UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

ANÁLISIS DEL DESEMPEÑO DE EQUIPO ASIC USADO PARA MINERÍA DE CRIPTOMONEDAS EN EL SALVADOR

PRESENTADO POR:

ROLANDO ALEXANDER ALVARADO ARIAS

ERICK ALEXANDER MEJÍA ALVARENGA

PARA OPTAR AL TITULO DE:

INGENIERO ELECTRICISTA

CIUDAD UNIVERSITARIA, SEPTIEMBRE 2025

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSC. JUAN ROSA QUINTANILLA

SECRETARIO GENERAL:

LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO:

ING. LUIS SALVADOR BARRERA MANCÍA

SECRETARIO:

ARQ. RAÚL ALEXANDER FABIÁN ORELLANA

ESCUELA DE INGENIERÍA ELÉCTRICA

DIRECTOR:

ING. WERNER DAVID MELÉNDEZ VALLE

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

Trabajo de graduación previo a la opción al grado de:

INGENIERO ELECTRICISTA

Titulo:

ANÁLISIS DEL DESEMPEÑO DE EQUIPO ASIC USADO PARA MINERÍA DE CRIPTOMONEDAS EN EL SALVADOR

Presentado por:

ROLANDO ALEXANDER ALVARADO ARIAS

ERICK ALEXANDER MEJÍA ALVARENGA

SAN SALVADOR, SEPTIEMBRE 2025

Trabajo de Graduación Aprobado por:

Docente Asesor:

ING. WALTER LEOPOLDO ZELAYA CHICAS

NOTA Y DEFENSA FINAL

En esta fecha, martes 8 de abril de 2025, en la Sala de Lectura de la Escuela de Ingeniería Eléctrica, a las 9:30 a.m. horas, en presencia de las siguientes autoridades de la Escuela de Ingeniería Eléctrica de la Universidad de El Salvador:

1. Ing. Werner David Meléndez Valle
   Director Interino

   Firma

2. MSc. José Wilber Calderón Urrutia
   Secretario

   Firma

ESCUELA DE INGENIERÍA ELÉCTRICA
DIRECCIÓN
FACULTAD DE INGENIERÍA Y ARQUITECTURA

Y, con el Honorable Jurado de Evaluación integrado por las personas siguientes:

- ING. WALTER LEOPOLDO ZELAYA CHICAS
  (Docente Asesor)

  Firma

- MSC. SALVADOR DE JESÚS GERMAN

  Firma

- ING. LUIS ERNESTO ESCOBAR BRIZUELA

  Firma

Se efectuó la defensa final reglamentaria del Trabajo de Graduación:

ANÁLISIS DEL DESEMPEÑO DE EQUIPO ASIC USADO PARA MINERÍA DE CRIPTOMONEDAS EN EL SALVADOR

A cargo de los Bachilleres:

- ALVARADO ARIAS ROLANDO ALEXANDER
- MEJÍA ALVARENGA ERICK ALEXANDER

Habiendo obtenido en el presente Trabajo una nota promedio de la defensa final: 8.4
(ocho punto cuatro)

Agradecimientos

Primeramente, agradezco a Dios por permitirme llegar a este punto final de la carrera, pero como dicen, ‘si Dios conmigo quien contra mí’. Las personas dicen que los superhéroes solo existen en las películas y yo siempre pensé eso, pero cuando vives en un país como El Salvador te das cuenta de que necesitas mucha ayuda para salir adelante, agradezco a Dios por ponerme a dos superhéroes en mi vida, este título universitario es para mis padres que me demostraron día a día que con esfuerzo que todo se puede conseguir, a mi mamá Maira Roxana Arias de Alvarado que la vi levantarse a las 4 de la mañana y llegar a las 6 de la tarde para que mi hermano y yo tengamos un mejor futuro, a mi papá José Rolando Alvarado Amaya que lo vi trabajar siempre, que me enseño que uno nunca debe decir que no puede hacer algo, siempre se puede aprender, a él que lo vi tener 2 trabajos para que yo pudiera estudiar, muchas gracias a los dos por todo.

También tengo que agradecer a mi familia, a mi hermano, Pedro Alvarado por estar conmigo siempre en toda mi vida, es con quien más he hablado y la persona en la que sé que siempre puedo confiar. Agradecer a mi abuelo, Juan por siempre estar ahí cuando más lo necesite, a mi abuela, Ana por siempre cocinar la mejor comida, a mi abuela, Mari, mis tíos y tías, es una gran familia que siempre me apoyo.

Agradezco a Dios porque puso personas muy buenas en mi camino, puso amigos buenos en la universidad, a Rodrigo Serrano, a mis amigos ingenieros Julio Flores, Oscar Vega, Juan Sánchez y a mi amigo y compañero de tesis Erick Alvarenga que estuvimos desde el primero año de la universidad estudiando para pasar las materias y finalizar esta carrera con amigos es mucho mejor.

Agradezco a personas buenas como don David Palma que me enseño electrónica y me insistió mucho por que aprendiera es de esas personas que hacen el bien sin esperar nada a cambio, siempre pienso que el país necesita más personas así. Agradezco a el ingeniero Walter Zelaya, nuestro asesor en esta tesis, que nos ayudó siempre para que este trabajo de graduación quedara de la mejor manera, a la niña Reinita que igual nos ayudó mucho y a los amigos y amigas que encontré al final de este camino que me apoyaron y han confiado en mí, muchas gracias.

Por último, pero no menos importante me agradezco a mí por no rendirme, porque todo esfuerzo es inútil si no crees en ti mismo.

ROLANDO ALVARADO

Agradecimientos

En primer lugar, quiero dar gracias a Dios y a la Virgen Santísima por brindarme la fortaleza, la inteligencia y la perseverancia necesarias para culminar esta etapa de mi vida. A mis padres, Rosa Yanira y José María, que ambos descansan en paz. Quienes con su esfuerzo y sacrificio hicieron posible que pudiera estudiar la carrera de Ingeniería Eléctrica en la Universidad de El Salvador. A mi hermano, Mario José, que siempre ha estado a mi lado apoyándome. Para mí ha sido una inmensa alegría que ambos hayamos compartido el sueño de formarnos en la Facultad de Ingeniería y Arquitectura.

A mi familia por su apoyo incondicional, en especial a mis abuelos, María Vidal y Miguel Ángel, quienes, ante la ausencia de mis padres, asumieron con amor la tarea de educarnos y de inculcarnos valores morales y religiosos.

Gracias a todos mis tíos y tías por su apoyo, comprensión y confianza, ya que sin su ayuda estudiar en la Universidad de El Salvador habría sido mucho más difícil. De manera especial, a mi tío, Juan Pablo, que descansa en paz, quien siempre estuvo pendiente de mí y de mi hermano, dándonos ánimo para seguir adelante en el estudio, gracias por todo, un fuerte abrazo hasta el cielo. También agradezco profundamente a mi tío, Jesús, por compartir conmigo su conocimiento en ingeniería y por estar siempre dispuesto a apoyarme, así como a mis tías, Marta Lilian y Blanca Alicia, quienes nunca dejaron de brindarnos su cariño y respaldo.

Mi próximo objetivo es seguir creciendo como profesional en el área de la distribución eléctrica, disfrutar la vida y compartir cada día con mi familia y mis amigos.

Por último, agradezco a mi compañero de trabajo de graduación y docente asesor por su paciencia, confianza y por los conocimientos que compartió con nosotros en todo este proceso, los cuales hicieron posible culminar este trabajo de graduación.

ERICK ALVARENGA

Contenido

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

La minería de criptomonedas se ha consolidado en la última década como una de las aplicaciones tecnológicas más relevantes que emplean la *blockchain* para gestionar sus datos, debido a sus ventajas en la validación de transacciones y en la seguridad de redes descentralizadas como Bitcoin. Este proceso requiere equipos especializados con gran potencia de cómputo, siendo los *Circuitos Integrados de Aplicación Específica* (ASIC) los más eficientes para ejecutar el algoritmo de consenso, "Prueba de Trabajo" (*Proof of Work, PoW*). Sin embargo, toda gran potencia de cómputo conlleva un gran consumo energético, lo cual, tanto en El Salvador como en el resto del mundo, ha dado lugar a un debate constante sobre su rentabilidad económica, impacto ambiental y sostenibilidad energética.

En este contexto, El Salvador se ha destacado como el primer país en el mundo en adoptar el Bitcoin como moneda de curso legal, en septiembre de 2021. Este hecho ha generado un gran interés en la minería de criptomonedas dentro del país. Sin embargo, esta adopción plantea interrogantes importantes, especialmente en relación con el uso de equipos ASIC. El consumo energético de estos dispositivos y su impacto en la infraestructura eléctrica local, junto con los costos asociados al consumo de energía, son aspectos cruciales para evaluar la rentabilidad de la minería en un país con condiciones energéticas particulares como las de El Salvador.

Con el objetivo de responder a estas interrogantes, se analizará el desempeño eléctrico y térmico del modelo Antminer S19 Pro, uno de los equipos ASIC más utilizados en la industria de la minería de Bitcoin. Para esto, se realizarán mediciones experimentales en condiciones reales de operación, con el fin de evaluar parámetros como el consumo eléctrico, la distorsión total armónica y la eficiencia energética del equipo, comparando los resultados obtenidos con los valores proporcionados por el fabricante. Además, se evaluará la calidad de la energía suministrada, un factor clave para asegurar la estabilidad y prolongar la vida útil del sistema de minería.

Con esta investigación, se busca contribuir al conocimiento académico y técnico sobre la minería de criptomonedas en el país, tomando como referencia los precios locales de energía eléctrica y los escenarios de rentabilidad de la minería de Bitcoin. Además, se pretende ofrecer un análisis que sirva como base para futuras investigaciones y proyectos relacionados con la minería de criptomonedas, proporcionando una base teórica y práctica para comprender los beneficios y limitaciones de la implementación de equipos ASIC en un entorno real.

OBJETIVOS

OBJETIVO GENERAL:

- Evaluar el desempeño de un equipo ASIC Antminer S19 Pro para minería de Bitcoin en El Salvador, considerando su eficiencia energética, potencia de cómputo, rentabilidad y adaptabilidad al contexto local.

OBJETIVOS ESPECÍFICOS:

- Analizar las características técnicas de los principales equipos de minería de criptomonedas usados en El Salvador como CPU, GPU y ASIC.
- Comparar el consumo energético de los equipos de minería en relación con el consumo promedio en El Salvador y los costos de la energía eléctrica.
- Evaluar la rentabilidad energética de la minería de criptomonedas en El Salvador, tomando en cuenta las fluctuaciones del mercado de criptomonedas y el precio de la electricidad en el contexto salvadoreño.
- Identificar las ventajas y desventajas del uso de equipos de minería en función del clima, disponibilidad de piezas de repuesto y soporte técnico en el país.

DEFINICIONES

Activo digital: Recurso en formato digital que puede almacenarse, transferirse o intercambiarse electrónicamente, cuya autenticidad y propiedad suele estar respaldadas por tecnología como la cadena de bloques y la criptografía.

Altcoin: Cualquier criptomoneda distinta a Bitcoin que puede basarse en el mismo protocolo original con modificaciones, o implementar innovaciones propias. Suelen proponer mejoras en velocidad de transacción, escalabilidad, algoritmos de consenso o características específicas orientadas a distintos usos.

Antminer S19 Pro: Equipo de minería ASIC de alto rendimiento fabricado por Bitmain, diseñado para minar Bitcoin con una *tasa de hash* de 110 TH/s y una alta eficiencia energética.

ASIC (*Application Specific Integrated Circuit*): Circuito integrado diseñado para realizar una tarea específica con alta eficiencia. En minería de criptomonedas, se utiliza para ejecutar funciones hash de forma mucho más rápida que CPUs o GPUs.

Billetera caliente (*Hot Wallet*): Software o aplicación conectada permanentemente a Internet que permite gestionar claves privadas de criptomonedas para realizar transacciones rápidas. Ofrece alta accesibilidad, pero presenta mayor exposición a riesgos de ciberseguridad.

Billetera fría (*Cold Wallet*): Dispositivo o medio de almacenamiento fuera de línea utilizado para resguardar claves privadas de forma segura. Reduce la exposición a ataques cibernéticos al no estar conectado a Internet, siendo idóneo para almacenamiento a largo plazo.

***Blockchain* (cadena de bloques):** Registro distribuido, descentralizado e inmutable en el que las transacciones se almacenan en bloques enlazados criptográficamente. Cada bloque contiene un conjunto de transacciones validadas, y su estructura garantiza transparencia, seguridad y resistencia a modificaciones no autorizadas.

Bloque: Unidad de datos en una *blockchain* que agrupa un conjunto de transacciones validas y verificadas, enlazadas criptográficamente al bloque anterior.

Clave privada: Código criptográfico único y secreto que permite autorizar transacciones y acceder a fondos almacenados en una billetera digital. Su resguardo es crítico para mantener la seguridad y propiedad de los activos digitales. Esto es comparable con un *password*.

Clave pública: Identificador derivado matemáticamente de la clave privada que puede compartirse libremente para recibir fondos. No permite el acceso a los fondos, pero se utiliza para verificar la autenticidad de las transacciones. Esto es un comparado a un *user*.

Descentralización: Distribución de funciones, control y toma de decisiones en un sistema sin depender de una autoridad central. En la *blockchain*, significa que la validación de transacciones y el almacenamiento de datos se llevan a cabo en múltiples nodos.

DLT (*Distributed Ledger Technology*): Tecnología de registro distribuido que mantiene datos sincronizados en múltiples ubicaciones y accesibles a todos los participantes autorizados. No requiere una autoridad central y garantiza la integridad de la información.

Distorsión Total Armónica (THD): Medida que cuantifica el contenido de armónicos en una señal eléctrica con relación a su componente fundamental. Se expresa como porcentaje y puede referirse a tensión (THDv) o corriente (THDi), siendo un parámetro relevante en calidad de energía.

Eficiencia energética (J/TH): Relación entre la energía consumida, medida en joules, y el número de terahashes a los que opera equipo de minería. Un valor más bajo indica mayor eficiencia.

Función *hash*: Algoritmo que convierte datos de cualquier tamaño en una cadena fija, única y unidireccional, usada para verificar la integridad de la información.

***Halving*:** Evento programado en la red Bitcoin que reduce a la mitad la recompensa que reciben los mineros por cada bloque validado. Ocurre cada 210,000 bloques, aproximadamente cada cuatro años, y tiene un impacto directo en la oferta monetaria y potencialmente en el precio del activo.

***Hashrate* (tasa de hash):** Velocidad con la que un equipo de minería ejecuta cálculos criptográficos necesarios para validar bloques. Se mide en hashes por segundo, siendo comunes múltiplos como gigahashes (GH/s), terahashes (TH/s).

Nodo completo (*Full Node*): Equipo que descarga, almacena y valida toda la cadena de bloques de una red. Participa en la verificación de transacciones y bloques, asegurando el cumplimiento de las reglas del algoritmo de consenso.

Nodo ligero (*Light Node*): Equipo o software que valida transacciones descargando únicamente los encabezados de los bloques, sin almacenar todo el historial de la *blockchain*. Reduce el consumo de recursos a cambio de depender de nodos completos para obtener datos.

Nonce: Número arbitrario que un minero modifica repetidamente para encontrar un *hash* de bloque que cumpla con el nivel establecido de *dificultad de la red*. Es un parámetro esencial del algoritmo Prueba de Trabajo (*Proof of Work*).

***Peer to Peer* (P2P):** Modelo de comunicación y transacción directa entre dos o más participantes sin intervención de intermediarios centralizados. En la *blockchain*, se permite el intercambio de activos de manera descentralizada.

Pool de minería: Agrupación de mineros que combinan su capacidad de cálculo para aumentar la probabilidad de encontrar bloques. Las recompensas obtenidas se distribuyen entre los participantes según la potencia de cómputo aportada.

Raíz de Merkle: Hash único que representa todas las transacciones incluidas en un bloque. Se genera a partir de un árbol de Merkle y sirve para verificar la integridad de los datos.

UTXO (*Unspent Transaction Output*): Salida de transacción no gastada en la red Bitcoin u otras criptomonedas basadas en el mismo modelo. Representa unidades de valor que pueden emplearse como entradas en transacciones futuras.

CAPÍTULO 1. LAS CRIPTOMONEDAS EN EL SALVADOR

Las criptomonedas representan una innovación significativa en el ámbito financiero global, caracterizadas por su sistema descentralizado y respaldadas por la tecnología *blockchain*. En El Salvador, el interés por las criptomonedas ha crecido en los últimos años desde que se legalizó el uso de Bitcoin. En el país, este fenómeno ha despertado debates sobre los desafíos económicos previos, el impacto social y las perspectivas a largo plazo, marcando un punto de partida para analizar cómo en realidad se comporta esta criptomoneda.

Existe una diferencia entre Bitcoin y bitcoin: cuando se refiere al dinero digital, a la criptomoneda, se le denomina *"*bitcoin*"* (en minúscula); en cambio, cuando se habla del sistema que respalda esta moneda se escribe *"*Bitcoin*"* con mayúscula inicial.

1.1 Historia de las criptomonedas

El surgimiento de las criptomonedas comenzó en las décadas de 1980 y 1990 con el movimiento *cypherpunk*, una corriente ideológica que promovía el uso de la criptografía como herramienta fundamental para proteger la libertad financiera. Uno de los primeros intentos fue cuando el criptógrafo David Chaum, en 1983, creó un sistema criptográfico llamado *eCash*, pensado como un concepto de efectivo electrónico anónimo, que permitía pagos electrónicos privados y seguros usando criptografía avanzada.

En 1998, Wei Dai propuso *B-money*, un sistema de efectivo electrónico anónimo y distribuido que describía un modelo sin intermediarios centralizados. Ese mismo año, Nick Szabo conceptualizó Bit Gold, un sistema de moneda digital descentralizada basado en la *"*Prueba de Trabajo*"* (*Proof of Work*). Aunque estos sistemas no llegaron a implementarse, sirvieron como base para que más adelante Satoshi Nakamoto utilizara estos conceptos en su criptomoneda (Jiongyu Song, 2022).

El punto de inflexión se dio en el año 2008 en un contexto de una profunda crisis financiera global y desconfianza en el sistema bancario, a través de una entidad o grupo anónimo bajo el seudónimo Satoshi Nakamoto se publicó un artículo llamado *Bitcoin: A peer-to-peer Electronic Cash System*, que describía un sistema de efectivo electrónico *peer-to-peer* sin necesidad de intermediarios, este documento de solo nueve páginas planteó por primera vez una cadena de bloques (*blockchain)* y

una nueva forma de dinero digital, presentando una solución que abordaba los desafíos de la descentralización (Jiongyu Song, 2022).

1.1.1 Surgimiento de Bitcoin

El 3 de enero de 2009, Satoshi Nakamoto minó el primer bloque de bitcoin, llamado "bloque génesis", iniciando la red Bitcoin. El mensaje que incluía este bloque era: *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*. Este mensaje es interpretado como una declaración de principios sobre la necesidad de un sistema financiero alternativo. Este primer bloque inauguró la *blockchain* con una recompensa de 50 bitcoins (García, 2023).

El 12 de enero de 2009 tuvo lugar la primera transacción Bitcoin entre Satoshi y Hal Finney. Aunque en ese momento los bitcoins carecían de un valor comercial relevante, antes de finalizar el año, 1 BTC (o bitcoins) se cotizaba en menos de un centavo de dólar estadounidense, considerando el costo energético requerido por un computador para resolver un bloque. El 22 de mayo de 2010 se realizó la primera compra en bitcoins: dos pizzas por 10,000 BTC, un hecho que quedó marcado en la historia y ahora se celebra cada año como el Bitcoin *Pizza Day* (Hankin, 2025).

