Jun 18 15:51 ..
drwxr-x--- 15 laceci   laceci   4096 Jun 18 16:17 laceci
drwxr-xr-x  2 www-data www-data 4096 Jun 18 17:17 moodledata
root@laceci-VirtualBox:/home#
```

Figura B.17: Cambio de propietario para el directorio moodledata.

B.2.3. Configuración de la base de datos

Primero se activa la base de datos Maria DB, y luego creamos usuario y contraseña:

```
CREAT USER 'moodle'@'localhost' IDENTIFIED BY 'Laceci11#';
```

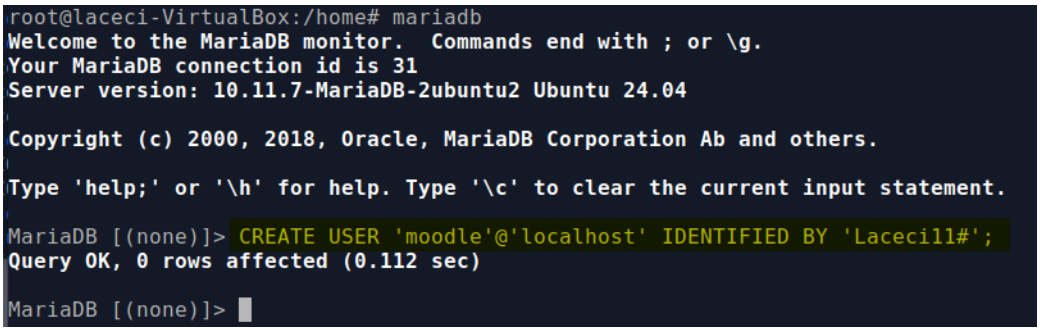


Figura B.18: Creación de usuario para base de datos.

Después creamos una base de datos bajo el nombre de *Moodle* y le daremos todos los privilegios. Para que funcione esto último empleamos el comando *FLUSH*:

```
CREATDE DATABASE Moodle;
GRANT ALL PRIVILEGES ON Moodle.* TO 'moodle'@'localhost';
FLUSH PRIVILEGES;
```

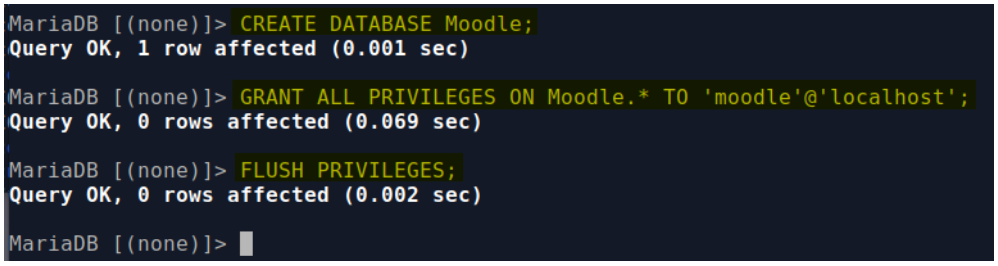


Figura B.19: Privilegios para el usuario de la base de datos.

B.2.4. Configuración de moodle

Ingresamos al sitio *localhost/moodle*:

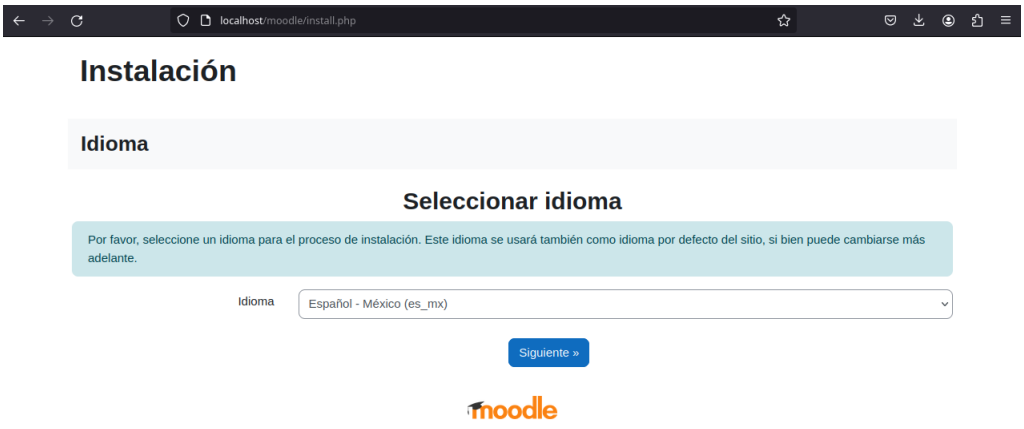


Figura B.20: Selección de idioma.

Después veremos la interfaz de rutas. Vamos a seleccionar el directorio *home/moodledata* que es donde creamos nuestra base de datos:

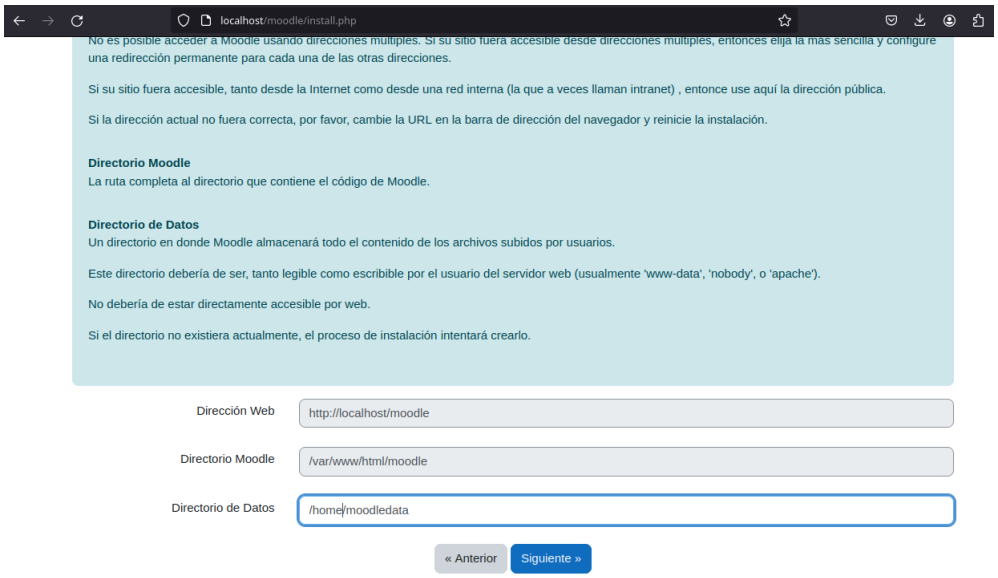


Figura B.21: Rutas de los directorios de Moodle y los Datos.

Seleccionamos nuestro controlador:

Figura B.22: Se selecciona MariaDB como controlador de la Base de Datos

Ingresamos los datos del usuario configurados anteriormente:

Figura B.23: Ajustes de la Base de Datos

En la siguiente interfaz damos continuar:

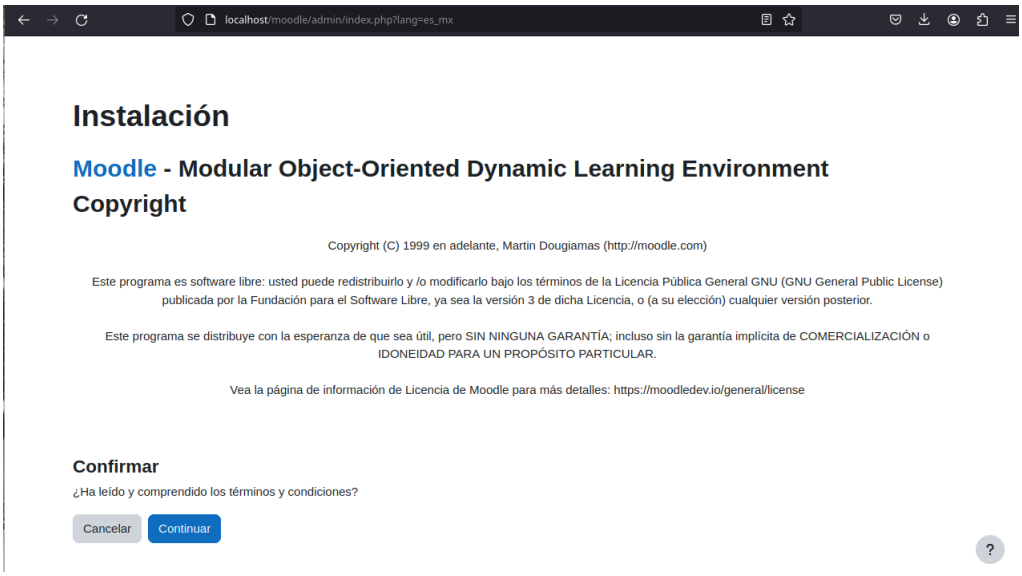


Figura B.24: Se aceptan los términos y condiciones

Después de esto nos aparecerán las siguientes recomendaciones, sin embargo, estas no afectan el funcionamiento de nuestro servidor:

Figura B.25: Comprobaciones del servidor previas a la instalación

Debido a que nuestro servidor no tiene salida a internet, no se necesita https para alcanzarlo desde la LAN de LACECI.

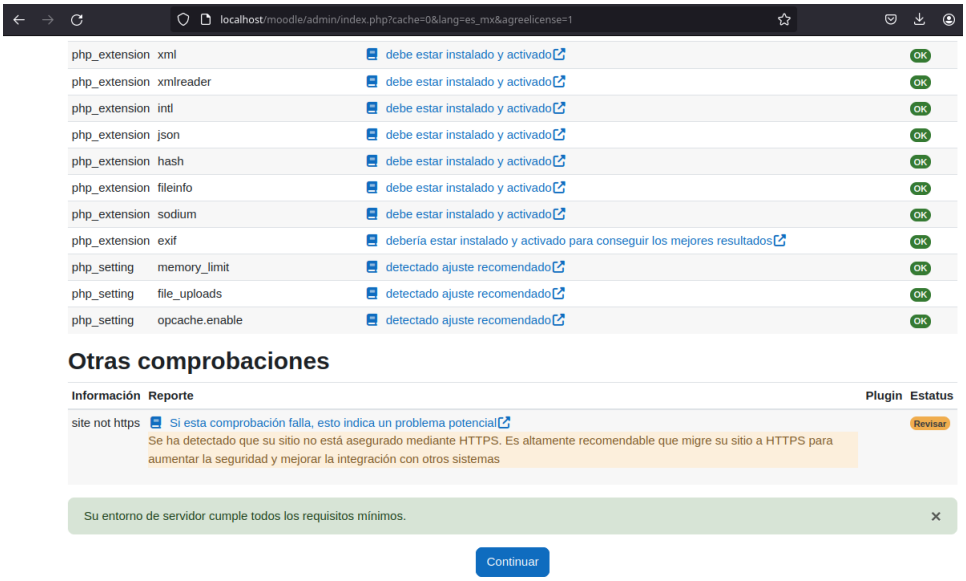


Figura B.26: Comprobaciones adicionales del servidor previas a la instalación

Después esperamos a que se realice la instalación. Cuando se valide que la instalación fue llevada a cabo correctamente daremos clic en continuar:

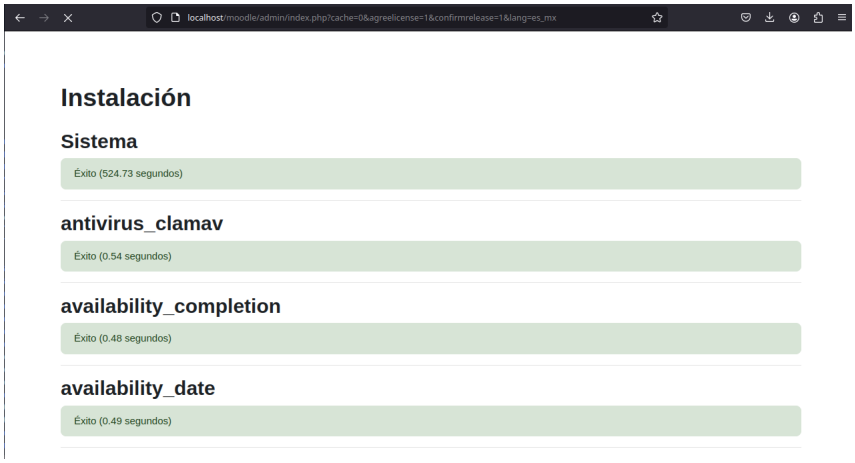


Figura B.27: Instalación y validación de los servicios

Ahora creamos nuestro usuario administrador y realizamos las últimas configuraciones de la página de inicio:

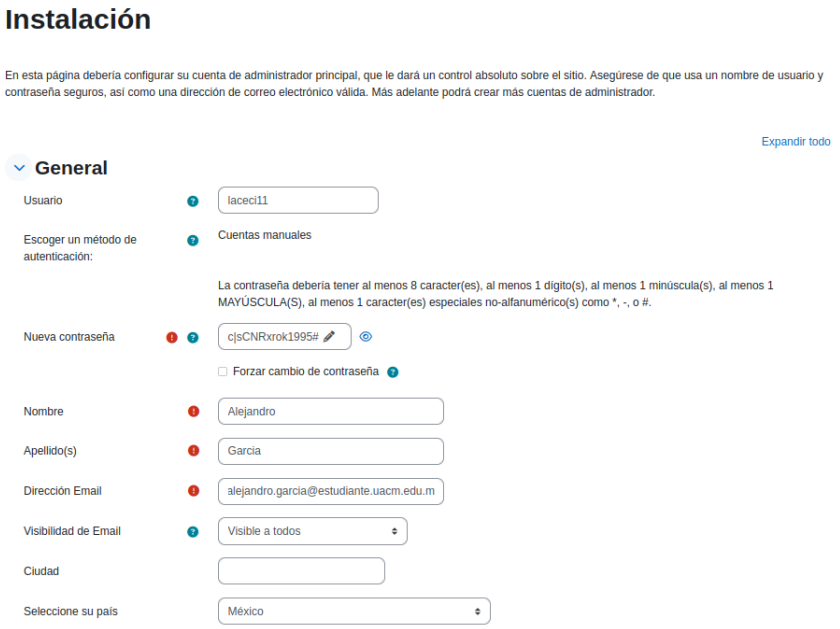


Figura B.28: Configuración del administrador principal

Después de guardar esta configuración se habrá concluido con la instalación

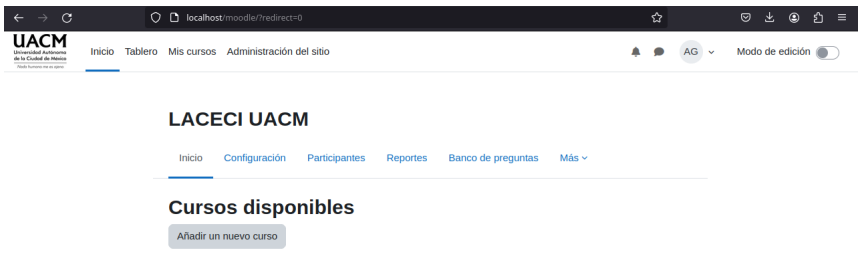


Figura B.29: Bienvenida de Moodle

B.3. Solución a errores presentados

En este capítulo se explican los errores que surgieron paulativamente en el transcurso de la instalación detallando los errores encontrados junto con sus respectivas soluciones. Cabe mencionar que al realizar cambios en nuestro servidor es neceserio reinicarlo para asegurarnos de que la configucación se realice se manera correcta.

B.3.1. Error kernel VirtualBox

Durante la instalación de VirtualBox se presentó el siguiente error:

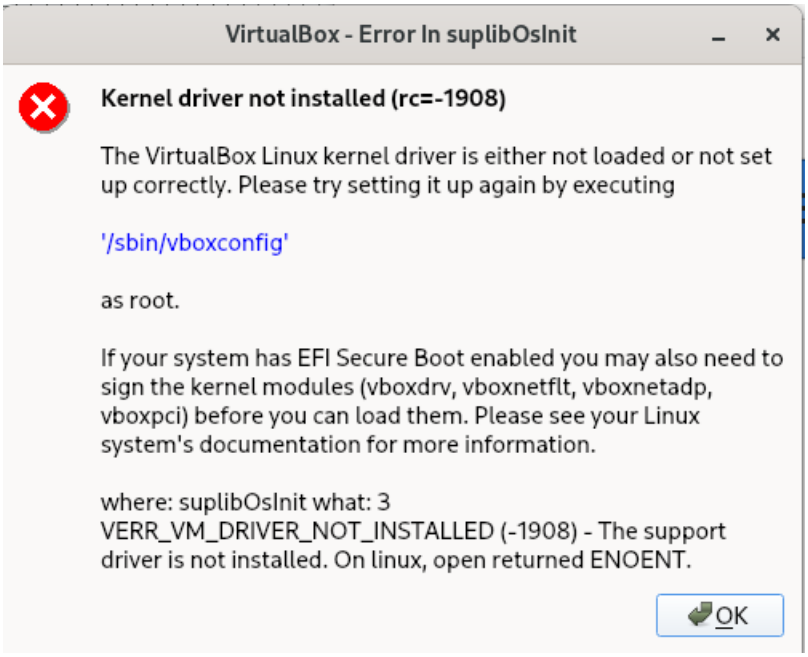


Figura B.30: Error rc=-1908

Esto nos indica que el controlador del kernel o las cabeceras de Linux no están cargadas o no se han configurado correctamente. Para solucionarlo se aplicaron tres instrucciones en la máquina física, los primeros dos se emplearon para la actualización del sistema. Seguido a eso se aplicó otra instrucción para la instalación del paquete esencial de compilación, esto último para la instalación de cabeceras de Linux de manera automática:

```
sudo yum update
sudo yum upgrade
sudo dnf install make automake gcc gcc-gcc++ kernel-devel
```

Referencias de la solución:
$https://www.youtube.com/watch?v=_Z TsesEHoUc$
$https://unix.stackexchange.com/questions/1338/what-is-the-fedora-equivalent-of-the-debian-build-essential-package$

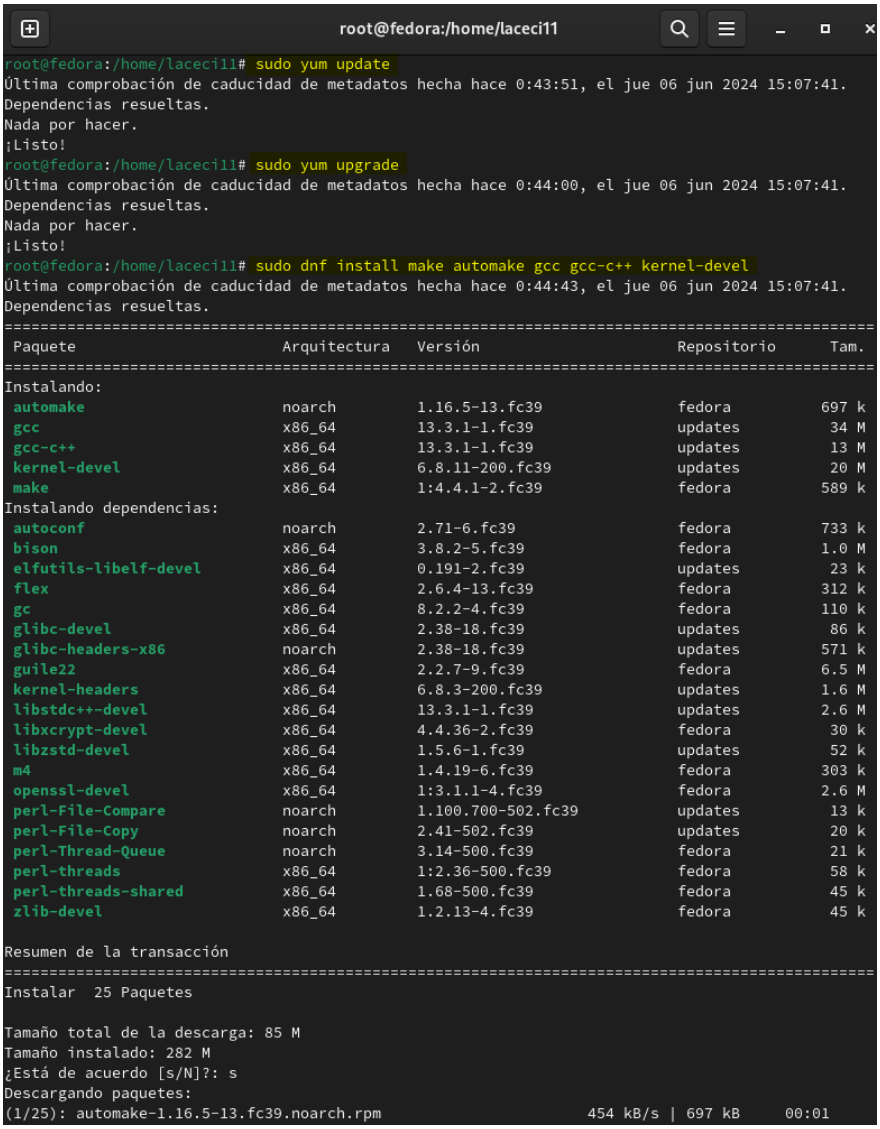


Figura B.31: Instalación de paquete esencial de compilación en Fedora.