El éxito inicial de Bitcoin dio paso al surgimiento de otras criptomonedas, comúnmente llamadas *altcoins.* En 2011 comenzaron a aparecer las primeras, con el objetivo de mejorar o adaptar la tecnología de Bitcoin a nuevos propósitos. En abril de 2011 se lanzó *Namecoin*, basada en el código de Bitcoin, diseñada para crear un servicio de registro de dominios DNS, demostrando que la *blockchain* podía aplicarse en otros campos más allá de las criptomonedas (R. Brown, 2024).

En términos regulatorios, muchos gobiernos aún no aceptan las monedas digitales, ya que las consideran mecanismos que pueden facilitar actividades ilícitas, dificultar la trazabilidad de los flujos financieros y generar desafíos en materia de supervisión y control. Un caso relevante es China, donde en 2013 el Banco Popular emitió una prohibición para que las instituciones financieras manejaran transacciones en Bitcoin, anticipándose a riesgos asociados con la estabilidad financiera y el control de capitales. Sin embargo, este enfoque restrictivo evolucionó significativamente, y en 2021 el gobierno chino endureció su postura al prohibir por completo el

uso, las transacciones, el minado y la negociación de criptomonedas, marcando un salto regulatorio importante en su política hacia las criptomonedas (Cade, 2014).

La gran transformación de las criptomonedas llegó con la concepción de Ethereum por Vitalik Buterin y su lanzamiento en 2015. Ethereum trascendió la función de moneda digital al introducir la capacidad de ejecutar contratos inteligentes en su *blockchain*, eliminando la necesidad de intermediarios y automatizando la ejecución de términos predefinidos. Ethereum no solo creó su propia criptomoneda, Ether (ETH), sino que se convirtió en una plataforma para la creación de aplicaciones descentralizadas y el desarrollo de nuevos *tokens*. Esta innovación marcó el inicio de la transformación del espacio criptográfico: de un sistema monetario a un ecosistema programable y multifuncional (Ortiz, 2023).

1.1.2 Actualidad y futuro de las criptomonedas

Las criptomonedas se han consolidado como parte del panorama financiero global, aunque con una evolución marcada por la volatilidad y la innovación continua. Bitcoin cuenta con la mayor base de usuarios y es la criptomoneda con mayor reconocimiento global, muestra de ello es que en 2021 El Salvador se convirtió en el primer país en declarar Bitcoin como moneda de curso legal.

En términos de marco regulatorio, la tendencia reciente es hacia una mayor calidad y supervisión. En 2023 el reglamento MiCa (*Markets in Crypto-Assets),* publicado por la Unión Europea establece un conjunto de reglas para la emisión y comercio de criptoactivos en todos los países miembros. Así mismo muchos otros países han emitido normas sobre el pago de impuestos de las criptomonedas y mecanismos de prevención de delitos financieros, reconociendo que este sistema presenta ciertas regulaciones. Aunque también existen países que si restringen fuertemente el uso de estos criptoactivos (García, 2023).

1.2 Funcionamiento de las criptomonedas

Las criptomonedas son activos digitales intangibles, cuyo funcionamiento se sustenta en mecanismos criptográficos que garantizan la integridad y seguridad de las acciones, además de regular la emisión de nuevas monedas, evitando la reproducción no autorizada. A diferencia de las monedas fiduciarias, las criptomonedas se caracterizan por su estructura descentralizada,

manejadas independientemente del control de gobiernos o instituciones financieras centralizadas. Su ecosistema económico se basa en protocolos de red *peer-to-peer* (*P2P*), donde las transacciones se registran y validan a través de una base de datos distribuida conocida como *blockchain*.

Una propiedad fundamental de las criptomonedas es el suministro controlado y decreciente, diseñada para imponer restricciones sobre la cantidad de unidades en circulación. En el caso de Bitcoin, el protocolo establece un límite absoluto de 21 millones de unidades. Esta escasez programada opera como un mecanismo deflacionario que, bajo condiciones de demanda sostenida, puede incentivar la apreciación del activo, replicando dinámicas observadas en mercados de bienes finitos, como los metales preciosos, particularmente el oro (Banco Santander, 2021).

1.2.1 *Blockchain*

La cadena de bloques o *blockchain* es una base de datos distribuida y descentralizada, diseñada para el registro inmutable y la verificación de transacciones digitales y activos. Su funcionamiento se sustenta en estructuras de datos enlazadas criptográficamente, garantizando la integridad, autenticidad y trazabilidad de la información, además de ofrecer resistencia frente a alteraciones no autorizadas mediante algoritmos criptográficos.

En los procesos de criptomonedas por ejemplo el bitcoin, la cadena de bloques actúa como un registro descentralizado y seguro. Esto significa que no posee una autoridad central o un intermediario que tenga un control total de datos o las transacciones que se generen con respecto a la criptomoneda. Esta descentralización se logra debido a su estructura que está conformada en bloques de información enlazados de forma cronológica y secuencial, lo que constituye el fundamento de su capacidad para mantener un ecosistema distribuido y seguro. La *blockchain* se basa en principios fundamentales que garantizan colectivamente su seguridad, confiabilidad y funcionalidad única (Zurdo, 2018).

Descentralización: Este principio establece que el control y la toma de decisiones se transfieren de una única entidad central a una red distribuida de computadoras participantes. Esta estructura distribuida garantiza la confianza, la validez y la usabilidad, ya que la información de cada bloque puede ser confirmada por todos los ordenadores participantes. Al eliminar los puntos únicos de

falla, la descentralización aumenta significativamente la resistencia a la censura o el control de cualquier entidad, fomentando un sistema más democrático e inclusivo (Kenneth Proctor, 2024).

Inmutabilidad: Una vez que los datos se registran en una cadena de bloques, no puede ser modificados ni eliminados. Esta característica crítica se logra vinculando bloques cronológicamente usando *hashes* criptográficos, donde cualquier alteración de un registro pasado rompería inmediatamente toda la cadena, haciendo que la discrepancia sea evidente en toda la red. Esto proporciona una pista de auditoría confiable y es crucial para prevenir el fraude y problemas como el "doble gasto" en monedas digitales (Kenneth Proctor, 2024).

Seguridad: *Blockchain* emplea técnicas avanzadas de *hash* criptográfico para asegurar cada bloque y transacción. Una función *hash* criptográfica toma datos de entrada de cualquier longitud y produce una cadena alfanumérica única de tamaño fijo, o *hash*, que actúa como una huella digital para esos datos. Se trata de un sistema unidireccional, lo que significa que es prácticamente imposible aplicar ingeniería inversa a la entrada original del *hash*, lo que garantiza la privacidad y la integridad de los datos. Además, las firmas digitales, que utilizan pares de claves públicas y privadas, añaden otra capa de seguridad, verificando el origen de la transacción y asegurando que su contenido no haya sido manipulado.

La tecnología *blockchain* ha experimentado una evolución significativa desde su surgimiento, dividiéndose en múltiples formas de implementación. Generalmente, las *"*Tecnologías de Registro Distribuido*"* (*Distributed Ledger Technologies*, *DLT*) se clasifican en tres tipologías principales: sistemas públicos, sistemas privados y sistemas híbridos. Cada uno de estos modelos presenta características distintivas en términos de acceso, control y grado de descentralización.

- **Sistema público:** los sistemas *blockchain* públicos son de acceso abierto, permitiendo que cualquier individuo se una a la red y participe en las transacciones sin necesidad de permisos. Esta arquitectura se caracteriza por una descentralización total, ya que ninguna entidad centralizada ejerce control sobre la red. Los nodos participantes pueden validar transacciones y contribuir a la adición de nuevos bloques a la cadena. Ejemplos emblemáticos de este tipo de red son Bitcoin y Ethereum, que representan las aplicaciones más reconocidas de *blockchain* público.

- **Sistema privado**: los sistemas *blockchain* privados imponen restricciones de acceso, limitando la participación a entidades previamente autorizadas. En este entorno, una organización central ejerce control sobre quién puede unirse a la red, validar transacciones y consultar los registros. Esta configuración es común en aplicaciones empresariales, donde las compañías utilizan *blockchain* privados para gestionar procesos internos, optimizar la eficiencia operativa y garantizar la integridad de los datos transaccionales.
- **Sistema híbrido**: los sistemas híbridos combinan elementos de las arquitecturas públicas y privadas, permitiendo acceso público a ciertos componentes de la red, mientras mantienen segmentos privados bajo control restringido. Esta combinación proporciona una mayor flexibilidad para adaptar la solución a las necesidades específicas de cada caso de uso, como sucede en aplicaciones de cadena de suministro, gestión de registros clínicos o plataformas gubernamentales.

En síntesis, la tecnología *blockchain* constituye una herramienta versátil para garantizar seguridad, transparencia y confiabilidad en una amplia variedad de aplicaciones, que abarcan desde las criptomonedas hasta la administración avanzada de datos. Su capacidad para eliminar intermediarios, proporcionar un registro inmutable de eventos y fortalecer la trazabilidad de las operaciones la convierte en un recurso estratégico de alto valor para numerosas industrias (Tapscott, 2016).

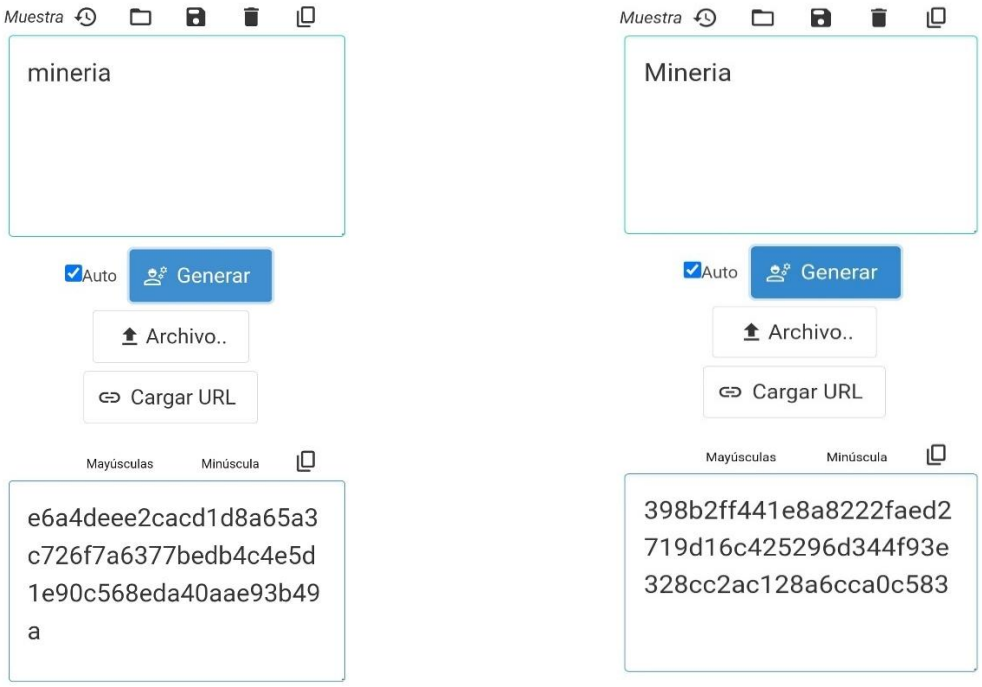
1.2.2 Función *hash*

Una función *hash* es un algoritmo que toma un número de cualquier tamaño o texto y las transforma en un número hexadecimal (es decir, en base 16, expresados con los dígitos 0-9 y los caracteres de la A-F) de un tamaño predeterminado que debe cumplir una serie de condiciones, tales como un bajo costo computacional, lo que significa que el valor *hash* se debe calcular de una manera rápida y eficiente. También en la conversión a números hexadecimal aplicado a cualquier entrada sin importar su cantidad de texto o números, debe cumplir exactamente con el mismo tamaño de *hash* (Aguilar, 2019).

El tamaño de una función *hash* va a depender del nivel de seguridad deseado. Así, por ejemplo, *SHA*-256 (*Secure Hash Algorithm, 256 bits*), da un resultado de 256 bits, con el cual se presenta

un número hexadecimal de 64 dígitos (cada número hexadecimal requiere 4 bits para almacenarse: $2^4 = 16$). Aunque también existen las funciones *SHA*-224 (para 56 dígitos), (96 dígitos) y *SHA 512* (128 dígitos). La función *SHA-256*, que es la función *hash* más reciente (publicada en 2015) de la familia *SHA3* la cual a su vez es publicada por el Instituto Nacional de Normas y Tecnología de Estados Unidos (Aguilar, 2019).

Una de las propiedades clave de las funciones *hash* criptográficas es que incluso pequeñas modificaciones en los datos de entrada, como el cambio de una letra de minúscula a mayúscula, generan salidas completamente diferentes. Esto se evidencia en la Figura 1.1, donde las entradas "minería" y "Minería" producen códigos *hash* distintos al ser procesadas con el algoritmo *SHA*-256.



(a) (b)

Figura 1.1 Codificación de datos con SHA-256: entrada "minería" y "Minería"

El *hash* es un versátil método criptográfico, utilizado en muchas aplicaciones como ocultar información de acceso o acreditación de cualquier elemento digital y la transforma en un conjunto de datos único. Dado que el robo de credenciales de usuario son el tipo de vulnerabilidades que más tardan en identificarse y contenerse, hasta 292 días según IBM (*International Business*

Machines), las funciones *hash* resultan esenciales para blindar la información y evitar pérdidas significativas para las empresas.

Las funciones y los valores *hash* son una parte fundamental en el campo de la criptografía y de gran utilidad en diversas aplicaciones, la más común es la verificación de contraseñas ya que en lugar de almacenar contraseñas en texto se encarga de organizar y almacenar *hash* de cada contraseña lo que quiere decir que cuando un usuario intenta iniciar sesión, el sistema calcula el *hash* de la contraseña ingresada y la compara con el *hash* almacenado en la base de datos, si esto coincide se le permite el acceso.

Otra herramienta de las funciones *hash* es la verificación de la integridad de los datos, cuando se transfieren archivos o almacena información en un sistema, se genera un valor *hash* de los datos originales. Este *hash* acompaña a los datos durante el envío o se almacena junto a ellos y al llegar a su destino o en caso de que se quiera verificar la integridad se recalcula el *hash* y se compara con el valor original, la coincidencia entre ambos asegura que los datos permanecen sin alteraciones. Además, las funciones *hash* desempeñan un papel crucial en la organización y recuperación eficiente de datos en sistema de almacenamiento y base de datos, facilitando un acceso rápido y seguro.

Estas funciones realizan una serie de operaciones matemáticas que transforman la entrada en una salida de longitud fija. Además, son unidireccionales, lo que implica que, dada la salida (el *hash*), computacionalmente es extremadamente costoso determinar la entrada original. Así, a partir de un valor *hash*, no se pueden descifrar los datos introducidos inicialmente, lo que es fundamental para garantizar la confidencialidad de la información.

1.2.3 Protocolo de consenso

En las redes *blockchain*, el protocolo de consenso representa el conjunto de reglas y mecanismos que permiten a los nodos participantes acordar el estado actual de la cadena de bloques. Este acuerdo distribuido es esencial para garantizar que las transacciones sean válidas, estén correctamente ordenadas y no puedan ser modificadas de manera arbitraria, todo sin la necesidad de una autoridad central.

El objetivo principal de un protocolo de consenso es mantener la coherencia y la seguridad del sistema incluso en presencia de actores maliciosos o fallos en los nodos. A continuación, se describen los tres mecanismos de consenso más representativos en el ecosistema *blockchain*, junto con sus características técnicas y ejemplos de implementación.

***Proof of Work* (*PoW*)**

El protocolo de Prueba de Trabajo (*Proof of Work*, *PoW*) es un mecanismo de consenso utilizado para validar transacciones y asegurar la integridad del libro mayor en redes *blockchain* descentralizadas. Este esquema se basa en la resolución de un problema computacionalmente complejo, cuya solución requiere una cantidad considerable de recursos y tiempo, lo que garantiza que solo los nodos con capacidad suficiente puedan proponer nuevos bloques válidos.

En la red Bitcoin, cada nodo agrupa transacciones recientes en un bloque candidato y compite con otros para resolver un desafío criptográfico basado en la función *hash SHA*-256. Este reto consiste en encontrar un valor que, al ser incluido en el bloque, produzca un *hash* que cumpla con ciertos requisitos de dificultad. Esta búsqueda implica un proceso de prueba y error intensivo que demanda poder de cómputo significativo.

Una vez que un nodo encuentra una solución válida, el bloque es transmitido a la red, verificado por otros nodos y, si es aceptado, se añade a la cadena de bloques. El nodo que propone el bloque es recompensado con una cantidad determinada de bitcoins, junto con las tarifas de transacción asociadas al bloque. Esta recompensa actúa como incentivo económico, promoviendo la participación y el uso sostenido de recursos computacionales para mantener la red operativa.

Este procedimiento se repite aproximadamente cada diez minutos, lo que permite mantener una frecuencia constante en la adición de nuevos bloques y en la sincronización del estado de la cadena en toda la red. En conjunto, el sistema *PoW* proporciona una base robusta para la verificación distribuida y transparente de las transacciones, apoyándose en el trabajo computacional como garantía de consenso.

Proof of Stake (*PoS*)

El protocolo de Prueba de Participación (*Proof of Stake*, *PoS*) es una alternativa al enfoque computacionalmente intensivo de la Prueba de Trabajo. En lugar de basarse en el poder de cómputo, *PoS* determina qué nodo tiene derecho a validar el siguiente bloque en función de la cantidad de activos digitales que posee y mantiene bloqueados (*staking*) dentro de la red.

El principio detrás de *PoS* es que los participantes con mayor participación económica tienen un mayor incentivo para actuar en beneficio de la red. Al eliminar la necesidad de resolver problemas criptográficos complejos, este mecanismo reduce considerablemente el consumo energético y la infraestructura técnica requerida para participar como validador.

El proceso comienza con la selección aleatoria o ponderada de validadores, quienes se encargan de verificar las transacciones y proponer nuevos bloques. Si el bloque propuesto es aceptado por los demás nodos, el validador recibe una recompensa, generalmente en forma de comisiones por transacción o emisiones programadas de tokens.

Un ejemplo notable de implementación de *PoS* es Ethereum, que, tras su transición desde *PoW*, introdujo un sistema en el que los validadores deben comprometer una cantidad mínima de 32 ETH para ser elegibles. Esta participación puede ser penalizada si el validador actúa de manera maliciosa o negligente, lo que introduce mecanismos de disuasión y refuerza la seguridad del sistema.

Delegated Proof of Stake (*DPoS*)

El protocolo de Prueba de Participación Delegada (*Delegated Proof of Stake*, *DPoS*) introduce un modelo basado en votación de todos los participantes para mejorar la eficiencia del consenso sin comprometer la seguridad de la red. En este protocolo, los participantes no validan bloques directamente, sino que delegan su poder de voto a un número limitado de representantes, llamados delegados o testigos.

Estos delegados son responsables de proponer y validar bloques de forma rotativa, siguiendo un calendario predefinido o un sistema de rondas. A diferencia de *PoS* tradicional, *DPoS* separa el papel económico del usuario del rol operativo del validador, lo que permite optimizar la velocidad de procesamiento y reducir la latencia en la confirmación de transacciones.

La selección de delegados está determinada por la cantidad de votos que reciben, los cuales están directamente relacionados con la cantidad de tokens que los usuarios poseen. Este sistema permite una representación proporcional, aunque introduce una forma de centralización funcional, ya que solo un subconjunto limitado de nodos tiene la capacidad de escribir en la cadena.

1.2.4 Árbol de Merkle

Un árbol de Merkle, llamado así en honor al profesor Ralph Merkle, es una estructura de datos jerárquica que utiliza funciones *hash* para organizar y verificar grandes volúmenes de información. En esta estructura, los datos se agrupan en pares y se les aplica un algoritmo *hash* para producir nuevos valores que representan combinaciones de los datos originales. Este proceso se repite en varios niveles, combinando los resultados *hash* anteriores en niveles superiores del árbol. La finalidad de este método es asegurar que cualquier modificación en los datos originales sea detectable al comparar los resultados de los cálculos *hash* a lo largo de la estructura (Rasuse, 2024).

El término "árbol" se utiliza para una estructura de datos ramificada, en la que los elementos se organizan jerárquicamente desde una base (hojas) hasta un único punto superior (raíz). En el caso de los árboles de Merkle, se componen de tres tipos de principales nodos: nodos hoja, nodos intermedios (o no hoja) y una raíz.

Los nodos hoja se ubican en la base del árbol y representan los *hashes* individuales de cada transacción en un bloque, conocidos como *TXID (Transaction ID* o en español como Identificador único de una Transacción*)*. Cuando se busca una transacción en un explorador de bloques, lo que se puede observar es el *hash* de dicha transacción.

Estos nodos se agrupan en pares, y cada par se combina para formar un nuevo nodo, aplicando una función *hash* sobre la concatenación de los dos *hashes* hijos. Los nodos generados en este proceso forman el siguiente nivel del árbol: los nodos intermedios. Aunque no contienen directamente los datos de las transacciones, sí almacenan un resumen *hash* de las combinaciones por debajo. A medida que se asciende en el árbol, el número de nodos se reduce a la mitad en cada capa.

A medida que se asciende en el árbol, cada capa de nodos intermedios se forma agrupando pares de nodos de la capa inferior, aplicando una función *hash* sobre la combinación de sus valores. Esto da lugar a una nueva capa con la mitad de los nodos que la anterior, haciendo que el árbol se

estreche progresivamente. Este proceso continúa hasta que quedan solo dos nodos en la última capa. La combinación final de estos dos valores, tras aplicar una última función *hash*, da origen al nodo superior del árbol: la raíz de Merkle (Rasuse, 2024).

Raíz de Merkle

La raíz de Merkle es el resultado final del proceso de *hashing* jerárquico aplicado sobre las transacciones de un bloque. Esta raíz actúa como un identificador criptográfico único que representa el estado agregado de todas las transacciones incluidas en dicho bloque. La estructura del árbol de Merkle, es posible verificar la validez de cualquier nodo hoja (es decir, cualquier *hash* de transacción) sin requerir el procesamiento del conjunto completo, lo que optimiza los procesos de verificación y reduce la carga computacional para los nodos participantes (Binance Academy, 2020).

Dentro del protocolo Bitcoin, la raíz de Merkle se incorpora directamente en el encabezado de cada bloque junto con otros campos esenciales como la versión del protocolo, el *hash* del bloque anterior, la marca de tiempo, la dificultad objetivo y el *nonce*. Cualquier modificación, inserción o eliminación de transacciones altera la estructura del árbol y, por ende, produce una raíz distinta. Esto permite detectar manipulaciones de manera eficiente y garantizar la inmutabilidad de los datos en la red.

La generación de la raíz sigue un procedimiento iterativo: cada transacción se *hashea* individualmente (aplicando *SHA*-256 dos veces), y luego los *hashes* se agrupan en pares, concatenan y se someten nuevamente a la función *hash*. Este proceso se repite hasta obtener un único *hash* superior que encapsula criptográficamente la totalidad del bloque. Satoshi Nakamoto destacó la importancia de esta estructura en el diseño de Bitcoin, ya que permite la validación distribuida sin la necesidad de confianza entre participantes, un principio fundamental en sistemas descentralizados (Rasuse, 2024).

Desde una perspectiva práctica, la raíz de Merkle representa el *hash* derivado de todas las transacciones incluidas en el bloque. Por ejemplo, en el bloque #854,046 de la red Bitcoin, la raíz de Merkle es:

4c825b4e6a4fea2ea96a1dd879ceff1f854d5be51fa01bb5fd4d95853db9f1bc

Este valor, como parte del encabezado, es uno de los elementos que se someten a una operación de *hash* doble utilizando *SHA*-256 (*SHA-256d*), generando así el *hash* del bloque:

00000000000000000005d886429368c23489583edfd77d0bfffecef8b570d00

Es importante señalar que este *hash* de bloque no forma parte del contenido del bloque en sí, sino que es calculado externamente y referenciado por el siguiente bloque en la cadena. Aunque conceptualmente distintos, tanto la raíz de Merkle como el *hash* de bloque cumplen funciones criptográficas críticas para asegurar la integridad de los datos y la continuidad de la cadena de bloques. (Rasuse, 2024)

1.2.5 Función de los árboles de Merkle en bitcoin

La utilización de árboles de Merkle no es de uso exclusivo en criptomonedas, su adopción se ha generalizado debido a su eficiencia para estructurar datos y permitir la verificación criptográfica de grandes volúmenes de información. Existen múltiples variantes de árboles de Merkle, adaptadas a diferentes objetivos de diseño y requisitos de seguridad. El protocolo de Bitcoin utiliza una versión ampliamente conocida de este tipo de estructura, razón por la cual se utiliza frecuentemente como referencia.

El cliente de Bitcoin no calcula un único *hash* a partir del bloque completo de datos de transacciones en una sola operación. En cambio, se realiza un proceso iterativo: se aplica la función *hash* individualmente a cada transacción (generalmente utilizando *SHA*-256 dos veces), y luego los resultados se agrupan en pares. Cada par concatenado se somete nuevamente a la función *hash*, y así sucesivamente, construyendo niveles superiores en la jerarquía del árbol. Este procedimiento continúa hasta obtener un único *hash* en el nivel superior. En el caso de que el número de transacciones en un bloque sea impar, la última transacción se duplica para mantener la simetría en el agrupamiento (Delton Rhodes, 2024).

La estructura resultante puede visualizarse como un árbol binario invertido: las hojas corresponden a los *hashes* de transacciones los nodos intermedios representan la combinación *hash* de sus respectivos hijos, y el nodo raíz es el *TXID* que representa criptográficamente todo el conjunto de transacciones del bloque. En aplicaciones prácticas, el árbol puede contener cientos o miles de

transacciones, aunque los esquemas visuales simplificados suelen limitarse a unos pocos niveles por motivos didácticos.

El proceso de construcción de un árbol de Merkle puede visualizarse como una estructura jerárquica binaria invertida. En el diagrama, cada nodo base marcado como "T" representa una *transacción* individual del bloque. A cada transacción se le aplica una función *hash* criptográfica para obtener los *nodos hoja*, indicados como "H". Estos *hashes* se agrupan en pares, se concatenan y se *hashean* nuevamente para formar los nodos intermedios, que actúan como ramas dentro del árbol (Rasuse, 2024).

Por ejemplo, en la Figura 1.2 se muestra que si un nodo desea verificar que la transacción T_D está incluida en el bloque, solo necesita conocer la raíz de Merkle $H_{ABCDEFGH}$ y un conjunto mínimo de *hashes* complementarios: H_{CD}, H_{AB} y H_{EFGH}. Utilizando estos valores, el nodo puede reconstruir el camino de *hashing* desde H_D hasta la raíz y comprobar su validez sin acceder al resto de las transacciones del bloque. Esta técnica se conoce como *Merkle proof*, y permite verificaciones eficientes con una cantidad logarítmica de datos respecto al número total de transacciones.

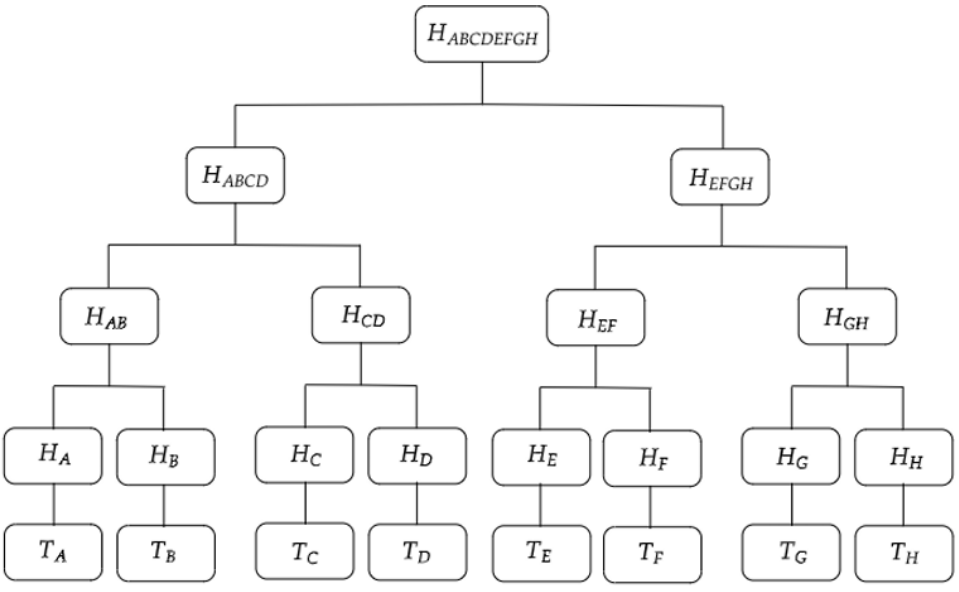


Figura 2.2 Árbol de Merkel

Los árboles de Merkle presentan una serie de ventajas clave en el contexto de sistemas distribuidos y, en particular, en redes *blockchain*. Una de sus propiedades más relevantes es que permiten la verificación de la pertenencia de una transacción a un bloque específico sin necesidad de descargar y procesar toda la cadena de bloques, cuyo tamaño puede superar varios cientos de gigabytes. Esta propiedad es esencial para los nodos ligeros (SPV, *Simplified Payment Verification*), que no almacenan la cadena completa pero aún pueden verificar transacciones con seguridad criptográfica.

1.3 Transacciones de criptomonedas

El proceso de una transacción de criptomonedas es un conjunto complejo de componentes interconectados que colaboran para garantizar la transferencia segura en un entorno distribuido. Desde el inicio en una billetera digital hasta la confirmación en la *blockchain*, cada paso es fundamental para mantener la integridad y seguridad del sistema.

1.3.1 Billeteras digitales (*wallets*)

Las billeteras de criptomonedas son herramientas, que permiten a los usuarios interactuar con redes *blockchain* y diseñadas para almacenar y gestionar las claves criptográficas privadas de un usuario. Estas claves otorgan acceso a los fondos digitales y permiten realizar operaciones como enviar, recibir y gastar criptomonedas. Es fundamental comprender que las billeteras no almacenan los bitcoins en sí, sino las claves privadas que proporcionan control sobre los activos registrados en la *blockchain*.

Hot wallets **(Billeteras calientes)**: Son aplicaciones de software que operan en dispositivos conectados a internet, como computadoras, teléfonos celulares o extensiones de navegador de internet. Ofrecen accesibilidad y facilidad de uso para transacciones frecuentes, pero están más expuestas a riesgos de seguridad debido a su conexión constante a la red.

Cold Wallets **(Billeteras Frías):** Son dispositivos físicos, como unidades USB especializadas, que almacenan las claves privadas en un entorno completamente desconectado de internet. Proporcionan un nivel superior de seguridad, siendo ideales para el almacenamiento a largo plazo de grandes cantidades de criptomonedas.

Cada billetera genera un par criptográfico único: una clave pública y una clave privada. La clave pública funciona como un identificador abierto similar a un número de cuenta bancaria y permite generar direcciones a las que otros pueden enviar fondos. La clave privada, en cambio, es un código secreto conocido únicamente por el propietario, indispensable para firmar digitalmente las transacciones y autorizar el uso de los fondos asociados a la clave pública. La pérdida de la clave privada implica la pérdida irreversible de acceso a los activos digitales, ya que no existe ninguna entidad central que pueda recuperar esos fondos.

La autonomía del usuario sobre sus activos digitales constituye uno de los pilares fundamentales de Bitcoin, eliminando la necesidad de intermediarios financieros. No obstante, esto conlleva una responsabilidad directa: el resguardo seguro de las claves privadas recae exclusivamente en el usuario. Sin mecanismos externos de recuperación, la seguridad personal se convierte en un factor crítico dentro del ecosistema Bitcoin (Bitpanda, s.f.).

1.3.2 Nodos y mineros

Los nodos son entidades computacionales que ejecutan el protocolo Bitcoin, manteniendo una copia completa y actualizada de la *blockchain*. Estos nodos validan transacciones y bloques, verifican el cumplimiento de las reglas del mecanismo de consenso y propagan información a través de la red *peer-to-peer*, asegurando así la coherencia y consistencia global de los datos sin depender de ninguna autoridad centralizada. Los nodos pueden implementarse en diversos entornos de hardware, desde estaciones de trabajo personales hasta servidores dedicados y configuraciones especializadas de alto rendimiento.

Existen distintos tipos de nodos:

- Nodos completos (*full nodes):* almacenan y validan todo el historial de la *blockchain*, verificando todas las reglas de consenso.
- Nodos ligeros *(light nodes):* utilizan una verificación simplificada *(SPV, Simplified Payment Verification)* que solo descarga encabezados de bloques y delega ciertas comprobaciones a nodos completos.
- Nodos mineros *(mining nodes):* son nodos completos que además participan activamente en la creación de nuevos bloques mediante el proceso de minería.

Los mineros son nodos especializados que participan en el proceso de validación y consolidación de bloques dentro de la red Bitcoin mediante el mecanismo de Prueba de Trabajo. Este proceso consiste en la resolución computacional de problemas criptográficos, específicamente el cálculo de un *hash* que cumpla con los requisitos de dificultad establecidos por la red. El primer minero en encontrar una solución válida obtiene el derecho exclusivo de añadir el siguiente bloque a la *blockchain*. Como incentivo económico, el minero ganador recibe una recompensa de bloque, compuesta por una cantidad predeterminada de nuevos bitcoins más las tarifas acumuladas de las transacciones incluidas en dicho bloque (Bitpanda, s.f.).

1.3.3 Entradas y Salidas de Transacción No Gastadas (*UTXO*)

El modelo contable utilizado en Bitcoin se denomina *UTXO* (*Unspent Transaction Output*), y representa una desviación significativa del sistema tradicional basado en saldos de cuenta. A diferencia de los sistemas centralizados donde se registra un saldo global asociado a cada cuenta, el modelo *UTXO* considera cada unidad de Bitcoin como una salida individual no gastada de una transacción previa. Estas salidas, o *UTXOs*, son indivisibles en términos de gasto: una vez referenciadas en una transacción posterior, se consideran completamente consumidas.

En la construcción de una transacción, el emisor debe seleccionar uno o más *UTXOs* como entradas, cuya suma sea suficiente para cubrir el monto del envío más las comisiones correspondientes. Posteriormente, la transacción genera nuevas salidas: una que transfiere el valor deseado al receptor y, opcionalmente, otra que retorna el excedente a una dirección controlada por el remitente. Esto permite una trazabilidad clara y verificable en la cadena de bloques, garantizando que cada fracción de Bitcoin proviene de una transacción anterior válida.

El saldo efectivo de un usuario, por tanto, no se encuentra centralizado en una cuenta única, sino que está distribuido entre los distintos *UTXOs* no gastados que controla. Esta lógica opera de manera distinta al manejo de efectivo físico: al realizar un pago con un billete de alta denominación, se recibe el cambio en billetes de menor valor. De esta forma, el modelo *UTXO* no solo garantiza la integridad de los fondos, sino que también introduce una flexibilidad operativa compatible con entornos descentralizados y sin intermediarios (Bitpanda, s.f.).

1.3.4 Etapas de las transacciones con una criptomoneda

El proceso de realizar una transacción en una red de criptomonedas como Bitcoin está compuesto por una serie de etapas técnicas que permiten garantizar la seguridad, trazabilidad y validez descentralizada de las operaciones. A continuación, se describen en detalle las etapas principales de dicho proceso.

1. Generación de la billetera digital

El primer paso consiste en que el usuario genere una billetera digital, que funciona como su interfaz personal con la red *blockchain*. Al instalar una aplicación o software especializado, el sistema crea una o más direcciones públicas, las cuales se derivan criptográficamente de claves privadas únicas. Estas claves privadas deben mantenerse en secreto, ya que son necesarias para autorizar cualquier operación. Las direcciones públicas pueden compartirse libremente y actúan como identificadores para recibir fondos (Antonopulos, 2010).

2. Creación de la transacción

Una vez que el usuario desea enviar criptomonedas, selecciona la dirección de origen (es decir, una donde tenga fondos disponibles) y define la cantidad a transferir hacia la dirección del destinatario. Las transacciones en Bitcoin, por ejemplo, utilizan *salidas de transacciones no gastadas* (*UTXOs*) como entradas. Esto implica que se hace referencia a fondos previamente recibidos que aún no han sido utilizados. El usuario puede incluir una comisión voluntaria destinada a motivar a los mineros a priorizar su transacción para ser incluida en el siguiente bloque.

3. Firma digital de la transacción

La transacción, antes de ser transmitida a la red, debe ser firmada digitalmente con la clave privada correspondiente a la dirección emisora. Esta firma tiene varias funciones esenciales: verifica que el emisor posee realmente los fondos, garantiza la integridad de los datos contenidos en la transacción, y evita que se puedan modificar sin invalidar la firma. Al completarse esta firma, la transacción adquiere validez técnica y puede ser enviada a la red de nodos.

4. Propagación a la red y almacenamiento en la *mempool*

Una vez firmada, la transacción es propagada a la red de nodos de la criptomoneda. Cada nodo recibe la transacción y la somete a una serie de validaciones de acuerdo con las reglas del protocolo. Si es válida, la transacción es almacenada en una estructura temporal llamada *mempool* (memory pool o en español *pool de memoria*). Cada nodo mantiene su propia *mempool*, por lo que el contenido puede variar entre nodos. En este punto, la transacción está lista para ser seleccionada por los mineros.

5. Selección de transacciones por los mineros

Los mineros escogen de la *mempool* aquellas transacciones que desean incluir en el siguiente bloque. Como el tamaño de los bloques es limitado, no pueden incluir todas, por lo que generalmente priorizan aquellas con comisiones más altas. Esto da lugar a un sistema de mercado competitivo donde las comisiones fluctúan en función de la demanda (Antonopulos, 2010).

6. Minado y resolución del problema criptográfico

El proceso de minado consiste en que los mineros compiten por resolver un problema matemático, conocido como Prueba de Trabajo. Esto implica encontrar un hash válido que cumpla con el nivel de dificultad ajustado por la red. El primer minero en encontrar la solución válida es quien tiene derecho a añadir un nuevo bloque a la cadena de bloques. Este bloque incluirá las transacciones seleccionadas y validadas, y el minero será recompensado con una cantidad fija de criptomoneda (recompensa por bloque) más las comisiones asociadas.

7. Inclusión en la *blockchain* y confirmaciones

El bloque minado es transmitido a la red y verificado por los demás nodos. Una vez validado, se añade de manera permanente a la cadena de bloques. La transacción incluida se considera ahora confirmada. Cada nuevo bloque añadido después de ese punto representa una confirmación adicional. Cuantas más confirmaciones acumula una transacción, más difícil es revertirla, lo que garantiza su seguridad e irreversibilidad.

Este conjunto de etapas, desde la creación de la cartera digital hasta la confirmación de la transacción en la cadena de bloques, se encuentra representado de forma esquemática en la Figura 1.3, la cual ilustra visualmente el flujo completo de una transacción dentro de la red Bitcoin. Dicha figura permite comprender los componentes y procesos involucrados, incluyendo la firma criptográfica, la verificación por los nodos, y la actividad minera para la validación y registro definitivo en la *blockchain* (Antonopulos, 2010).