```
sudo /sbin/vboxconfig
```

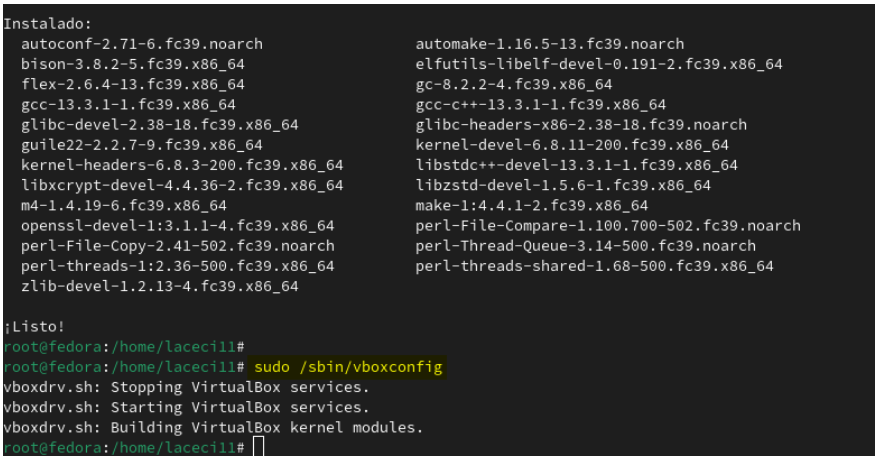


Figura B.32: Ejecución de vboxconfig

B.3.2. Instalaciones requeridas de php

Durante la instalación de moodle se presentaron errores solicitando la instalación de algunos servicios de php. A continuación se muestran dichos errores y sus soluciones correspondientes.

Extensiones cURL y Zip

Este error apareció después de seleccionar el idioma en Moodle. Para su solución se aplicaron las siguientes instrucciones para la instalación de extensiones solicitadas:

Figura B.33: Comprobación de entorno

```
apt install php-curl php-zip
```

```
root@laceci-VirtualBox:/home# apt install php-curl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  php8.3-curl
Se instalarán los siguientes paquetes NUEVOS:
  php-curl php8.3-curl
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 42.1 kB de archivos.
Se utilizarán 171 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php8.3-curl amd64 8.3.6-0maysync1 [40.3 kB]
Des:2 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php-curl all 2:8.3+93ubuntu2 [1836 B]
Descargados 42.1 kB en 1s (66.3 kB/s)
Seleccionando el paquete php8.3-curl previamente no seleccionado.
```

Figura B.34: Instalación de php-curl

```
root@laceci-VirtualBox:/home# apt install php-zip
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libzip4t64 php8.3-zip
Se instalarán los siguientes paquetes NUEVOS:
  libzip4t64 php-zip php8.3-zip
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 84.9 kB de archivos.
Se utilizarán 289 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://mx.archive.ubuntu.com/ubuntu noble/universe amd64 libzip4t64 amd64 1.7.3-1.1ubuntu2 [53.6 kB]
Des:2 http://mx.archive.ubuntu.com/ubuntu noble/universe amd64 php8.3-zip amd64 8.3.6-0maysync1 [29.5 kB]
Des:3 http://mx.archive.ubuntu.com/ubuntu noble/universe amd64 php-zip all 2:8.3+93ubuntu2 [1832 B]
Descargados 84.9 kB en 1s (94.2 kB/s)
Seleccionando el paquete libzip4t64:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 179998 ficheros o directorios instalados actualmente.)
```

Figura B.35: Instalación de php-zip

Reiniciamos apache para guardar los cambios:

```
service apache2 restart
```

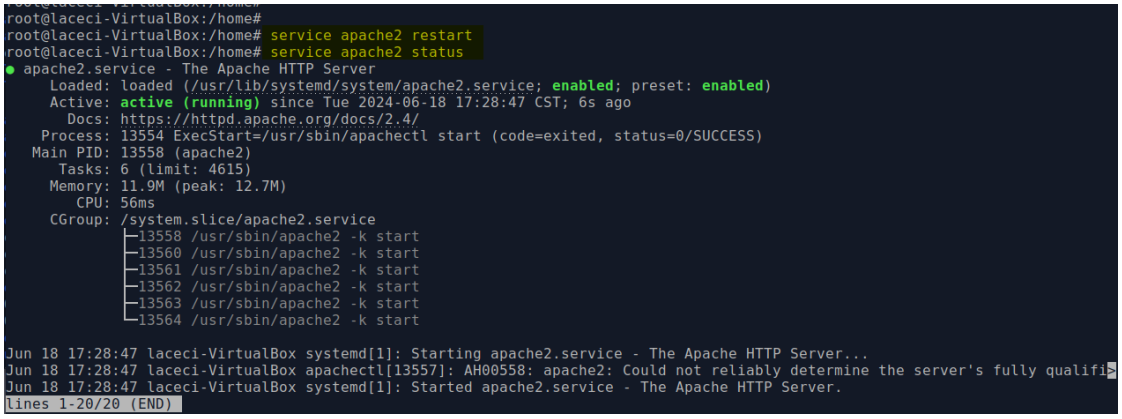


Figura B.36: Reinicio de servicios apache2

Extensión MySQLi

El siguiente error se presentó en los ajustes de la base de datos. Para su solución se instaló la extensión mysqli:

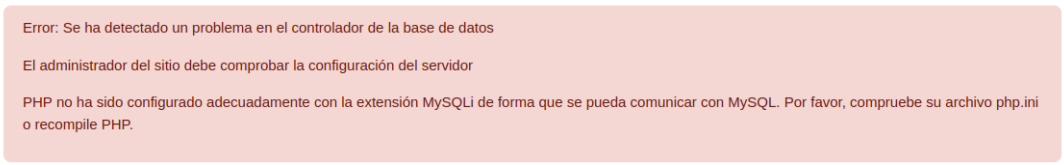


Figura B.37: Error de configuración de MySQLi

```
apt install php-mysqli
```

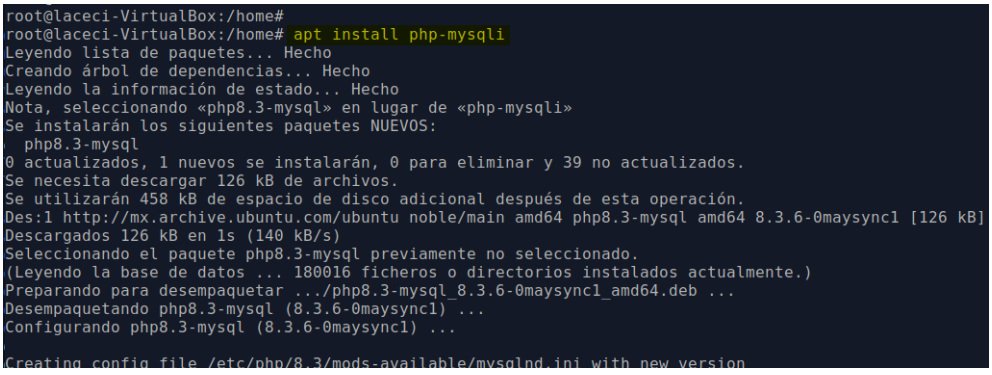


Figura B.38: Instalación de php-mysqli

Reiniciamos apache para guardar los cambios.

```
service apache2 restart
```

Extensiones xml y mbstring

Después de la instalación anterior, aparecerán estos mensajes solicitando la instalación de dos extensiones. Por lo que se aplicaron las siguientes instrucciones para su respectiva instalación:

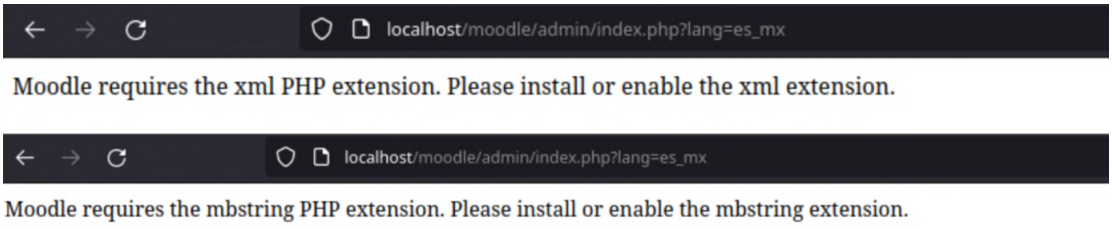


Figura B.39: Error de configuración de xml y mbstring

```
apt install php-xml php-mbstring
```

```
root@laceci-VirtualBox:/home#
root@laceci-VirtualBox:/home# apt install php-xml
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  php8.3-xml
Se instalarán los siguientes paquetes NUEVOS:
  php-xml php8.3-xml
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 128 kB de archivos.
Se utilizarán 516 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php8.3-xml amd64 8.3.6-0maysync1 [126 kB]
Des:2 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php-xml all 2:8.3+93ubuntu2 [1856 B]
Descargados 128 kB en 1s (127 kB/s)
root@laceci-VirtualBox:/home# apt install php-mbstring
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  php8.3-mbstring
Se instalarán los siguientes paquetes NUEVOS:
  php-mbstring php8.3-mbstring
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 513 kB de archivos.
Se utilizarán 1250 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://mx.archive.ubuntu.com/ubuntu noble/main amd64 php8.3-mbstring amd64 8.3.6-0maysync1 [512 kB]
Des:2 http://mx.archive.ubuntu.com/ubuntu noble/universe amd64 php-mbstring all 2:8.3+93ubuntu2 [1848 B]
Descargados 513 kB en 1s (647 kB/s)
Seleccionando el paquete php8.3-mbstring previamente no seleccionado.
```

Figura B.40: Instalación de php-xml y php-mbstring

Reiniciamos apache para guardar los cambios.

```
service apache2 restart
```

Extensiones gd e intl

Para concluir con la instalación se debe comprobar el servidor con todas las extensiones solicitadas. En este caso nos recomienda la extensión soap para plugins complementarios, sin embargo, no es crítico para el servidor y no afecta en su funcionamiento por lo que se descartó. Para el resto de extensiones se aplicaron las siguientes instrucciones para su instalación:

```
apt install php-gd php-intl
```

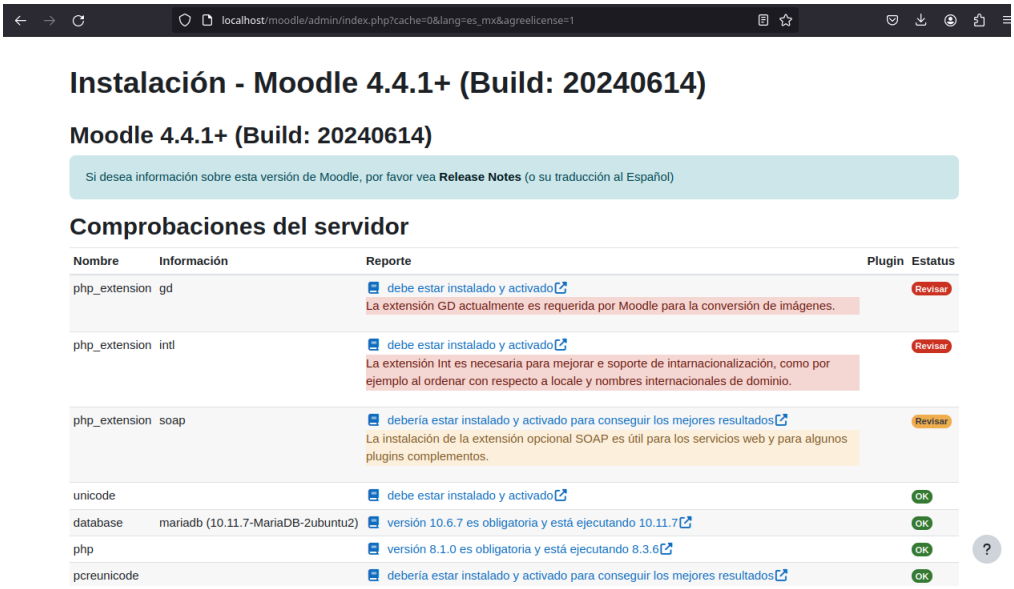


Figura B.41: Error de configuración de gd e intl

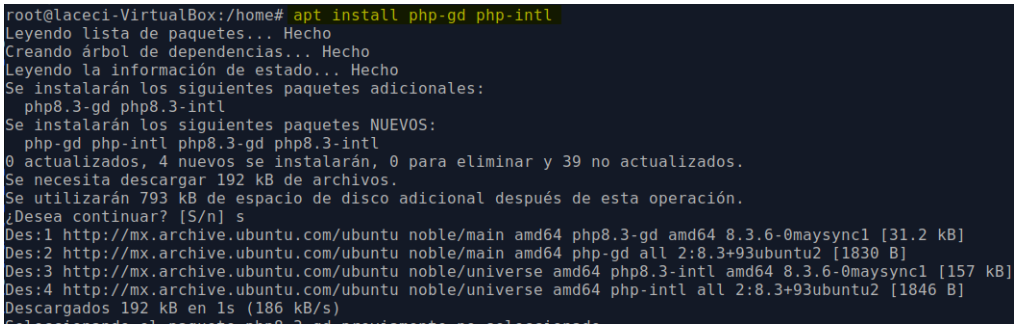


Figura B.42: Instalación de php-gd y php-intl

Reiniciamos apache para guardar los cambios.