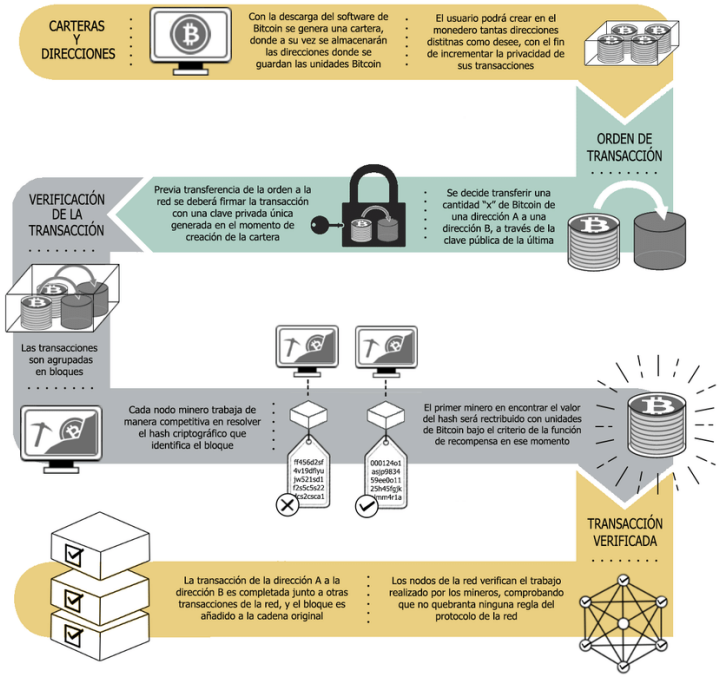


Figura 3.3 Proceso de una transacción en Bitcoin.

1.4 Proceso de minería de criptomonedas

La minería de criptomonedas constituye un componente esencial en las redes *blockchain*, particularmente en aquellas basadas en *PoW*, como Bitcoin. Este proceso consiste en la ejecución intensiva de operaciones computacionales, mediante las cuales se resuelven algoritmos criptográficos que permiten validar y registrar nuevas transacciones en la cadena de bloques.

Los participantes de la red, comúnmente denominados mineros, operan equipos especializados integrando hardware de alto rendimiento y software optimizado que garantizan la integridad, seguridad y descentralización del sistema. La selección del equipo adecuado depende de las características técnicas de la criptomoneda objetivo, considerando factores como la dificultad de

minado, el algoritmo de consenso y el consumo energético, a fin de maximizar la eficiencia operativa.

El propósito central de la minería es garantizar que las transacciones sean verificadas correctamente y que solo datos válidos sean añadidos al registro distribuido, previniendo amenazas. A través del proceso *PoW*, los mineros compiten por encontrar soluciones válidas a complejos cálculos, lo cual, al ser alcanzado, les otorga el derecho de incorporar un nuevo bloque a la *blockchain*. En sistemas como Bitcoin, esta acción es además incentivada con recompensas en forma de nuevas unidades monetarias y comisiones por transacción (JeFreda R Brown, 2024).

1.4.1 Minería en Bitcoin

En el funcionamiento de la red Bitcoin, los mineros desempeñan un papel fundamental al encargarse de validar las transacciones y registrarlo en la *blockchain*. Esta actividad, cumple una función crítica en la estabilidad, seguridad y descentralización del sistema. A través del proceso de minado, los mineros consolidan las transacciones no confirmadas en estructuras denominadas bloques y compiten entre sí para validar dichos bloques conforme a las reglas del protocolo.

El proceso de minado inicia con la recopilación de transacciones pendientes almacenadas en la *mempool* de la red. Estas transacciones han sido enviadas por los usuarios, pero aún no han sido confirmadas ni registradas de forma definitiva. Los mineros seleccionan y agrupan estas transacciones para conformar un bloque candidato, el cual representa una propuesta técnica para ser añadido como el próximo elemento de la cadena. La selección de transacciones suele priorizar aquellas que ofrecen comisiones más elevadas, dado que estas tarifas representan una parte significativa de la recompensa que el minero recibe por validar y anexar el bloque. Este criterio de selección optimiza los incentivos económicos inherentes al protocolo de *Proof of Work* (Euny Hong, 2024).

1.4.2 Resolución del *nonce*

Esta etapa representa la fase más competitiva y computacionalmente intensiva del proceso de minado en Bitcoin. Los mineros compiten entre sí para encontrar un valor de *nonce* (*number only used once*), un número que, al combinarse con los datos del bloque y procesarse mediante la

función criptográfica *SHA*-256, genera un *hash* que sea igual o inferior a un umbral definido por la dificultad de la red. Este procedimiento se basa en un enfoque de prueba y error, en el que los mineros modifican iterativamente el *nonce* y recalculan el *hash* del bloque hasta obtener un valor que cumpla con el criterio de dificultad.

La cantidad de intentos posibles por segundo se conoce como *hashrate* o "tasa de hash" y determina la capacidad de cómputo de un minero. Cuanto mayor sea esta tasa, mayor será la probabilidad de encontrar el *nonce* válido antes que los demás participantes de la red. Sin el *nonce*, el *hash* de salida de los datos del bloque sería un único valor, lo cual imposibilitaría el ajuste necesario para cumplir con los parámetros dinámicos de dificultad impuestos por el protocolo de consenso (Euny Hong, 2024).

1.4.3 Validación y adición de nuevos bloques a la cadena

Una vez que un minero encuentra un *nonce* válido y genera un *hash* que satisface el umbral de dificultad impuesto por la red, el bloque candidato es enviado a todos los nodos participantes. Cada nodo verifica de forma independiente la validez del bloque, comprobando la integridad de las transacciones incluidas, la coherencia del *hash* del bloque anterior y la validez del nuevo *hash* frente al criterio de dificultad.

Si el bloque cumple con todas las reglas del protocolo, es aceptado por la red y se añade a la cadena de bloques como parte de la secuencia principal. Debido a la naturaleza descentralizada del sistema y al uso de funciones criptográficas irreversibles, el bloque se convierte en un elemento permanente e inmutable de la *blockchain*, sirviendo como base para la construcción de los bloques futuros.

1.4.4 Ajuste de dificultad de minado

Uno de los mecanismos fundamentales del protocolo de Bitcoin es el ajuste automático de la dificultad de minado, diseñado para mantener constante el intervalo promedio entre bloques. Este ajuste ocurre cada 2016 bloques, aproximadamente cada dos semanas, y depende directamente de la *tasa de hash* total de la red.

Si el tiempo promedio para minar un bloque durante ese período es inferior a 10 minutos, la dificultad se incrementa con el objetivo de desacelerar la producción de bloques. Por el contrario, si la red se desacelera debido a una reducción en la participación de mineros, la dificultad disminuye. Este sistema garantiza que los bloques se añadan a la *blockchain* a intervalos regulares, independientemente de las fluctuaciones en la capacidad computacional de la red.

Además de estabilizar el tiempo de generación de bloques, el ajuste de dificultad actúa como un regulador económico interno. A medida que el valor de Bitcoin cambia, la rentabilidad del minado varía, lo que influye en la entrada o salida de mineros. Este ciclo de retroalimentación crea un equilibrio dinámico entre dificultad, participación y rentabilidad, influyendo directamente en las decisiones operativas y estratégicas dentro de la industria minera (Euny Hong, 2024).

1.4.5 Recompensas por bloque y *halving*

Los mineros de Bitcoin son incentivados mediante dos mecanismos principales: el subsidio por bloque y las tarifas de transacción. El subsidio por bloque consiste en una cantidad fija de bitcoins generados con cada nuevo bloque minado, asignada directamente al minero que consigue añadirlo a la *blockchain.* Esta emisión controlada forma parte de la política monetaria deflacionaria diseñada en el protocolo original de Bitcoin. El segundo componente son las tarifas de transacción, que los usuarios adjuntan voluntariamente a sus operaciones con el fin de priorizar su inclusión en la *blockchain*. El minero que valide el bloque obtiene la totalidad de las tarifas asociadas a las transacciones que decida incluir.

Para que todo esto sea regulable existe el *halving* el cual es un evento programado en el protocolo de Bitcoin que ocurre cada 210,000 bloques (aproximadamente cada cuatro años), reduciendo a la mitad el subsidio por bloque. Su objetivo es disminuir progresivamente la tasa de emisión de nuevas monedas, hasta alcanzar el límite máximo de 21 millones de bitcoins.

Este mecanismo establece una política monetaria deflacionaria, en contraste con los sistemas fiduciarios. Al reducir la oferta de nuevos bitcoins, el *halving* tiende a influir en el valor percibido del activo, promoviendo escasez y reforzando su carácter de reserva de valor. Es un elemento clave en la estructura económica de Bitcoin y una de las principales razones detrás de su comportamiento cíclico en los mercados financieros (Euny Hong, 2024).

Se estima que el ultimo Bitcoin se minara alrededor del año 2140, llegando al final del *halving*, actualmente la recompensa por bloque minado es de 3.125 BTC, según la Tabla 1.1 donde vemos la cantidad de *halving* que han ocurrido hasta la fecha. Una vez llegado al año 2140 los mineros ya no dependerán de los Bitcoins recién generados como incentivo, sino únicamente de las comisiones por transacción. Esta transición implica un cambio significativo en el modelo económico para los mineros a largo plazo, donde se cuestiona la estabilidad de las tarifas de transacción y la congestión de la red para mantener suficientes incentivos que aseguren la red en el futuro distante.

Año del *halving*	**Bloque del *halving***	**Recompensa por bloque en bitcoins**	**Evento**
2009	Bloque Génesis	50 BTC	Inicio
2012	210.000	25 BTC	1° *halving*
2016	420.000	12.5 BTC	2° *halving*
2020	630.000	6.25 BTC	3° *halving*
2024	840.000	3.125 BTC	4° *halving*
2028 (Estimado)	1.050.000	1.5625 BTC	5° *halving*

Tabla 1.1 Evolución de la recompensa por bloque de Bitcoin

1.4.6 Métodos de minado de criptomonedas

Existen distintas formas de participar en el proceso de minado, cada una con implicaciones técnicas, económicas y operativas específicas. La elección del método depende de factores como la disponibilidad de recursos, el nivel de conocimiento técnico, la tolerancia al riesgo y las expectativas de rentabilidad.

Minado individual (*solo mining*)

La minería en solitario consiste en la operación independiente de un nodo minero que intenta resolver bloques sin colaborar con otros participantes. En este modelo, el minero asume la totalidad

del proceso de validación y, en caso de éxito, recibe el 100 % de la recompensa del bloque, incluyendo el subsidio correspondiente y las tarifas asociadas a las transacciones incluidas.

Sin embargo, la minería en solitario implica una inversión inicial considerable en hardware especializado y un consumo energético constante. En el contexto actual de alta dificultad y competencia global, la probabilidad de que un minero individual resuelva un bloque es extremadamente baja, lo que genera ingresos variables y poco predecibles. Los períodos sin recompensa pueden ser prolongados, lo que convierte esta modalidad en una opción viable solo para operadores con una *tasa de hash* sustancial y una alta tolerancia al riesgo.

Minería en grupo (*pool mining*)

La minería en grupo, o *pool mining*, es una estrategia colaborativa en la que varios mineros combinan su capacidad de procesamiento para aumentar colectivamente sus probabilidades de validar bloques. Al integrarse en un *pool*, cada minero contribuye con una fracción de potencia computacional, y las recompensas obtenidas se distribuyen entre los participantes según su contribución relativa, siguiendo el esquema definido por el operador del *pool*.

Esta modalidad se ha convertido en el estándar de la industria, especialmente desde que la dificultad de minado superó las capacidades individuales de muchos mineros. Participar en un *pool* permite obtener ingresos más regulares y estables, aunque proporcionalmente menores, a cambio de reducir la varianza y la incertidumbre propias de la minería en solitario.

La mayoría de los *pools* aplican una tarifa de operación sobre las recompensas distribuidas, destinada a cubrir los costos de mantenimiento de la infraestructura compartida. Esta estructura ha facilitado la participación de mineros con recursos limitados, aunque también ha generado cierta preocupación en torno a la concentración de la tasa de *hash* en unos pocos *pools* de gran escala.

Minería en la nube *(cloud mining*)

La minería en la nube es un modelo que permite participar en la minería de criptomonedas sin necesidad de adquirir ni operar equipos físicos. En lugar de montar una infraestructura propia, el usuario alquila una cierta tasa de hash (*hashrate*) a empresas especializadas que operan centros de datos dedicados exclusivamente a actividades de minería.

El acceso a este servicio se realiza mediante contratos generalmente de duración fija en los que el usuario paga una tarifa proporcional a la potencia contratada. A cambio, recibe una parte de las criptomonedas generadas, según su participación en el total de capacidad operativa de la empresa. Este modelo elimina la necesidad de gestionar directamente el hardware, los costos energéticos, el mantenimiento técnico o los sistemas de refrigeración, reduciendo así las barreras de entrada para nuevos participantes.

Entre los actores reconocidos del sector se encuentran empresas como Genesis Mining y plataformas como Binance, las cuales han ofrecido servicios de minería en la nube en distintos momentos. Sin embargo, la dinámica del mercado y las condiciones regulatorias hacen que la disponibilidad y confiabilidad de estos servicios varíen con el tiempo, por lo que es fundamental realizar una evaluación exhaustiva antes de aportar recursos en este modelo (Mining Bitcoin, s.f.).

1.4.7 Seguridad en la minería y prevención del doble gasto

El doble gasto consiste en la posibilidad de utilizar una misma moneda en más de una transacción de forma fraudulenta. A diferencia del dinero físico, que no puede ser replicado digitalmente, los activos digitales son susceptibles a la copia y reutilización, lo que plantea un desafío fundamental en el diseño de monedas electrónicas seguras.

En los sistemas financieros tradicionales, una autoridad central actúa como intermediario de confianza para verificar, registrar y evitar este tipo de inconsistencias. Sin embargo, en criptomonedas descentralizadas como Bitcoin, donde no existe una entidad centralizada, se requiere una solución alternativa que garantice la integridad de las transacciones. En su propuesta original, Satoshi Nakamoto planteó que el problema del doble gasto podía resolverse marcando temporalmente las transacciones (*timestamping*) y encadenándolas mediante funciones criptográficas, de manera que cada bloque confirmara el anterior dentro de una estructura verificable.

Para que este mecanismo funcione eficazmente, es necesario contar con una red distribuida robusta y suficientemente rápida que mantenga el consenso sobre el estado de la cadena. Redes como Bitcoin y Ethereum han logrado mitigar el riesgo de doble gasto gracias a su elevada descentralización y poder computacional o *tasa de hash* (Freeman Law, 2023).

No obstante, el ataque más crítico relacionado con el doble gasto en redes de *blockchain* es el denominado ataque del 51%. Este se produce cuando un actor (o grupo coordinado) logra controlar más del 50% de la tasa de *hash* en un sistema *PoW*, o de los mecanismos de validación en otras variantes de consenso. En este escenario, el atacante puede alterar el orden de las transacciones, excluir operaciones legítimas y revertir pagos previamente confirmados, posibilitando el doble gasto.

Este tipo de ataque resulta más factible en redes con bajo nivel de participación o que han experimentado bifurcaciones recientes, ya que cuentan con una menor tasa de hash o un número reducido de mineros. En contraste, en redes como Bitcoin, el costo computacional y energético necesario para alcanzar dicho control es tan elevado que vuelve el ataque económicamente inviable (Freeman Law, 2023).

1.5 Ley Bitcoin y proyecto de minería en El Salvador.

El 8 de junio de 2021, la Asamblea Legislativa de El Salvador recibió una propuesta enviada por la ministra de Economía, María Luisa Hayem Brevé, que contenía un proyecto de decreto legislativo denominado "Ley Bitcoin". Este documento, compuesto por 16 artículos, fue recibido y enviado a la Comisión Financiera durante la sesión plenaria ordinaria n.º 7 celebrada ese mismo día. La comisión emitió el dictamen favorable n.º 3, y el 9 de junio de 2021, la Ley Bitcoin fue aprobada con 62 votos a favor (Asamblea Legislativa, 2021).

Este marco regulatorio representa el primer precedente a nivel internacional que establece el uso del Bitcoin como medio de pago con carácter de moneda de curso legal y poder liberatorio dentro de un territorio nacional. La legislación fue aprobada apenas cinco horas después de su presentación, tras una discusión que no superó las 2 horas y 21 minutos. La normativa tiene como finalidad explícita la promoción de la inclusión financiera de la ciudadanía salvadoreña y estipula el reconocimiento del Bitcoin como moneda de curso legal sin limitaciones en transacciones del ámbito público y privado, conforme lo estipula el Artículo I del Decreto Legislativo n.º 57 (Rivas, 2024).

1.5.1 implementación y recepción publica de bitcoin en El Salvador

El 7 de septiembre de 2021 entró en vigor la *Ley Bitcoin*, convirtiendo a El Salvador en el primer país del mundo en adoptar el Bitcoin como moneda de curso legal junto al dólar estadounidense. La propuesta, canalizada a través del Ministerio de Economía y aprobada por la Asamblea Legislativa, fue presentada oficialmente como *Proyecto de la Ley Bitcoin en El Salvador* (Rivas, 2024).

Los resultados de un estudio realizado por el Banco Mundial sobre la economía digital en El Salvador para el año 2022, muestra que casi el 50% de la población salvadoreña no hace uso de Internet, a pesar de que hay más de 11.6 millones de líneas móviles activas, según la Superintendencia General de Electricidad y Telecomunicaciones. Un dato que aproxima la cantidad de celulares que circulan en un país con 6.3 millones de personas (Alemán, 2022).

Para fomentar la adopción, el Estado implementó la aplicación de billetera digital *Chivo Wallet*, la cual ofrecía un incentivo inicial de US$ 30 en Bitcoin a cada ciudadano que la descargara. Simultáneamente, el gobierno adquirió entre 200 y 400 BTC mediante un fideicomiso público respaldado con US$ 150 millones, destinado a garantizar la conversión automática entre Bitcoin y dólares estadounidenses (BBC News Mundo, 2021).

Como parte del despliegue logístico, se instalaron más de 200 cajeros automáticos de uso exclusivo para la aplicación, permitiendo retiros sin comisiones, con el objetivo de facilitar el acceso a la moneda digital y promover la inclusión financiera. Según estimaciones realizadas durante los primeros 100 días de la implementación, entre el 46 % y 56 % de la población descargó la aplicación; sin embargo, únicamente entre el 36 % y 40 % continuó utilizándola de forma regular, mientras que un número considerable de usuarios accedió a la plataforma una sola vez para cobrar el bono inicial (BBC News Mundo, 2021).

1.5.2 Impacto del bitcoin en la economía de El Salvador

El gobierno de El Salvador promovió la adopción del Bitcoin bajo una narrativa de transformación económica, centrada en la promesa de aumentar la inclusión financiera, atraer inversión extranjera y reducir los costos de envío de remesas. No obstante, la adopción de esta moneda en un inicio generó mucha incertidumbre en la población. Diversos informes señalaron que el desconocimiento

sobre el uso de criptomonedas y la percepción de obligatoriedad en su aceptación provocaron una reacción negativa, especialmente en los primeros meses de aplicación de la ley (Fordham, 2022).