```
service apache2 restart
```

Configuración *input_vars*

En la siguiente comprobación se solicita la configuración de la variable *max_input_vars* solicitando un valor mínimo de 5000 por lo que se le asignó 7000 y se quitó el *;* del inicio:

```
nano /etc/php/8.3/apache2/php.ini
```

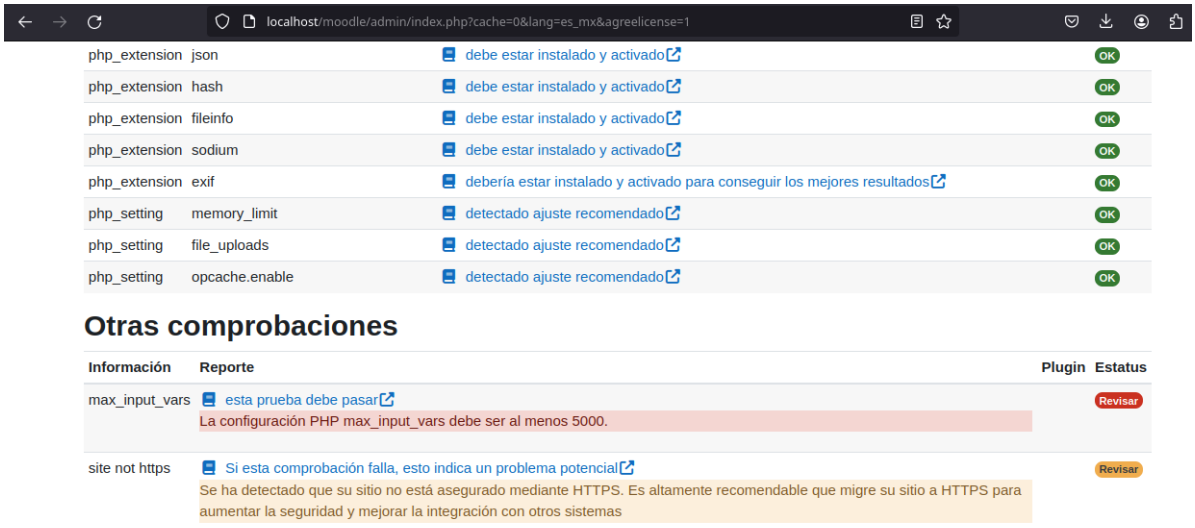


Figura B.43: Error de configuración max_input_vars

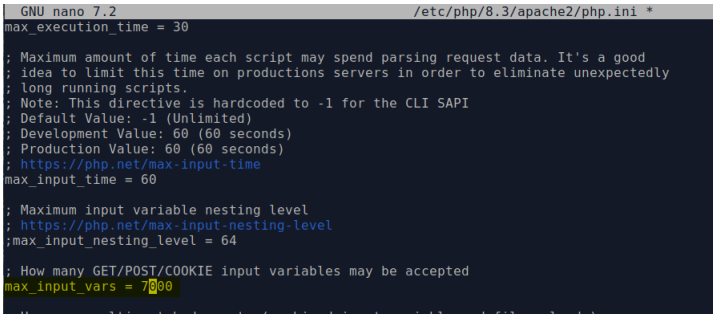


Figura B.44: Configuración de la variable max_input_vars

Para concluir con la configuración, dentro de ese mismo archivo se cambiaron las siguientes configuraciones para aumentar el tamaño de Megabytes de carga y descarga dentro de moodle. El tamaño puede ser el que se desee, en este caso se eligió de 400 MB para mayor facilidad respecto a su almacenamiento.

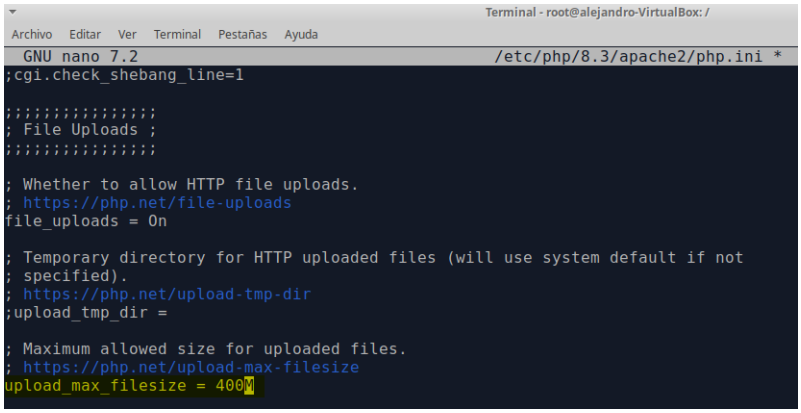


Figura B.45: Configuración de aumento de 400 MB para cargar archivos.

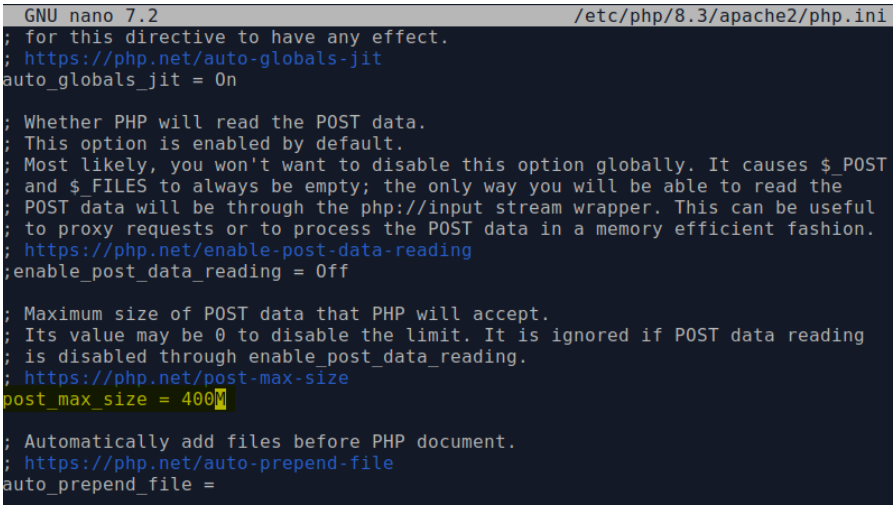


Figura B.46: Configuración de aumento de 400 MB para descargar archivos.

Reiniciamos apache para guardar los cambios.