En términos cuantitativos, el impacto del Bitcoin sobre el flujo de remesas ha sido marginal. Según datos del Banco Central de Reserva de El Salvador, entre septiembre de 2021 y julio de 2022 ingresaron al país aproximadamente US$ 130.83 millones en remesas a través de billeteras digitales basadas en criptomonedas, lo que representó apenas un 1.8 % del total de remesas registradas (US$ 7,043.66 millones) en ese mismo periodo. El mes con mayor recepción por esta vía fue octubre de 2021, cuando se contabilizaron US$ 29.68 millones (4.67 %), pero esa cifra descendió gradualmente a niveles mensuales que oscilaron entre los US$ 12.57 y US$ 9.39 millones. Estos datos reflejan que, pese a los esfuerzos institucionales, el uso de Bitcoin para remesas no logró consolidarse como una práctica extendida o sostenida entre la diáspora salvadoreña (Cantizzano, 2022).

A nivel internacional, instituciones financieras se mostraron reservadas frente a lo que estaba pasando en El Salvador. El Fondo Monetario Internacional (FMI), en 2022 advirtió que los riesgos de adoptar Bitcoin como moneda de curso legal podían superar los beneficios a corto plazo. Estas advertencias reflejaban preocupación de que esta criptomoneda pudiera comprometer la estabilidad económica y fiscal del país, esto al aparecer en medios de comunicación locales fueron causantes de más incertidumbre en las personas al uso de las criptomonedas (Prensa grafica, 2021).

1.5.3 Proyectos de minería de Bitcoin en El Salvador

El Salvador inició una estrategia de minería de Bitcoin como complemento a su política de adopción legal, buscando generar valor económico mediante la validación descentralizada de transacciones en la red *blockchain*. Esta iniciativa se basó en una planta de energía geotérmica ubicada en Berlín, Usulután, alimentada por el volcán Tecapa. Desde 2021, esta instalación ha dedicado aproximadamente 1.5 MW del total de 102 MW generados para operar unos 300 procesadores *ASIC (Application Specific Integrated Circuit* o en español como *Circuito de Aplicación Especifica)*, logrando minar cerca de 474 BTC, cuyo valor rondaba los 29 millones de dólares a mayo de 2024. Este modelo ha sido presentado como pionero en minería sostenible, utilizando energía renovable en lugar de combustibles fósiles (Nelson Renteria, 2024)

Paralelamente, se impulsó el proyecto privado público *Volcano Energy*, anunciado en junio de 2023, con una inversión inicial de US$ 250 millones y un compromiso total de hasta US$ 1,000 millones. Este proyecto combina un parque eléctrico de 241 MW, distribuido en 169 MW solares y 72 MW eólicos en Metapán, con planes futuros de integración geotérmica para asegurar suministro continuo. *Volcano Energy* aspira a convertirse en la mayor planta de minería en el país (Energy, 2023).

Además, en octubre de 2023 se lanzó el primer pool de minería nacional, "Lava Pool", en colaboración con Luxor Technology, para canalizar la potencia computacional de *Volcano Energy* y ofrecer retornos a los mineros mediante una comisión adecuada. En abril de 2024, se anunció que la fase inicial con inicio en enero de 2025 operará con 85 MW fotovoltaicos y 49.6 MW eólicos; el excedente energético se inyectará a la red nacional. Se proyecta que cuando se habilite la fase geotérmica se donarán a la red los excedentes solares y eólicos, y el Estado recibirá el 23 % de las ganancias (Cointelegraf, 2023).

A pesar del enfoque sostenible, la minería en El Salvador plantea preocupaciones socioambientales. Se advierte según periódicos locales y medios de comunicación que el uso energético adicional podría otorgar desigualdades en el acceso a la electricidad, afectando a hogares que ya enfrentan limitaciones en cobertura energética. (César Artiga & Meraris López, 2021).

CAPÍTULO 2. HARDWARE Y SOFTWARE APLICADO A LA MINERÍA DE CRIPTOMONEDAS

En el contexto de la minería de criptomonedas, uno de los factores importantes para el éxito operativo y económico es la elección adecuada del equipo computacional y software especializado. Los avances tecnológicos han dado lugar al desarrollo de sistemas especializados de alto rendimiento en el ámbito de la minería, capaces de maximizar la eficiencia energética, la capacidad de procesamiento, parámetros fundamentales para lograr alcanzar niveles sostenibles de rentabilidad.

Este capítulo presenta los principales tipos de hardware y software usados en la minería de criptomonedas, como los *CPU*, *GPU* y ASIC, destacando el uso de los ASIC, los cuales son diseñados únicamente en la minería de Bitcoin. Asimismo, se examinan las herramientas de software que permiten la configuración, supervisión y automatización del funcionamiento de estos dispositivos, con el fin de maximizar su productividad operativa.

2.1 Hardware de minería

En los inicios de Bitcoin, la minería se realizaba exclusivamente con *CPU* (*Unidades Centrales de Procesamiento)* de propósito general. El bloque génesis de Bitcoin, minado por *Satoshi Nakamoto* el 3 de enero de 2009, fue producido usando un ordenador personal común, ya que en ese momento no existía competencia en la red y la *dificultad* de minado era muy baja. Las *CPU* son el cerebro de cualquier computadora y ejecutan instrucciones de propósito general. Durante 2009 y 2010, potentes *CPU* multinúcleo de Intel o AMD podían minar Bitcoin de forma viable debido al bajo *hashrate* global y a la baja *dificultad* para encontrar nuevos bloques. Sin embargo, a medida que Bitcoin ganó valor de mercado y más participantes se unieron a la red, la potencia computacional requerida para competir por las recompensas creció exponencialmente (Christine, 2021).

La primera gran innovación llegó en 2010 con el uso de *GPU* (*Unidades de Procesamiento Gráfico*) para minar. Las *GPU*, diseñadas originalmente para renderizar gráficos de videojuegos,

poseen cientos o miles de núcleos capaces de ejecutar operaciones matemáticas en paralelo, lo que les permite encontrar los *hashes* con la función *SHA-256* mucho más rápido que en una *CPU* convencional. Esto permitió que la minería con GPU incrementara significativamente la eficiencia para producir bloques respecto a la minería con *CPU*, con un costo de hardware apenas el doble que el de un ordenador con un buen procesador (Christine, 2021).

Para 2014, la mayoría de *GPU* lograban una *tasa de hash* menor a 1 GH/s (giga*hash* por segundo) minando Bitcoin, mientras que ya existían equipos especializados capaces de más de 1,000 GH/s (1 TH/s) consumiendo mucho menos energía. Esto volvió obsoleta la minería de Bitcoin con *GPU*, aunque este tipo de hardware siguió siendo útil para minar otras criptomonedas con algoritmos diferentes. No obstante, dicho hardware continuó siendo relevante en la minería de otras criptomonedas, como en el caso de Ethereum, cuyo diseño permitía una minería eficiente mediante *GPUs* (Faster Capital, s.f.).

La verdadera revolución llegó en 2013 con la introducción de los primeros ASIC diseñados exclusivamente para minar Bitcoin. En lugar de reutilizar hardware existente, empresas dedicadas emprendieron el desarrollo de chips de silicio optimizados únicamente para la función *hash SHA-256* con la máxima velocidad y eficiencia. El primer ASIC minero de Bitcoin fue lanzado a inicios de 2013 por la compañía china Canaan Creative.

Por ejemplo, los primeros ASIC incrementaron el *hashrate*, superando ampliamente el desempeño de las *GPU* y a costos energéticos menores. Esta transición dejo obsoletos a los mineros basados en *GPU* para Bitcoin desde 2013. Desde entonces, los ASIC han dominado completamente la minería de Bitcoin, y su desarrollo ha seguido avanzando rápidamente con sucesivas generaciones de hardware que integran tecnologías de semiconductores cada vez más avanzadas (Christine, 2021).

2.1.1 Minería con *CPU*, *GPU* y Rig de minería

La evolución tecnológica de la minería de criptomonedas ha estado fuertemente influenciada por la progresiva transición entre distintas formas de procesamiento, desde *CPU* de propósito general hasta unidades de procesamiento gráfico (*GPU*). Hubo un momento antes de que los ASIC fueran la mejor opción como estándar en la minería de Bitcoin, que los mineros optaron por usar los *GPUs*

en algo que se llama rigs de minería (*mining rigs*). Estos sistemas permitieron la expansión modular de la capacidad de cómputo mediante la integración de muchos *GPU* en configuraciones optimizadas para minería.

Minería con *CPU*

La minería con *CPU* representa el punto de partida histórico del proceso de generación de criptomonedas mediante *Proof of Work (PoW)*. Las *CPU* son microprocesadores de propósito general diseñados para ejecutar instrucciones secuenciales y manejar tareas complejas con bajo nivel de paralelismo. Su arquitectura interna está optimizada para versatilidad, priorizando el rendimiento en aplicaciones generales como procesamiento de texto, navegación, cálculos matemáticos complejos y ejecución de sistemas operativos.

Durante los primeros meses del funcionamiento de la red Bitcoin (2009–2010), el *hashrate* global era suficientemente bajo como para que una *CPU* convencional pudiera competir por la resolución de bloques. Por ejemplo, un procesador Intel Core 2 Duo podía generar hasta 5-10 mega *has*hes por segundo (*MH/s*), rendimiento que en ese momento era suficiente dada la baja *dificultad* de minado.

Sin embargo, a medida que el interés por Bitcoin aumentó y más nodos se incorporaron a la red, el nivel de *dificultad* ajustado dinámicamente por el protocolo creció de manera exponencial, desplazando rápidamente a las *CPU* como opción viable. Además, desde el punto de vista energético, las *CPU* presentan una baja eficiencia cuando se comparan con arquitecturas paralelas, consumen una cantidad considerable de energía, pero con una baja *tasa de hash* (*hashrate*), lo cual limita su escalabilidad y rentabilidad.

Minería con *GPU*

El uso de *GPU* para minería supuso la primera gran separación tecnológica dentro del ecosistema Bitcoin. Las *GPU* están diseñadas para ejecutar miles de operaciones en paralelo, lo que las hace altamente eficientes en tareas que requieren cálculos masivos y repetitivos, como renderizado gráfico y procesamiento de algoritmos de *hash*. Su arquitectura está compuesta por cientos o miles

de núcleos de ejecución que operan bajo el principio de ejecución masivamente paralela (*SIMD*, *Single Instruction Multiple Data*), característica que las *CPU* no poseen en la misma escala.

Por esta razón, las *GPU* demostraron ser mucho más efectivas para ejecutar funciones criptográficas como *SHA-256*. Una sola tarjeta gráfica de gama alta, como la AMD Radeon HD 5970, podía alcanzar hasta *800 MH/s*, superando en más de 50 veces a una *CPU* promedio de la época. Este aumento exponencial en el rendimiento propició la adopción generalizada de *GPU* por parte de mineros independientes y pequeños operadores que buscaban una solución de mayor capacidad, sin incurrir en los costos de adquirir un equipo ASIC.

Además de su capacidad de procesamiento, las *GPU* ofrecían mayor eficiencia energética en términos de *hash por segundo* y un mayor control en la capacidad de aumentar la potencia, permitiendo configurar sistemas personalizados con múltiples tarjetas en paralelo, las cuales fueron llamadas después *rig de minería* (Seth, 2024).

La necesidad de aumentar la capacidad de cómputo llevó al diseño de plataformas modulares conocidas como *rigs de minería*. Estos sistemas consisten en configuraciones físicas y lógicas diseñadas específicamente para integrar múltiples *GPU* operando en paralelo, conectadas a una sola placa base y gestionadas mediante software especializado de minería. En esencia, un *rig de minería* es una infraestructura de cómputo como se muestra en la Figura 2.1, donde se agrupan 8 GPU con el propósito de maximizar la potencia, rendimiento y consumo energético en tareas específicas de minería.

Figura 2.1 Rig de minería con 8 GPU

Componentes principales de un *rig* de minería

- **Placa madre** (motherboard): debe contar con múltiples puertos PCIe para permitir la conexión simultánea de varias tarjetas gráficas, usualmente entre 6 y 13 slots.
- **Procesador (*CPU*)**: aunque el foco está en las *GPU*, es necesario un procesador para gestionar el sistema operativo y el software de minería. Se utiliza generalmente una *CPU* de bajo consumo.
- **Memoria RAM**: se emplea una cantidad mínima (4–8 GB) suficiente para garantizar la estabilidad del sistema operativo.
- **Almacenamiento**: típicamente discos de estado sólido (SSD) de 120–240 GB para rápida carga del firmware y del sistema.
- **Fuente de alimentación (*PSU*, *Power Supply Unit*)**: es el componente encargado de suministrar la energía eléctrica necesaria a la planta de minería. Para operar eficientemente equipos de minería de alto rendimiento, las fuentes de alimentación deben ser capaces de entregar entre 1,200 W y 2,000 W de potencia continua.
- **Tarjetas gráficas (*GPU*)**: el componente crítico del sistema, seleccionadas por su alta capacidad de procesamiento (*hashrate*), bajo consumo por *MH/s* y buena capacidad de refrigeración.
- **Estructura metálica abierta**: facilita la ventilación y la disipación térmica, elementos fundamentales para evitar el sobrecalentamiento.

2.1.2 Minería con ASIC

La aparición de los *Application Specific Integrated Circuits* (ASIC) marcó un punto de inflexión en la evolución tecnológica de la minería de Bitcoin. A diferencia de las *CPU* y *GPU*, dispositivos de propósito general, los ASIC son circuitos integrados diseñados específicamente para realizar una única función de manera extremadamente eficiente: en este caso, ejecutar cálculos de funciones *hash* SHA-256 requeridos en el algoritmo de consenso *Proof of Work* (*PoW*) de Bitcoin.

Desde su introducción en 2013, los ASIC han desplazado completamente a las *GPU* en términos de eficiencia, capacidad de procesamiento y rentabilidad. Su diseño especializado permite alcanzar

tasas de *hash* significativamente superiores a las que puede ofrecer un conjunto completo de *rigs* basados en *GPU*, con un consumo energético mucho más eficiente. En la actualidad, un solo equipo ASIC es capaz de superar en rendimiento a múltiples plataformas *GPU* operando en paralelo, lo que ha consolidado su adopción como estándar en operaciones mineras de mediana y gran escala. Esta evolución tecnológica ha convertido a los ASIC en el componente central de la infraestructura de minería de Bitcoin a nivel global.

Una de las ventajas más significativas de los ASIC es su alta potencia de cómputo. Mientras que una *GPU* de alto rendimiento puede alcanzar hasta 1 GH/s, los ASIC modernos operan en el orden de los terahash por segundo (TH/s), con un consumo energético optimizado que permite alcanzar eficiencias superiores a los 25 a 30 J/TH (julios por *terahash*), dependiendo del modelo y generación de fabricación (Vermaak, 2022).

Al utilizar equipos ASIC para minería de bitcoin se deben considerar diversos factores importantes, como las siguientes:

- **Costos iniciales:** Al adquirir un equipo ASIC para minería de bitcoin, se debe considerar algunos costos tales como, costo del equipo, costos de envío y tarifas de importación.
- **Capacidad de procesamiento (*hashrate*):** La *tasa de hash* es la velocidad a la que el equipo puede realizar los cálculos criptográficos para añadir bloques a la cadena de bloques de Bitcoin. Mientras mayor sea el *hashrate* mayor serán las posibilidades de poder validar un bloque. Por lo tanto, es importante tener una buena potencia de cómputo.
- **Consumo de energía eléctrica:** La energía que consumen los equipos ASIC es un factor importante para determinar los costos operativos y de rentabilidad. Este tipo de equipos consume una gran cantidad de energía. En la actualidad existen equipos ASIC que consumen más de 7,000 W.
- **Eficiencia energética:** La eficiencia energética es un parámetro relevante en la operación de equipos de minería, ya que influye directamente en la optimización de los costos operativos. En el ámbito de la minería de criptomonedas, este parámetro se define como la relación entre el consumo de energía y la *tasa de hash*, expresándose mediante la fórmula: *Eficiencia = consumo de energía / tasa de hash*. Una menor relación indica una mayor

eficiencia, lo que implica que el equipo puede generar una mayor *tasa de hash* con un consumo eléctrico reducido.

- **Ruido:** El ruido generado por los equipos ASIC es un aspecto significativo para considerar. La mayoría de los equipos ASIC están equipados con ventiladores. Estos ventiladores pueden generar ruido significativo. Por lo tanto, se debe considerar la ubicación de los equipos. Colocar el equipo en un espacio cerrado o en una ubicación con aislamiento acústico ayuda a reducir la transmisión del ruido al entorno. Además, en entornos de minerías grandes, es importante ubicar los equipos en espacios aislados, en zonas no habitadas. (Vermaak, 2022)

A continuación, se presenta la Tabla 2.1 la cual es una comparación que resume las diferencias más relevantes entre *CPU*, *GPU* y ASIC en el contexto específico de la minería de criptomonedas. Esta comparación técnica permite comprender las razones detrás de la progresiva adopción de soluciones cada vez más especializadas, desde equipos de propósito general hasta hardware optimizado exclusivamente para tareas criptográficas. (Han Su, 2025)

Parámetro técnico	***CPU***	***GPU***	**ASIC**
Propósito de diseño	Uso de propósito general	Gráfico y cómputo paralelo	Minería específica (algoritmo SHA-256, Scrypt, etc.)
Arquitectura	Núcleos complejos, ejecución secuencial	Múltiples núcleos simples, ejecución paralela	Circuitos dedicados para función de *hash*
***Hashrate* típico**	5 a 50 MH/s	100 a 1,000 MH/s	50 a 200 TH/s
Eficiencia energética	Muy baja (no apta para minería actual)	Moderada (40 a 100 J/MH o 0.04 a 0.1 J/TH)	Muy alta (20 a 30 J/TH)
Consumo energético promedio	60–120 W	150–350 W por tarjeta	3,000–6,000 W por unidad
Costo de adquisición	Bajo (US$ 100 – 300)	Medio (US$ 300 – 800 por unidad)	Alto (US$ 2,000 – 6,000 por equipo)
Vida útil estimada	Alta (uso general)	Media (2–3 años en minería intensiva)	Baja-media (1–2 años en minería continua)

Facilidad de implementación	Muy alta (uso inmediato)	Alta (requiere configuración y drivers)	Media (requiere firmware y configuración de red)
Flexibilidad de uso	Alta (varios fines)	Media (algunas criptomonedas)	Nula (solo útil para un algoritmo específico)
Nivel de ruido y calor	Bajo	Medio-alto	Muy alto (refrigeración especializada requerida)
Rentabilidad en minería BTC	Obsoleta desde 2011	Obsoleta desde 2013	Alta (en condiciones óptimas de red y energía)
Escalabilidad operativa	Muy limitada	Moderada (usando *rigs*)	Alta (diseñado para minería a gran escala)

Tabla 2.1 Comparación de los tres tipos de hardware de minería de criptomonedas

2.1.3 Modelos ASIC para minar bitcoin

La industria de los *Circuitos Integrados de Aplicación Específica* (ASIC) utilizados en la minería de Bitcoin está conformada por un conjunto de fabricantes que han logrado posicionarse como referentes tecnológicos, gracias a su capacidad de innovación en eficiencia energética, escalabilidad y rendimiento de procesamiento. Entre los fabricantes más relevantes destacan Bitmain (Antminer) y MicroBT (WhatsMiner), reconocidos por el diseño de equipos que ofrecen una alta *tasa de hash* con consumos energéticos optimizados. Estos dispositivos son ampliamente utilizados en plantas de minería, donde se requiere una operación continua, control térmico eficiente y estabilidad bajo condiciones exigentes. A continuación, se presentan algunos de los modelos ASIC más utilizados actualmente en la minería de Bitcoin.