```
service apache2 restart
```

Referencias

34, G. A. (2023). ¿qué es y para que sirve un hash? *Protecciónd atos*.

Amazon, A. (2023). ¿qué es la minería de datos? *AWS Amazon*.

Amengual, J. (2021). *Fundamentos de blockchain*. To the moon.

Andersen, D. (2024). Consumo energético de las criptomonedas aumentará más del 30 % en 2026. *Cointelegraph*.

Andrade, C., y Cedillo, D. (2004). *Criptografía en la seguridad de sistemas informáticos* (B.S. thesis). Universidad del Azuay.

Anirudh, V. (2022). Blockchain in supply chain by walmart. *Linkedin*.

Anáhuac. (2023). ¿en qué consiste un lms y cómo funciona? *Anáhuac México*.

Aparo, C. (2023). Blockchain y sus posibles aplicaciones en el sector jurídico. *Impact Lawyers*.

APD, R. (2019). ¿cuáles son los principales retos y riesgos del blockchain? *apd*.

Aritmetrics. (2022). Qué es moodle. *Aritmetrics*.

Aritmetrics. (2023). Qué es big data. *Aritmetrcis.com*.

Arnab Kumar, T. M. (2020). Blockchain: The india strategy. *NITI Aayog*.

Arteaga, E. (2023). Smart contracts: Perspectivas en la legislación mexicana actual y consideraciones para su aplicación. *CONAHCYT*.

Axinte, M. (2023). ¿qué es el feed de datos? *DataFeedWatch Blog*.

Baggetta, M. (2022). A concise history of blockchain technology. *Blockgeeks*.

Broncano, J. (2015). Criptografía clásica, cifrado asimétrico: Rabin, merkle-hellman. *Universidad Tecnologica del Perú*.

Buttu, M. (2016). *El gran libro de python*. Marcombo, S.A.

CABALLERO GONZÁLEZ, C., y CLAVERO GARCÍA, J. A. (2017). *Salvaguarda y seguridad de los datos*. Ediciones Paraninfo, SA.

Canle, E. (2022). Google colab, una nueva herramienta de google pensaba para especialistas de ia y data analysis. *TokioSchool*.

Casas, M. C. (2019). *Las fintech de préstamos o crowdlending*. REUS Editorial.

Comunicado no. 039 banco de méxico, shcp y cnbv advierten sobre riesgos de utilizar activos virtuales. (2021).

CONOCER. (2024). Estándar de competencia. *CONOCER*.

Contreros, R. (2022). ¿qué es ftx? *cryptoconexion*.

Díaz, J. C. G. (1995). *Criptografía: historia de la escritura cifrada*. Editorial Complutense.

Dobaño, R. (2023). Stripe: qué es y cómo funciona esta pasarela de pago. *Quipu*.

DTT, D. (2023). Acerca de deloitte... *Deloitte.com*.

Díaz, M. (2022). Rúbricas de evaluación: qué son, cómo crearlas y ejemplos. *codim*.

Euroinnova. (2023). *Qué es una aula virtual y para qué sirve?* Autor.

Fairfield, J. (2014). Smart contracts, bitcoin bots, and consumer protection. *Washington and Lee University School of Law*.

Fernández, J. A. M. (s.f.). *Sistemas seguros de acceso y transmisión de datos (mf0489_3)*. Grupo Editorial RA-MA.

Garrido, I. (2023). Bitshares (bts): ¡esto es lo que deberías saber sobre la criptomoneda bitshares. descripción, historia, opiniones de las criptomonedas. *FXMAG*.

Georgina Arcos, W. Y. (2018). *Iv congreso internacional de ingenierías*. Universidad Politécnica estatal del Carchi.

Gómez, W. (2023). ¿qué es un árbol merkle? *bit2me Academy*.

Herrera, J. (2023). Cambridge corrige sus estimaciones sobre el consumo eléctrico de bitcoin. *Cripto-noticias*.

INAP. (2024). Competencias conocer. *INAP*.

Insider, B. (2023). ¿qué puedo comprar con criptomonedas en méxico? *Bussines Insider México*.

Iñigo. (2019). ¿qué es la mempool en bitcoin? *bit2me Academy*.

JaeShup Oh, I. S. (2017). A case study on business model innovations using blockchain: focusing on financial institutions. *Asia Pacific Journal of Innovation and Entrepreneurship*.

Joaquín López Lérida, J. J. M. P. (2016). *La economía de blockchain, los modelos de negocio de la nueva web*. kolokium.

Johnsonbaugh, R. (1999). *Matemáticas discretas*. Prentice Hall.

Jordi Salazar, S. S. (2016). Internet de las cosas. *Yechpedia*.

Julio Ponce, F. Q., Aurora Torres. (2014). Inteligencia artificial. *LATIn*.

Levy, G. (2021). Análisis de la tecnología blockchain, su entorno y su impacto en modelos de negocio. *Udemy*.

Lory Kehoe, D. D., Eric Piscini. (2018). Blockchain & ciberseguridad. *Deloitte*.

Lozano, M. (2020). Lamp ¿qué es? instalación de apache, mysql y php en un servidor cloud con linux. *arsys*.

López, A. (2022a). Criptografía: Qué son los algoritmos hash y para qué se utilizan. *RZ redes zone*.

López, A. (2022b). Luna y ust: dos criptoactivos que dejarán una marca en la historia de la innovación. *cryptoconexion*.

Maher Alharby, A. v. M. (2017). Blockchain based smart contracts : A systematic mapping study. *3rd International Conference on Artificial Intelligence and Soft Computing*.

Maldonado, J. (2022). Qué es hyperledger fabric, la blockchain de las empresas. *observatorioblockchain.com*.

Maria Gonzalez, A. P. (2021). *Criptografía esencial*. DGP Editores SAS.

McCarthy, J. (2007). *What is artificial intelligence?* Stanford, CA 94305.

Meijer, C. R. D. (2019). Blockchain and big data: A great mariage. *FinExtra*.

Millán, A. (2023). Como funciona kickstarter para financiar tu proyecto. *skydropsx.com*.

Mohanty, D. (2019). *R3 corda for architects and developers*. Apress.

Montenegro, J. (2021). Sha-2 (sha-256) — explicación del algoritmo paso a paso — incluye implementación en matlab. *My School-365, Fuente: https://www.youtube.com/watch?v=S4UvSKMpwHU*.

Murray, M. (2019). Tutorial: A descriptiv orial: A descriptive introduction t oduction to the block o the blockchain. *Communications of the Association for Information Systems*.

Navarro, W. (2023). Historia del blockchain, la solución a un problema. *Sales & Marketing Manager de Addalia*.

NetApp. (2023). ¿qué es la inteligencia artificial? *NetApp*.

Network, U. I. (2020). *A practical guide to using blockchain within the united nations*. Autor.

Noelle Acheson, H. N., John Biggs. (2022). How do bitcoin transactions work? *CoinDesk*.

Norman, A. T. (2019). *Todo sobre tecnología blockchain*. Tektime.

Nzuva, S. (2019). Smart contracts implementation, applications, benefits, and limitations. *International Institute fos Science, Technology and Education (IISTE)*.

OIT. (2024). Consejo nacional de normalización y certificación de competencias laborales - conocer. *Organización Internacional del Trabajo*.

Oracle. (2023). ¿qué es big data? *Oracle*.

Rabah, K. (2018). Convergence of ai, iot, big data and blockchain: A review. *The Lake Institute Journal*.

Rial, S. (2023). Desafío 2023: qué pasará con las criptomonedas y dónde será importante poner el foco. *Ámbito financiero*.

Rodriguez, A. (2019). ¿cuál es el problema de la escalabilidad de blockchain? *Medium*.

Román, A. (2023). *Internet de las cosas teoría y práctica*. Universidad de Colima.

Rovira, P. (2021). Tutorial completo sha256 explicado paso a paso (incluye 224, 384, 512). *Pere Rovira - Tutoriales*.

Salces, D. (2022). ¿quién es gavin andresen? *W3volution*.

Sanz, J. (2015). *Criptografía, conceptos básicos*. AEINSE.

Services, S. (2023). ¿sabes para qué sirve watson, la ia de ibm? *sm-services.es*.

Sevilla, A. (2020). Crowdfunding. *economipedia*.

Sola, A. (2021). hashing. *techtarget.com*.

Stallings, W. (2004). *Fundamentos de seguridad en redes aplicaciones y estándares*. Pearson Educación S.A.

Swan, M. (2015). *Blockchain blueprint for a new economy*. O'Reilly.

Talan, M. (2023). ¿cómo blockchain puede mejorar los sistemas de inteligencia artificial? *criptoconexion.com*.

Thomas, R. L. (2023). *Códigos y cifrados clásicos*. Ediciones Lerner.

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo editorial PATRIA.

Wattana Viriyasitavat, D. H. (2018). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*.

Weber, R. H. (2010). Internet of things – new security and privacy challenges. *ELSEVIER*.

Xubuntu.org. (2024). *Capítulo 1. ¿qué es xubuntu?* xubuntu.org.

Zimmermann, J. (2013). Cypherpunks. *Teknokultura*.

Álvarez Rojas, L. R. (2018). *Blockchain y bitcoin: Fundamentos esenciales*. Universidad Técnica Federio Santa María.

Glosario

API: (Interfaz de Programación de Aplicaciones) Es un software intermedio que tiene la función de comunicar a las aplicaciones entre sí, sirviendo como un mensajero que envía y traduce la comunicación de estas. 16

Bitcoin: Es una moneda virtual o criptomoneda que se utiliza para adquirir productos o servicios a través de internet. 12

Criptoanálisis: Estudia los métodos para romper los cifrados. 21

Criptografía: Se encarga de estudiar los métodos de cifrado. 21

Criptología: Es la rama que se encarga de estudiar la criptografía y el criptoanálisis. 25

DDoS: Es un tipo de malware que bloquea el equipo de la victima encriptando su contenido. El atacante suele pedir una recompensa para recuperar la información. 66

Escalabilidad: Es la capacidad de adaptación y respuesta de un sistema con respecto al rendimiento del mismo a medida que aumentan de forma significativa el número de usuarios de este. 68

Ethereum: Es una plataforma de código abierto basada en blockchain que permite construir criptomonedas y proyectos descentralizados. Cuenta con una criptomoneda nativa llamada Ether (ETH). 30

Machine Learning: Es una rama de la inteligencia artificial que se encarga de imitar de manera automática y precisa la forma en que los humanos aprenden. 58

Malware: Es cualquier software malicioso capaz de dañar dispositivos, robar información y causar pérdidas económicas al usuario u organización. Algunos tipos de malware son los virus, troyanos, spyware, ransomware, etc. 65

Metadatos: Son datos que sirven para describir grupos de otros datos, describen el contenido de los archivos o la información de estos. 55

Minerales conflictivos: Aquellos que fueron extraidos en medio de conflictos armados o en condiciones de abuso a los derechos humanos. 59

Peer to peer: La red igual a igual no necesita un servidor central para permitir la comunicación. Ambos hosts conectados pueden funcionar como cliente o servidor. 12

Privacidad: Es la capacidad de un individuo u organización de controlar y servar la recopilación y el uso que se hace de sus datos. 69

Ransomware: Es un ciberataque que desborda la capacidad del sitio de la vícitma enviando una cantidad masiva de solicitudes causando que no funcione correctamente o se sature el servicio. 66

Rendimiento: Se refiere a los resultados esperados en un determinado tiempo, en el cuál se espera obtener buenos resultados con poco trabajo. 68

SaaS: Software como servicio es un modelo basado en la nube que brinda aplicaciones a sus usuarios a través de un navegador o aplicación. 71

Sostenibilidad: Se refiere al cimplimiento de las necesidades presentadas sin comprometer la capacidad de las generaciones futuras de satisfacer las suyas, garantizando el equilibrio entre crecimiento económico, cuidado del medio ambiente y bienestar social. 68

Startup: Se define como aquella organización que desarrolla productos o servicios de gran inovación que son altamente demandados en el mercado. 59

Token: Es un activo físico o digital creado por una organización para utilizarse como modelo de negocio dentro de esta, ya que fuera de la organización no tiene ningún valor. 16

Siglas

AES Advanced Encryption Standard. 22

API Application Programming Interface. 16

DDoS Distributed Denial of Service. 66

DES Data Encryption Standard. 22

GDPR General Data Protection Regulation. 48

LFPDPPP Ley Federal de Protección de Datos Personales en Posesión de Particulares. 48

NIST National Institute of Standards and Technology. 25

NSA National Security Agency. 25

RSA Rivest, Shamir y Adleman. 23

SHA Secure Hash Algorithm. 25