Antminer S21

- **Descripción:** El Antminer S21, ilustrado en la Figura 2.2, es un equipo especializado para la minería de Bitcoin desarrollado por la empresa Bitmain y lanzado en julio de 2024. Este modelo opera bajo el algoritmo SHA-256 y destaca por integrar un sistema de refrigeración por aire de alta eficiencia, diseñado para mantener temperaturas operativas estables en

entornos de carga continua. Su arquitectura representa un equilibrio optimizado entre potencia de cómputo y consumo energético, lo que lo convierte en una opción competitiva en términos de eficiencia energética dentro de su generación. Además, se posiciona como uno de los modelos con mejor relación costo/rendimiento dentro de la serie S21, favoreciendo su adopción en plantas de minería de mediana y gran escala.

- **Especificaciones:** El Antminer S21 está diseñado para operar con el algoritmo SHA-256, utilizado en la minería de Bitcoin. Ofrece una *tasa de hash* de 200 TH/s y presenta un consumo eléctrico de 3,500 W, lo que se traduce en una eficiencia energética de 17.5 J/TH. Genera un nivel de ruido aproximado de 75 dB, y sus dimensiones físicas son 400 × 195 × 290 mm, con un peso neto de 15.4 kg. Fue lanzado al mercado en julio de 2024 y tiene un precio estimado de US$ 2,900.

Antminer S21 Pro

- **Descripción:** El Antminer S21 Pro es una versión mejorada dentro de la línea de equipos desarrollados por Bitmain, específicamente optimizada para el algoritmo SHA-256, utilizado en la minería de Bitcoin. Aunque su diseño externo se mantiene consistente con el modelo base de la Figura 2.2, incorpora mejoras a nivel interno en componentes clave como el sistema de gestión térmica y la eficiencia del sistema de alimentación. Estas optimizaciones permiten alcanzar una mayor *tasa de hash* y una eficiencia energética superior, posicionando al Antminer S21 Pro como una de las opciones más avanzadas para aplicaciones en plantas de minería de alto rendimiento.
- **Especificaciones:** El Antminer S21 Pro opera con el algoritmo SHA-256, y representa una mejora dentro de la misma serie. Alcanza una *tasa de hash* de 234 TH/s, con un consumo eléctrico de 3,510 W, logrando una eficiencia energética de 15 J/TH. Mantiene un nivel de ruido cercano a 75 dB, y comparte las mismas dimensiones físicas de 400 × 195 × 290 mm y un peso neto de 15.4 kg. Su lanzamiento se realizó en julio de 2024, con un valor estimado de US$ 3,400.

Figura 2.2 Antminer S21

Whatsminer M66

- **Descripción:** El WhatsMiner M66 es un equipo de alta eficiencia diseñado para la minería de Bitcoin bajo el algoritmo SHA-256, desarrollado por la empresa MicroBT. A diferencia de los modelos que utilizan refrigeración por aire, el M66 incorpora un sistema de enfriamiento líquido (*hydro cooling*), lo que permite una disipación térmica más eficiente y un funcionamiento estable en entornos de alta densidad computacional. Además, presenta un formato más compacto en comparación con equipos de la serie Antminer, lo que facilita su integración en plantas de minería con infraestructura optimizada para enfriamiento líquido. Un equipo Whatsminer se ilustra en la Figura 2.3 donde su tamaño facilita la incorporación en los "liquid cooled rack" (*rack con enfriamiento liquido*).
- **Especificaciones:** El WhatsMiner M66 opera con el algoritmo SHA-256, utilizado en la minería de Bitcoin. Ofrece una *tasa de hash* de 280 TH/s y presenta un consumo eléctrico de 5,572 W, lo que le confiere una eficiencia energética de 17 J/TH. Genera un nivel de ruido cercano a los 75 dB, con variaciones según el sistema de enfriamiento implementado. Sus dimensiones físicas son 267 × 147 × 401 mm, y tiene un peso neto de 18 kg. Fue lanzado al mercado en 2024, con un precio promedio de US$ 4,200.

Whatsminer M66S Hydro

- **Descripción:** El WhatsMiner M66S Hydro es una variante mejorada dentro de la línea de equipos desarrollados por MicroBT, orientada a la minería de Bitcoin mediante el algoritmo SHA-256. Este modelo mantiene el mismo diseño físico que el WhatsMiner M66, como se muestra en la Figura 2.3, diferenciándose únicamente a nivel interno por sus mejoras en potencia de procesamiento y parámetros de eficiencia energética. Conserva el mismo sistema de refrigeración líquida, lo que le permite operar de manera estable bajo cargas térmicas elevadas. Está especialmente diseñado para ofrecer un mayor *hashrate* manteniendo un equilibrio aceptable en consumo energético.
- **Especificaciones:** El equipo ofrece una *tasa de hash* de 298 TH/s, con un consumo eléctrico de 5,513 W, lo que se traduce en una eficiencia energética de 18 J/TH. Genera un nivel de ruido menor en comparación con sistemas de refrigeración por aire, al depender de enfriamiento líquido. Sus dimensiones y peso varían según la configuración del sistema de refrigeración instalado.

Figura 2.3 Whatsminer M66

2.2 Software de minería de criptomonedas

El software de minería de criptomonedas representa el componente esencial que permite la interacción entre el hardware minero y la red *blockchain*. Su función principal es coordinar el trabajo del minero, comunicarse con el *pool* de minería o directamente con la red descentralizada,

y gestionar las tareas de cómputo necesarias para encontrar soluciones válidas a los problemas criptográficos del protocolo de consenso *Proof of Work (PoW)*. Además, proporciona funcionalidades de monitoreo, configuración y optimización del rendimiento operativo. Existen dos grandes categorías de software de minería, el sistema operativo del hardware y los programas de minería que conectan con la red Bitcoin (Frumkin, 2022).

2.2.1 Principales software de minería

En este estudio se analizarán los principales softwares de minería actuales, desde los inicios de la minería de criptomonedas, debido a la aparición de Bitcoin en 2009, han surgido diversos programas o software diseñados para facilitar este proceso. A lo largo del tiempo, el mercado se ha ido consolidando y actualmente existen varios proveedores reconocidos que dominan la industria los cuales se distinguen por su rendimiento y factores clave como su modelo de pago y su facilidad de uso.

CGMiner

CGMiner, fue creado por Con Kolivas en 2011 y es uno de los programas o software más usados para el minado de Bitcoin basado en Linux, el cual ha sido codificado por completo en el lenguaje de programación C, por lo cual es compatible con todos los sistemas operativos. Asimismo, está basado en el código de uno de los primeros programas populares de minado llamado CPUMiner. El CGMiner es una excelente plataforma para la aplicación de minería versátil y de código abierto. Gracias a su arquitectura modular, ha evolucionado hasta ofrecer cierta compatibilidad con otros algoritmos como el SHA-256 y con otras criptomonedas (Aaron, 2025).

El programa se ejecuta desde línea de comando, tal como se muestra en la Figura 2.4, lo que permite un control detallado sobre parámetros como la velocidad de los ventiladores, la *tasa de hash* y la gestión de *pools de minería*. Aunque no cuenta con una interfaz gráfica de usuario (GUI), su robustez y grado de control lo convierten en una herramienta preferida por usuarios avanzados.

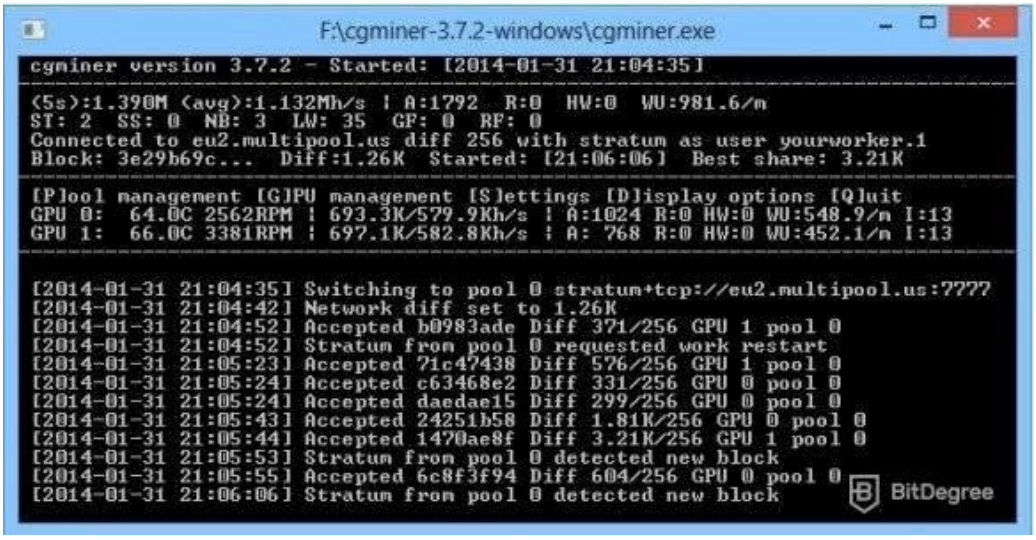


Figura 2.4 Acceso desde línea de comando a CGMiner.

CGMiner es compatible con múltiples sistemas operativos, incluyendo Linux, MacOS y Windows, y su enfoque en el rendimiento le permite escalar eficazmente la potencia de *hash* sin introducir latencia significativa. Originalmente soportaba CPU y GPU, pero las versiones más recientes han descontinuado este soporte en favor de ASIC, debido a los cambios en la eficiencia del hardware de minería (Kanade, 2023).

BFGMiner

BFGMiner, presentado en 2012 por Luke Dash jr, es un software de minería de código abierto diseñado principalmente para trabajar con hardware FPGA y ASIC, excluyendo el uso de GPU. Aunque fue inicialmente muy popular, no superó la difusión de herramientas como CGMiner.

Se caracteriza por ofrecer sólidas opciones de personalización, lo que permite a los usuarios monitorear en tiempo real la temperatura del hardware, gestionar plataformas de manera remota e incluso detectar e iniciar subprocesos inactivos, lo que optimiza el rendimiento del sistema. El software está escrito en lenguaje C y es compatible con los sistemas operativos Linux, MacOS y Windows.

Una de sus funciones destacadas es la posibilidad de realizar minería simultánea utilizando múltiples algoritmos, como *Scrypt* y *SHA-256*, lo cual puede contribuir a diversificar el riesgo y aumentar la eficiencia en ciertas configuraciones. Su uso se realiza mediante una interfaz de línea

de comandos, que incluye atajos de teclado personalizables, ofreciendo un control preciso del proceso de minería. No obstante, la ausencia de una Interfaz Gráfica de Usuario (*GUI*) puede representar una barrera para usuarios principiantes o con menos experiencia técnica. En la Figura 2.5 se muestra una captura de pantalla del entorno de ejecución por la línea de comandos de BFGMiner, donde se visualiza en tiempo real el rendimiento del minero y los parámetros clave del sistema (Legge1, 2025).

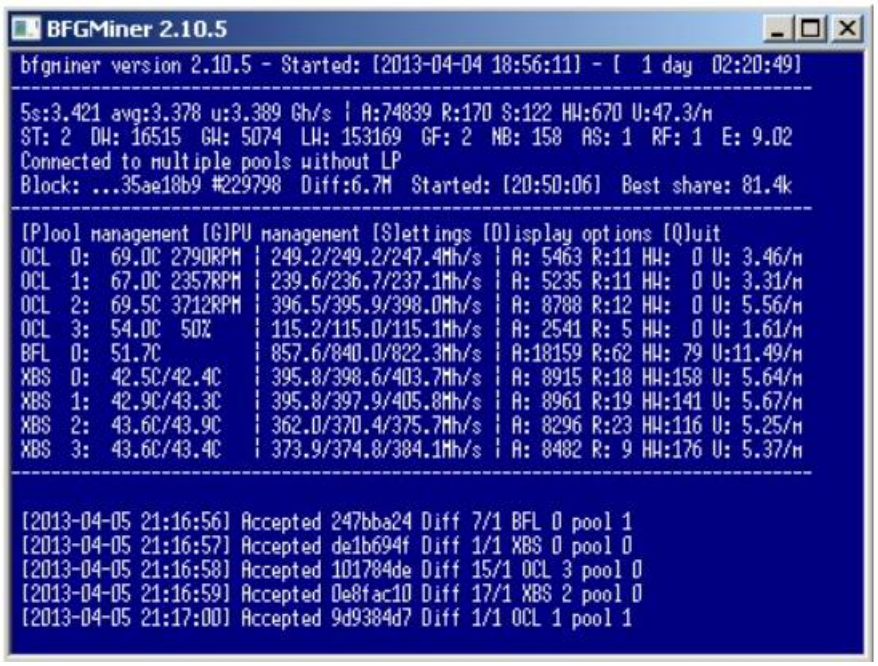


Figura 2.5 Acceso desde línea de comando a BFGMiner

EasyMiner

EasyMiner es una interfaz gráfica de usuario (GUI) desarrollada para facilitar la operación de herramientas de minería como CGMiner, actuando como una capa de abstracción que permite a los usuarios interactuar con dicho software sin requerir conocimientos avanzados en programación. Esta solución está orientada a usuarios principiantes o intermedios que desean iniciar procesos de minería sin enfrentarse a la complejidad de configuraciones manuales mediante líneas de comandos.

El software es compatible con Unidades de Procesamiento Gráfico (GPU) y Unidades Centrales de Procesamiento (CPU), lo que permite su ejecución en una amplia gama de hardware. Mediante

su panel de control gráfico, EasyMiner proporciona representaciones visuales en tiempo real de variables clave del proceso de minería, tales como la *tasa de hash* (*hashrate*), ganancias estimadas.

En términos de seguridad, EasyMiner afirma implementar medidas de protección orientadas a la confidencialidad de las operaciones del usuario. Su documentación oficial hace referencia a mecanismos diseñados para reducir la exposición a amenazas externas durante el proceso de minería, incluyendo la protección de sesiones y configuraciones que refuerzan la integridad de los datos manejados por el sistema.

Una vez instalado y configurado, *EasyMiner* proporciona una interfaz visual desde la cual el usuario puede gestionar todos los parámetros operativos relevantes para el proceso de minería. Esta capa gráfica simplifica la configuración de aspectos técnicos como los puertos de conexión, las direcciones del *pool de minería* y las credenciales de los trabajadores, permitiendo además seleccionar entre distintos métodos de ejecución automática y ajustes de rendimiento. En la Figura 2.6 se muestra una captura de pantalla de la interfaz gráfica, la cual centraliza el control de los módulos de minería por *CPU* y *GPU*, facilitando su uso en entornos sin gestión técnica especializada (Legge1, 2025).

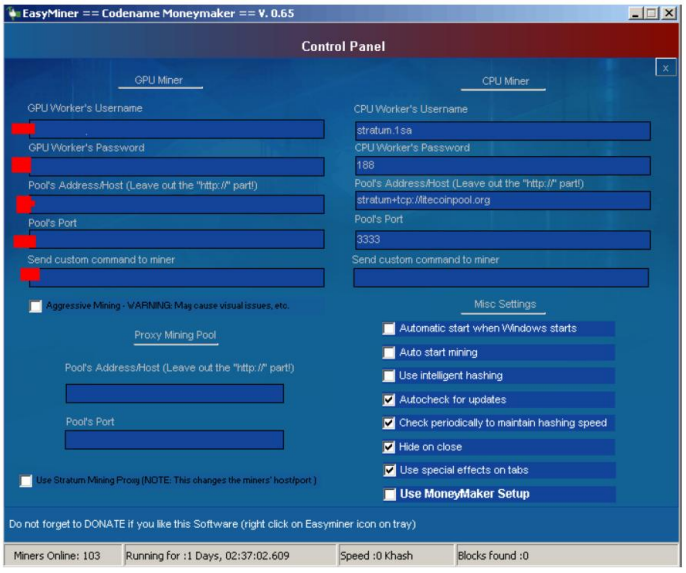


Figura 2.6 Interfaz gráfica de EasyMiner

Braiins OS

Braiins OS es un firmware de código abierto desarrollado por la empresa Braiins, reconocida por operar uno de los primeros *pools* de minería de Bitcoin, conocido como (actualmente Braiins Pool). Este software está diseñado específicamente para *Slush Pool* equipos ASIC utilizados en minería bajo el algoritmo SHA-256, principalmente modelos de la serie Antminer de Bitmain. Su principal objetivo es optimizar el desempeño energético y térmico de los dispositivos mineros mediante un control detallado de los parámetros internos de operación.

A diferencia del firmware propietario suministrado por los fabricantes, Braiins OS permite realizar ajustes avanzados a nivel de chip, tales como la modificación de la potencia de minado. Esta capacidad se traduce en una mejora significativa de la eficiencia energética del equipo, medida en julios por terahash (J/TH), al permitir una operación personalizada según las condiciones del entorno y el consumo eléctrico disponible.

Una de sus funciones más destacadas es el *autotuning*, un sistema de autoajuste que analiza en tiempo real el rendimiento térmico y energético de cada chip para encontrar el punto óptimo de operación. Este mecanismo no solo incrementa la eficiencia energética, sino que también extiende la vida útil del hardware al reducir el estrés térmico sobre los componentes (Frumkin, 2022)

La instalación de Braiins OS se realiza mediante una tarjeta microSD, desde la cual se carga la imagen del firmware. Una vez introducida en el equipo ASIC, el sistema inicia un proceso automático de flasheo, reemplazando el software de fábrica. Finalizada la instalación, el usuario accede a una interfaz web rediseñada, con monitoreo en tiempo real de parámetros como la *tasa de hash*, temperatura por chip, consumo estimado de energía y estado de conexión con los *pools* configurados.

Este firmware es compatible con modelos como el Antminer S9, S17, T17 y algunas variantes del S19, permitiendo una personalización avanzada en entornos industriales y domésticos. Además, al ser una solución de código abierto, proporciona mayor transparencia y auditabilidad frente a firmware cerrados, lo que lo hace ideal para operaciones que priorizan la seguridad, la estabilidad y la eficiencia del sistema minero (Frumkin, 2022).

2.2.2 *Pool* de minería

Un *pool* de minería de criptomonedas es una agrupación de mineros que combinan sus recursos computacionales con el objetivo de aumentar la probabilidad de resolver bloques en una red *blockchain*. A través de este enfoque colaborativo, los participantes distribuyen las tareas de cómputo entre múltiples nodos y, una vez que se encuentra un bloque, las recompensas obtenidas se reparten proporcionalmente entre los miembros del *pool*, en función de la contribución computacional de cada uno.

Las redes *blockchain* operan sobre un sistema descentralizado de nodos mineros que interactúan bajo un protocolo de consenso predefinido (como *Proof of Work* o *Proof of Stake*), cuya finalidad es validar y registrar transacciones en un libro mayor distribuido. Como se ha discutido en el capítulo anterior, estos protocolos son esenciales para garantizar la seguridad y confiabilidad de la red. Dentro de este contexto, los *pools* representan una estrategia efectiva para mitigar la creciente dificultad de minería y el alto nivel de competencia existente en redes como Bitcoin.

Dada la actual complejidad y nivel de competitividad de la minería de Bitcoin, resulta altamente improbable que un minero individual (con recursos limitados) logre obtener recompensas de forma constante sin participar en un *pool*. La *dificultad* de minería se ajusta dinámicamente según la cantidad total de potencia computacional conectada a la red, lo que favorece a quienes operan con mayores potencias de cómputo. Por esta razón, la gran mayoría de los mineros domésticos optan por unirse a *pools* que les permitan acceder a recompensas más frecuentes, aunque proporcionalmente menores (Legge, 2025).

En este estudio, se decidió no minar en solitario, ya que la probabilidad de éxito sin la participación en un *pool* sería significativamente reducida, dada la alta competencia actual y la limitación de recursos computacionales disponibles.

Al seleccionar un *pool* de minería, es importante considerar varios factores técnicos y operativos que influyen directamente en la rentabilidad y eficiencia de la actividad minera:

- **Comisiones**: La mayoría de los *pools* cobran un porcentaje sobre las recompensas obtenidas, que suele oscilar entre el 1 % y el 3 %. Si bien una comisión más baja puede parecer favorable, esta no debe ser el único criterio de selección, ya que *pools* con mayor

eficiencia y reputación pueden justificar una comisión más alta. Por ejemplo, F2Pool, uno de los *pools* más grandes y estables, aplica una comisión aproximada del 2.5 %.

- **Pago mínimo**: Hace referencia a la cantidad mínima de criptomoneda que debe alcanzarse para que se procese un pago. Si el monto acumulado en un periodo determinado no supera ese umbral, el pago se pospone hasta que la suma sea suficiente. Por ejemplo, si el pago mínimo es de 0.005 BTC y el minero ha generado 0.002 BTC, no recibirá el pago hasta alcanzar el mínimo establecido.
- **Tamaño del *pool***: El número de participantes y la potencia de cómputo total del *pool* influyen en la frecuencia con la que se resuelven bloques. En general, *pools* más grandes tienen una mayor probabilidad de éxito, aunque esto también implica que las recompensas se distribuyen entre más usuarios. Además, un gran tamaño puede ser un indicador indirecto de confiabilidad y estabilidad operativa.

Entre los *pools de minería* más reconocidos y utilizados a nivel global se encuentran Foundry USA, Antpool, F2Pool, MARA Pool y Braiins Pool. Este último ha sido pionero en la implementación del protocolo de comunicación Stratum V2, el cual mejora la seguridad, eficiencia y descentralización en la interacción entre los dispositivos ASIC y los servidores del *pool*. Asimismo, su integración con el firmware de código abierto Braiins OS permite una gestión avanzada del hardware de minería, optimizando tanto el consumo energético como el control sobre parámetros operativos clave, como la tasa de *hash* y la estabilidad térmica (Legge, 2025).

La distribución global de la *tasa de hash* de todos los participantes de *pool de minería* de Bitcoin se ilustra en la Figura 2.7, con base en datos de Hashrate Index consultados en mayo de 2025. En ella se observa que Foundry USA lidera el mercado con un 28.44 % de la *tasa de hash*, seguido por Antpool (17.1 %) y F2Pool (10.7 %). Otros actores como MARA Pool, Binance Pool y Braiins Pool también mantienen una participación, lo cual evidencia un ecosistema competitivo y en constante evolución (Hashrate Index, 2025).

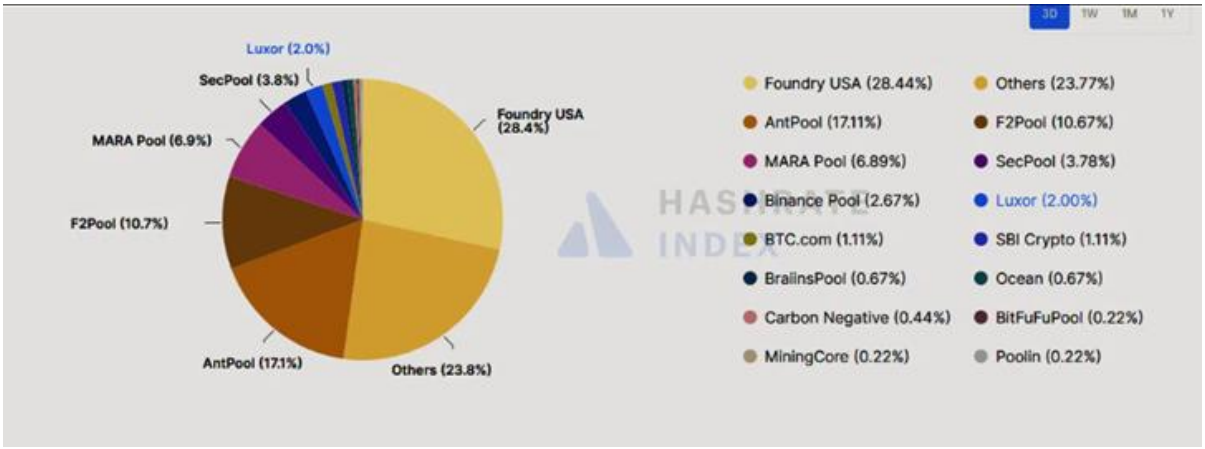


Figura 2.7 Distribución de la potencia de *hashrate* entre *pools* de minería de Bitcoin.

F2Pool

F2Pool es uno de los *pools* de minería más consolidados a nivel global, con aproximadamente el 18 % del total de bloques minados en la red Bitcoin, lo que lo posiciona como una de las principales entidades en esta industria. Fundado en 2013, fue uno de los primeros *pools* en operar de manera continua, y actualmente admite la minería de múltiples criptomonedas, no solo Bitcoin.

La plataforma aplica una comisión estándar del 2.5 % sobre las recompensas obtenidas y establece un umbral mínimo de retiro diario de 0.005 BTC. Los pagos se realizan de forma diaria. Su infraestructura es compatible con equipos de minería ASIC y GPU, y dispone de soporte técnico especializado, así como una interfaz web intuitiva y funcional. Además, F2Pool opera con un *hashrate* total estimado en 30.60 EH/s (30,600.0 TH/s), lo que refuerza su posición como uno de los *pools* con mayor capacidad de procesamiento en la red Bitcoin.

En términos operativos, F2Pool utiliza los métodos de distribución de recompensa *PPS+* (*Pay Per Share Plus*) y *PPLNS* (*Pay Per Last N Shares*). El método *PPS+* paga al minero por cada acción válida enviada, sin necesidad de esperar a que se encuentre un bloque, y también incluye una parte de las tarifas de transacción. Esto permite obtener pagos constantes según el trabajo aportado. Por otro lado, el método *PPLNS* distribuye las recompensas en función del número de acciones enviadas dentro de una ventana de tiempo reciente, favoreciendo a los usuarios que mantengan una conexión activa y estable durante más tiempo (Legge, 2025).

2.3 Configuración y optimización del equipo ASIC Antminer S19 Pro

La correcta instalación y configuración de un equipo ASIC *(Application Specific Integrated Circuit)* es un paso fundamental para garantizar su operación eficiente y segura en entornos de minería de criptomonedas. En esta sección se describe detalladamente el proceso aplicado durante la puesta en marcha de un Antminer S19 Pro, incluyendo los aspectos eléctricos, de red, firmware y monitoreo. Para optimizar el rendimiento energético y operativo, se empleó el firmware personalizado Braiins OS, el cual mejora la eficiencia y amplía las opciones de control del equipo respecto al software de fábrica.

2.3.1 Preparación para la instalación del equipo ASIC Antminer S19 Pro

El equipo utilizado en este estudio de desempeño fue el Bitmain Antminer S19 Pro, uno de los modelos más utilizados en operaciones de minería de Bitcoin a nivel industrial. Este ASIC opera bajo el algoritmo SHA-256, el cual destaca por su alto rendimiento computacional y eficiencia energética. En la Tabla 2.2 se detallan sus especificaciones técnicas clave, necesarias tanto para la planificación del entorno eléctrico como para el diseño del sistema de ventilación en caso de ser necesario y el control térmico del equipo.

Especificaciones	**Valor**
Versión	S19 Pro
Algoritmo/monedas criptográficas	SHA 256/BTC/BCH
Tasa de hash (TH)	110 ± 3%
Potencia (W)	3,250 ± 5%
Eficiencia energética (J/TH)	29.5 ± 5%
Nivel de ruido (dB)	75 ± 5%
Voltaje de entrada de CA de la fuente de alimentación (voltios)	200~240
Corriente de entrada de CA de la fuente de alimentación (amperios)	20(1-3)
Modo de conexión de red	RJ45 Ethernet 10/100

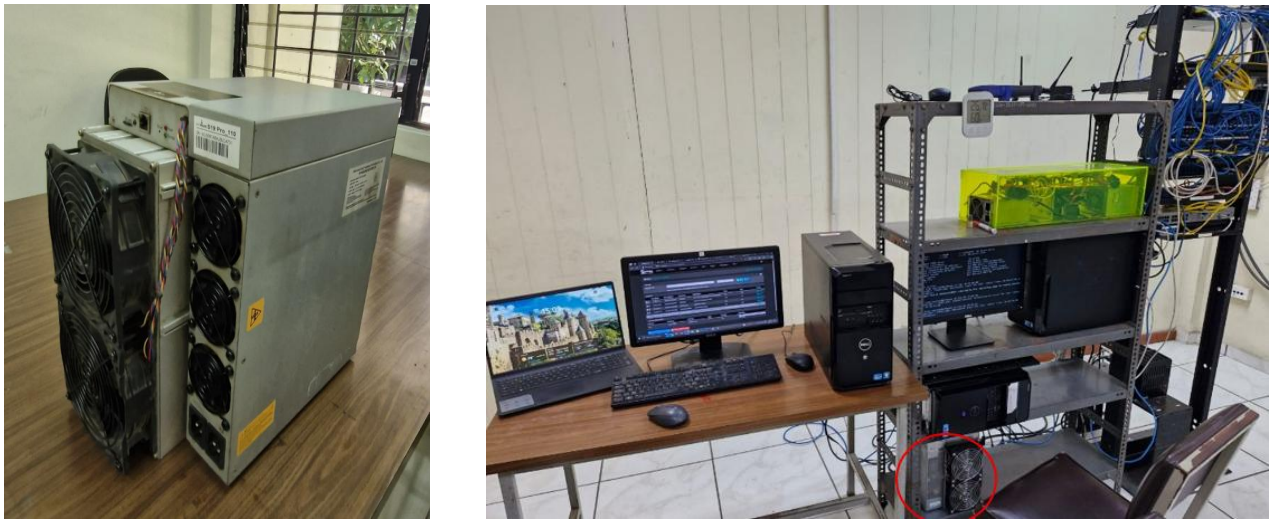
Tamaño del minero (largo x ancho x alto, sin embalaje), mm	370 x 195.5 x 290
Peso bruto, kg	15.2
Temperatura ambiente de funcionamiento (°C)	0 ~ 40
Temperatura ambiente de almacenamiento (°C)	-20 ~ 70
Humedad relativa de funcionamiento (sin condensación)	10 ~ 90%

Tabla 2.2 Detalles técnicos de Antminer S19 Pro.

El equipo opera a una potencia máxima de 3,412.5 W, según la tolerancia del fabricante (3,250 W ± 5 %). Este valor debe utilizarse como base para el dimensionamiento de la protección eléctrica y el cableado, garantizando así márgenes de seguridad adecuados para la operación continua. A un voltaje de 220 VAC y utilizando la potencia máxima, se obtiene una corriente de 15.51 A. Para garantizar una instalación segura y conforme a estándares internacionales, se selecciona un conductor de cobre calibre #10 AWG, el cual soporta hasta 30 A en instalaciones con conductores de un solo circuito, en condiciones normales de temperatura ambiente, de acuerdo con la Tabla 310.16 del NEC 2008 – NFPA 70 (NEC, 2008).

Además, se seleccionó una protección con interruptor termomagnético bipolar de 20 A, cumpliendo los criterios establecidos en la sección 240.4 (B) del NEC. También se instaló un cable de tierra de acuerdo con la Tabla 250.122 del NEC, donde se menciona que el mínimo calibre requerido para el conductor de tierra de cobre es #12 AWG. No obstante, se utilizó el mismo conductor de la fase (#10 AWG), para mejorar la capacidad de disipación de corrientes de falla.

Una vez completado el proceso de la conexión a la alimentación eléctrica del equipo se procede a ubica el Antminer, el cual tiene un peso y dimensiones considerables como se observa en la Tabla 2.2, considerando el nivel de ruido que puede alcanzar los 75 dB con carga máxima, se instaló en un área cerrada y con ventilación mínima para poder simular una condición de vivienda doméstica en El Salvador. En la Figura 2.8 (a) se puede observar el ASIC Antminer S19 Pro y en la Figura 2.8 (b) se muestra la instalación finalizada del equipo el cual está marcado con un círculo rojo.



(a) (b)

Figura 2.8 Fotografía del equipo Antminer S19 Pro, recien desempacado y en sitio de operación.

2.3.2 Configuración inicial del firmware

El Antminer S19 Pro incorpora de fábrica un firmware básico que permite acceder a su interfaz de configuración a través de un navegador web, utilizando una conexión de red mediante cable Ethernet RJ45 con velocidad 10/100 Mbps. El acceso inicial se realiza mediante credenciales predeterminadas, comúnmente configuradas como usuario: *root* y contraseña: *root*.

Para iniciar la configuración del equipo en red, se realizó la detección de su dirección IP local, necesaria para ingresar a la interfaz web. Esta tarea se llevó a cabo utilizando una herramienta de escaneo de red, *IP Scanner*, la cual permite identificar dispositivos conectados en la misma subred, facilitando así el acceso directo a través del navegador, en este caso resultó ser http://10.10.84.24 y al ingresar aparece una interfaz gráfica como se ilustra en la Figura 2.9. Aquí se muestra el firmware por defecto que trae el Antminer S19 Pro, el cual indica que se utiliza el algoritmo SHA256d, también se muestra una advertencia de que aún no está conectado a ningún *pool* por lo que no puede comenzar a minar.

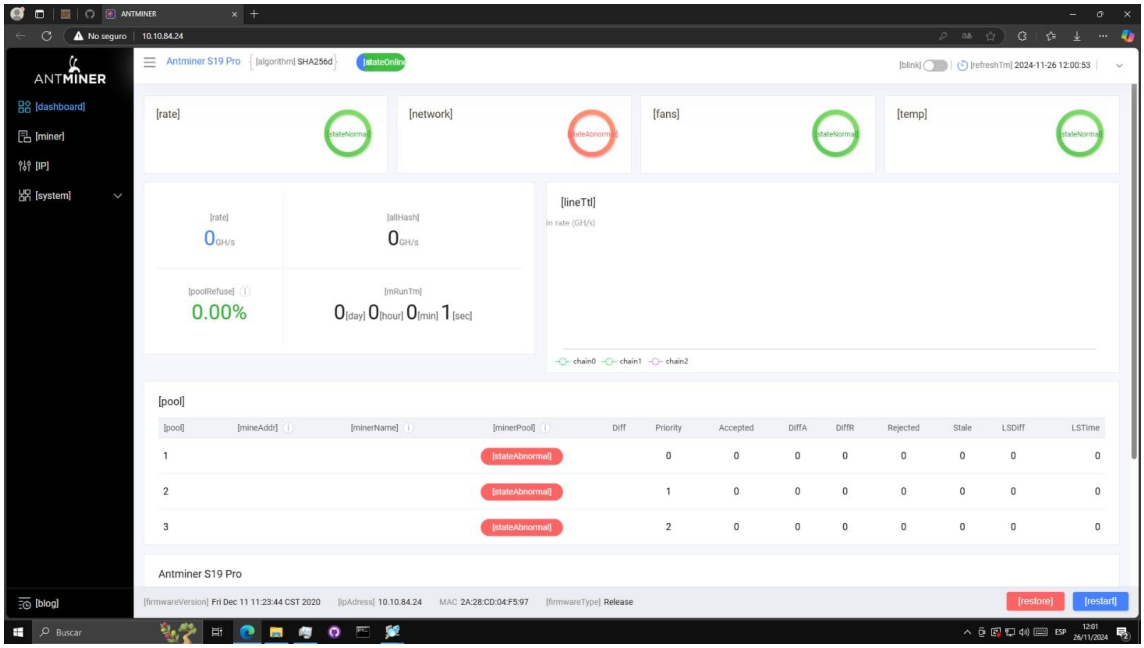


Figura 2.9 Página de inicio al ingresar al Antminer S19 Pro.

No obstante, este firmware presenta limitaciones operativas, particularmente en lo que respecta al control de la eficiencia energética, el ajuste de frecuencias de operación y la capacidad de registro detallado de datos del sistema. Estas restricciones pueden representar un obstáculo en entornos donde se requiere un control más preciso del consumo y el desempeño térmico del equipo. Por ello, se optó por instalar el firmware personalizado Braiins OS, desarrollado por el equipo de Braiins, creadores del primer *pool de minería*. Este firmware libre permite una gestión avanzada del ASIC a nivel de chip (Braiins, 2021).

El procedimiento de instalación fue el siguiente:

1. Descarga de la imagen de Braiins OS desde el sitio oficial.
2. Montaje de la imagen en una tarjeta microSD
3. Inserción de la tarjeta SD en el Antminer.
4. Energización del equipo, iniciando automáticamente el proceso de flasheo del firmware.

Finalizado este proceso, el equipo inició con la nueva interfaz como se muestra en la Figura 2.10, mucho más completa y visualmente intuitiva. Se desactivó el protocolo DHCP para evitar cambios en la IP y se asignó una IP estática (10.20.24.20) para facilitar el acceso remoto continuo.

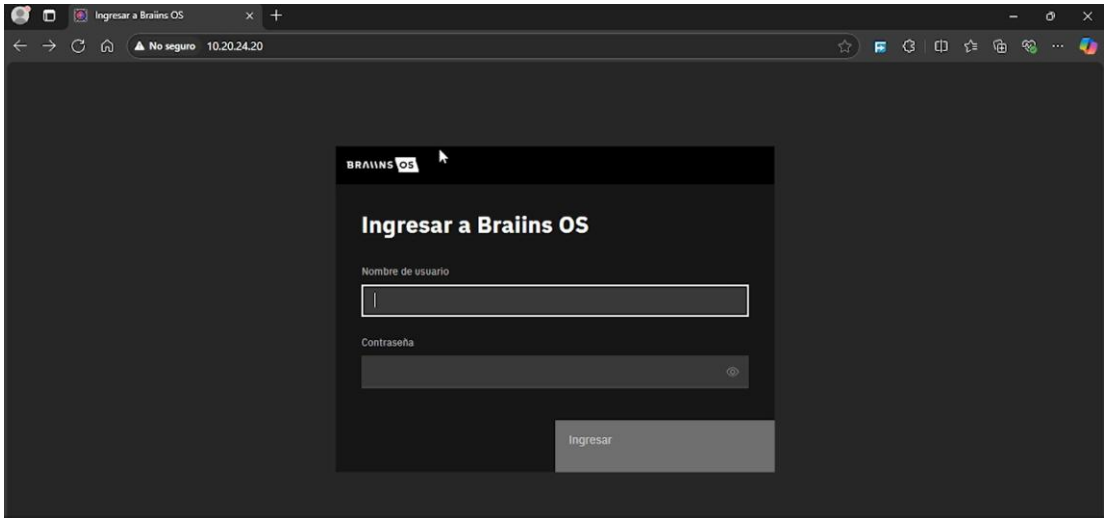


Figura 2.10 Página de inicio de Braiins OS

Posteriormente, se configuró la conexión al Braiins Pool, el cual se utilizó para tener un mejor entorno al utilizar Braiins OS, posteriormente se ingresaron los datos generados durante el registro en el *pool*. El equipo permite registrar hasta tres *pools* diferentes como se muestra en la Figura 2.11, donde se han agregado 3 distintos tipos de *pool*, operando en modo primario-secundario, es decir, en caso de fallo del *pool* principal, automáticamente comienza a trabajar con el siguiente configurado.

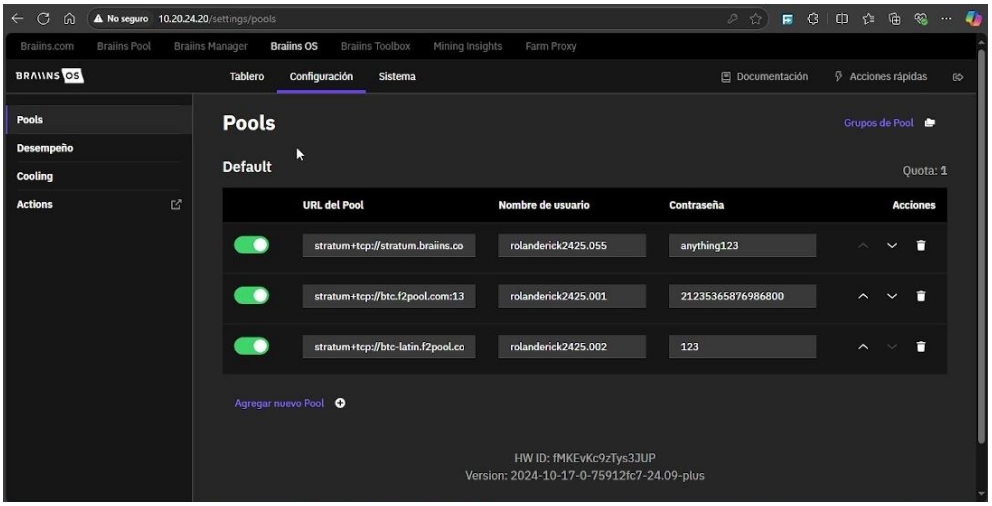


Figura 2.11 Configuración de los *pools* en el equipo minero.

2.3.3 Herramienta de análisis de desempeño

Una vez configurado el *pool de minería* y activado el firmware Braiins OS, el equipo inicia el proceso de minado. En este punto, el sistema incrementa automáticamente la velocidad de los ventiladores, generando un nivel de ruido cercano a las especificaciones del fabricante en operación máxima. En la Figura 2.12 se presenta la interfaz de monitoreo proporcionada por Braiins OS, donde se visualiza en tiempo real el comportamiento térmico y la *tasa de hash* del equipo durante una sesión de operación estable.

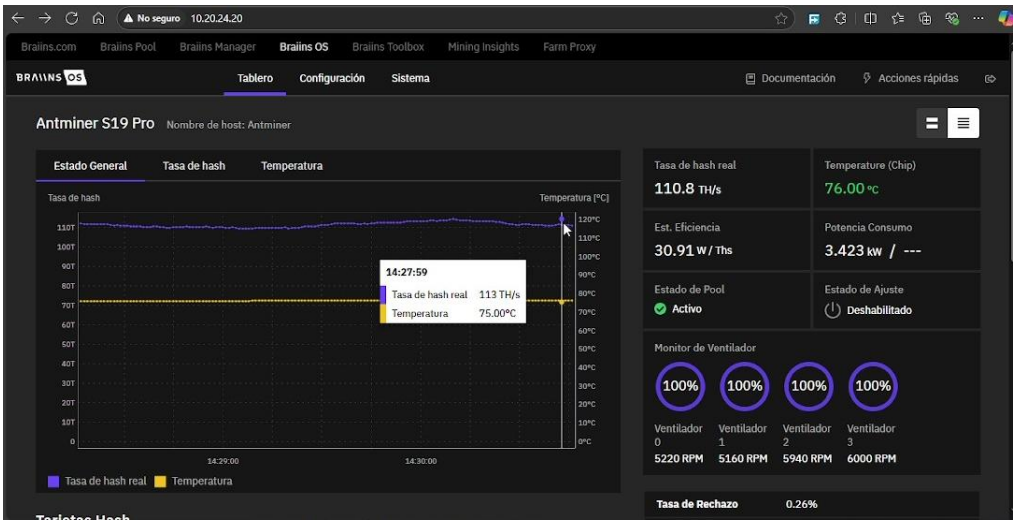


Figura 2.12 Interfaz de Braiins OS

A partir de los datos presentados en la Figura 2.12, se observa el comportamiento térmico y *tasa de hash* del Antminer S19 Pro durante una sesión de operación continua. La captura fue realizada con una temperatura ambiente de 33 °C, luego de cinco minutos de funcionamiento sostenido los chips ASIC alcanzaron una temperatura promedio de 76 °C, valor que se encuentra dentro del rango seguro de operación definido por el fabricante, que establece un umbral máximo de 95 °C para este modelo.

El equipo mantuvo una *tasa de hash* constante de 110.8 TH/s, con picos de hasta 113 TH/s, lo cual confirma la estabilidad del proceso de minado y el adecuado desempeño del sistema bajo condiciones térmicas moderadamente exigentes. Este resultado se encuentra dentro del rango esperado (110 ± 3 % TH/s), alcanzando los datos de las especificaciones técnicas del fabricante.

El consumo energético registrado fue de 3.423 kW, lo que representa el valor máximo dentro del margen de tolerancia especificado para este modelo (3,250 W ± 5 %). En consecuencia, la eficiencia energética se situó en 30.91 W/THs lo que es igual a 30.91 J/TH, apenas por encima del valor nominal de 29.5 J/TH. Esta diferencia es atribuible al incremento de la temperatura ambiente y a las condiciones reales de operación que reducen la eficiencia energética.

Por su parte, el sistema de ventilación operó al 100 % de capacidad, con velocidades que oscilaron entre 5,100 y 6,000 RPM en los tres ventiladores activos, garantizando una adecuada refrigeración del equipo. Este comportamiento corresponde a el incremento térmico asociado al entorno y al régimen de trabajo del ASIC.

En conjunto, los valores obtenidos durante la medición en campo confirman que el equipo opera dentro de los márgenes definidos por el fabricante, demostrando un desempeño térmico y computacional estable. Además, permiten validar que las condiciones eléctricas, térmicas y de red implementadas son técnicamente adecuadas para mantener el rendimiento y la seguridad operativa del sistema ASIC por un tiempo más prolongado.

2.4 Consideraciones finales

El análisis del presente capítulo permitió identificar que el uso de *hardware* especializado, como los ASIC, representa la opción más eficiente y rentable en la minería de Bitcoin. Modelos como el Antminer S21 Pro y el Whatsminer M66S Hydro ofrecen elevadas tasas de *hash* y un consumo energético optimizado, lo cual los posiciona como soluciones viables para operaciones de mediana y gran escala. La evolución desde CPU y GPU hacia ASIC refleja una clara tendencia hacia la especialización tecnológica en función del rendimiento computacional y la eficiencia energética.

Por otra parte, el software de minería cumple un rol esencial en la configuración, monitoreo y optimización del equipo. Soluciones como CGMiner, BFGMiner, EasyMiner y Braiins OS ofrecen distintos niveles de control, destacando este último por su capacidad de ajuste fino a nivel de chip. Asimismo, la participación en *pools* de minería como F2Pool o Braiins Pool permite mejorar la frecuencia de recompensas y maximizar la rentabilidad frente a la elevada dificultad de minado actual.

CAPÍTULO 3. DESEMPEÑO DEL EQUIPO ASIC ANTMINER S19 PRO

Este capítulo presenta la evaluación técnica y operativa del equipo ASIC Antminer S19 Pro bajo condiciones reales de funcionamiento. Para tal fin, se emplearon instrumentos especializados de medición eléctrica y térmica, con el objetivo de registrar parámetros clave como la *tasa de hash*, el consumo energético y la temperatura del equipo.

El análisis contempla la comparación entre las especificaciones nominales proporcionadas por el fabricante y las mediciones realizadas, así como la identificación de posibles variantes en el desempeño en entornos reales. Finalmente, se detallan las acciones de ajuste y optimización técnica implementadas para maximizar el rendimiento del equipo, contribuyendo a establecer lineamientos para una operación más eficiente y sostenible de equipos ASICs.

3.1 Evaluación del desempeño eléctrico y térmico del ASIC

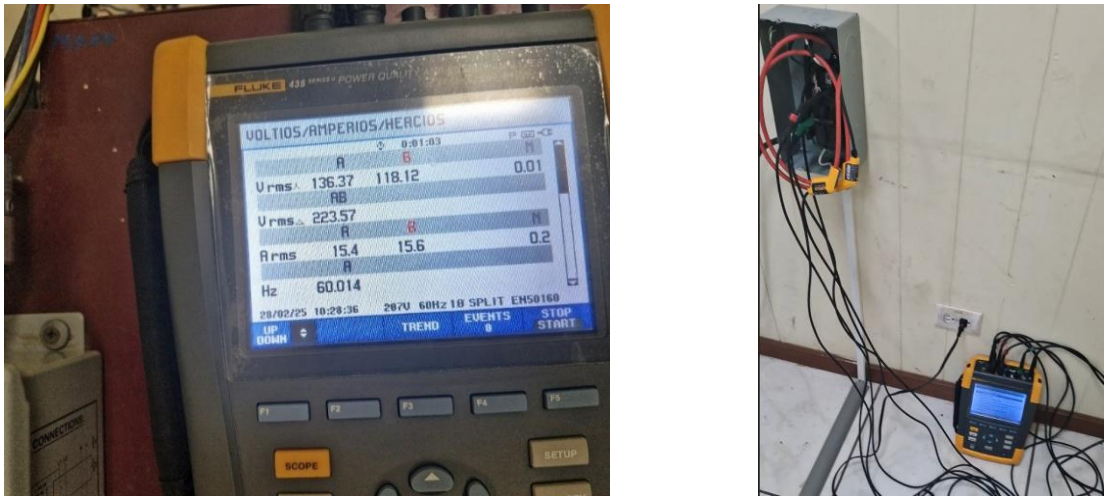
El análisis del desempeño eléctrico del Antminer S19 Pro tuvo como finalidad determinar su comportamiento energético en condiciones reales de operación. Esta evaluación se enfocó en registrar y analizar parámetros eléctricos fundamentales como tensión eléctrica o voltaje, corriente, potencia y frecuencia, los cuales son esenciales para caracterizar la eficiencia operativa del equipo durante procesos sostenidos de minería.

A través de la recopilación de datos en tiempo real, se identificaron patrones de consumo energético asociados a la actividad del equipo, evaluando su estabilidad operativa, respuesta ante cargas variables y el impacto de factores externos como la temperatura ambiente o la calidad del suministro eléctrico.

3.1.1 Medición de potencia eléctrica consumida por el ASIC

Para validar el comportamiento operativo del equipo Antminer S19 Pro durante el proceso de minería, se empleó un analizador de redes Fluke 435, tal como se muestra en la Figura 3.1. El Fluke 435 cuenta con funcionalidades avanzadas para el monitoreo de calidad de energía, como análisis de armónicos, transitorios, desequilibrio de fases y eventos de distorsión, lo cual permite

obtener una caracterización completa del entorno eléctrico. Su portabilidad y compatibilidad con sistemas monofásicos y trifásicos lo hacen ideal para entornos de evaluación técnica y validación de equipos de alto consumo energético como los ASIC (Fluke, s.f.).



(a) (b)

Figura 3.1 Fotografía de conexión y mediciones de analizador de redes

En la medición registrada en la Figura 3.1, se observa una tensión eficaz (*Vrms*) de aproximadamente 223.57 V, correspondiente al valor nominal de la red monofásica utilizada. Asimismo, la corriente eficaz (*Arms*) se encuentra en un rango de 15.4 a 15.6 Amperios, lo que refleja el consumo real del equipo durante operación continua. La frecuencia registrada fue de 60.01 Hz, lo que confirma la estabilidad del suministro eléctrico durante la sesión de prueba.

A partir de estos datos, fue posible realizar un cálculo de eficiencia energética instantánea, tomando como referencia un momento especifico durante el funcionamiento del equipo. La potencia eléctrica absorbida se calcula de la siguiente manera:

$$P = VxI = 223.57\,V\,x\,15.6\,A = 3{,}487.69\,W \approx 3.49\,kW$$

Dado que se configuró el Antminer S19 Pro para que operara a una *tasa de hash* de 110.8 TH/s, tal como se mostró en la Figura 2.12, con estos datos se puede realizar el cálculo de la eficiencia energética, un menor valor de J/TH indica una mayor eficiencia energética.

$$Eficiencia = \frac{3{,}487.69\,W}{110.8\,TH/s} \approx 31.48\,J/TH$$

Este resultado corresponde a un valor puntual, útil únicamente para caracterizar la eficiencia operativa en un instante específico del ciclo de operación, con esto solo se puede observar como el equipo opera con una eficiencia ligeramente inferior a la que se mostró en la Tabla 2.2, donde se especifica que tiene un valor promedio de 29.5 J/TH, la diferencia puede atribuirse a factores como la temperatura ambiente a la que se encuentra el equipo.

3.1.2 Mediciones térmicas del equipo ASIC

Otro parámetro importante por medir es la temperatura alcanzada en las conexiones eléctricas y en el equipo ASIC Antminer S19 Pro. Para esto se empleó una cámara termográfica FLIR i7, para registrar sin contacto la temperatura superficial en las conexiones eléctricas del Antminer S19 Pro. Este modelo utiliza un microbolómetro no refrigerado que detecta radiación en el espectro 7.5 a 13 µm, con una resolución de 140 × 140 píxeles, sensibilidad térmica <0.1 °C (NETD) y precisión de ±2 °C.

El rango de medición térmica va desde –20 °C hasta +250 °C, adecuado para aplicaciones eléctricas e industriales. Las imágenes se capturan en una tarjeta microSD con posterior análisis vía FLIR Tools. Para las mediciones en este estudio, la cámara se posicionó a una distancia aproximada de 60 cm, su distancia mínima focal, lo cual permite una lectura térmica confiable sobre superficies eléctricas compactas como interruptores o terminales (Flir Systems, s.f.).

Primero se realizaron mediciones de temperatura en las conexiones eléctricas, pues se esperaba un alto consumo de potencia y se buscaba identificar posibles concentraciones de calor tanto en el subtablero eléctrico instalado, como en los conductores. En la Figura 3.2 se observa que la temperatura superficial del subtablero eléctrico con el interruptor térmico de 20 A dos polos registra una temperatura de 33.5 °C, esta es una temperatura que se encuentra en el rango operativamente seguro, ya que según el estándar UL489, la elevación máxima permitida en terminales de breakers estándar es de 50 °C (Schneider Electric, 2017).

Figura 3.2 Medición de temperatura de subtablero eléctrico

Por otra parte, el comportamiento térmico del Antminer S19 Pro, alcanza temperaturas de hasta 45.3 °C en la carcasa externa de los ventiladores y zonas cercanas a los disipadores de calor, lo cual se ilustra en la Figura 3.3. Si bien estos valores todavía están dentro de un rango operativo que no perjudica el rendimiento del equipo, se empieza a reflejar que el entorno presenta una ventilación limitada. Estos datos preliminares sirven para tener la línea base para futuras pruebas en un periodo mayor, ya que el ASIC Antminer S19 Pro que en el que se están realizando las pruebas es reutilizado y previamente se realizó un mantenimiento preventivo en el equipo (cambio de pasta térmica y limpieza interna), entonces es necesario realizar estas pruebas antes de su funcionamiento por un periodo de tiempo más amplio.

(a)

(b)

Figura 3.3 Medición de temperatura de Antminer S19 Pro

3.2 Resultados obtenidos en un entorno operativo real

Con el fin de evaluar el comportamiento real del equipo Antminer S19 Pro en un periodo mayor, se llevó a cabo un análisis técnico basado en un monitoreo eléctrico continuo durante un intervalo de 24 horas. Esta evaluación permitió obtener un perfil de su consumo energético, estabilidad operativa, respuesta térmica y calidad de energía, bajo un entorno no climatizado representativo de las condiciones comunes en El Salvador.

En los siguientes párrafos se presentan los detalles metodológicos, los registros eléctricos obtenidos y el análisis técnico del rendimiento diario del equipo, considerando variables como la energía activa (Wh), el factor de potencia, la distorsión armónica (THD), los armónicos presentes y el impacto térmico sobre su desempeño.

3.2.1 Metodología de medición continua

Para evaluar el comportamiento energético del equipo Antminer S19 Pro bajo condiciones reales de operación, se implementó un monitoreo continuo de 24 horas utilizando un analizador de redes Fluke 435, reconocido por su precisión en el registro de parámetros eléctricos. Las mediciones se realizaron cada segundo ya que así se podrá obtener un mejor análisis respecto a cómo se va comportando el equipo cuando va cambiando la temperatura en el lugar donde se encuentra instalado.

Las mediciones se realizaron un fin de semana porque, en pruebas anteriores, el nivel de ruido era muy alto, llegando a 75 dB, y el área era muy pequeña y mal ventilada. Entonces las mediciones se realizaron desde el 1 de marzo de 2025 a las 10:45 a. m. hasta el 2 de marzo de 2025 a las 10:44 a. m. lo cual permitió observar directamente el efecto de la temperatura sobre el rendimiento eléctrico, tal como se muestra en el histograma representado en la Figura 3.4 donde se ve la potencia en vatios en el “eje x” y el número de eventos o mediciones realizadas en el “eje y”, aquí se muestra en el centro del histograma que el dato que aparece con más frecuencia (800 veces), estuvo entre 3,408 W y 3,420 W durante todo el periodo de mediciones.

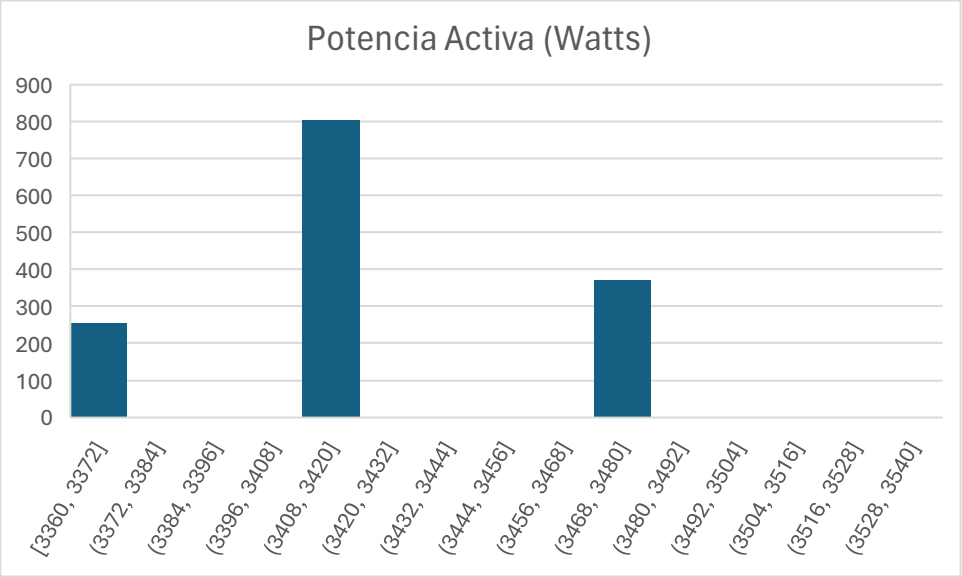


Figura 3.4 Potencia activa promedio

En este intervalo de tiempo, se registraron de forma continua variables clave como tensión, corriente, frecuencia, potencia activa (W), energía consumida, THD (*Total Harmonic Distortion*) y presencia de armónicos específicos. Estas mediciones permiten caracterizar no solo la estabilidad del sistema, sino también los efectos que una carga no lineal como un ASIC puede inducir sobre la red de distribución.

3.2.2 Comportamiento energético durante un día de prueba

Durante las 24 horas de operación continua, el analizador de redes registró un consumo total acumulado de 81,855 Wh, que corresponde únicamente al equipo Antminer S19 Pro. Este valor representa la energía activa consumida por el equipo de minería, excluyendo cargas auxiliares y pérdidas del sistema eléctrico. En la Figura 3.5 se muestra la acumulación del consumo energético durante el periodo registrado, graficada mediante el software Power Log 5.9.

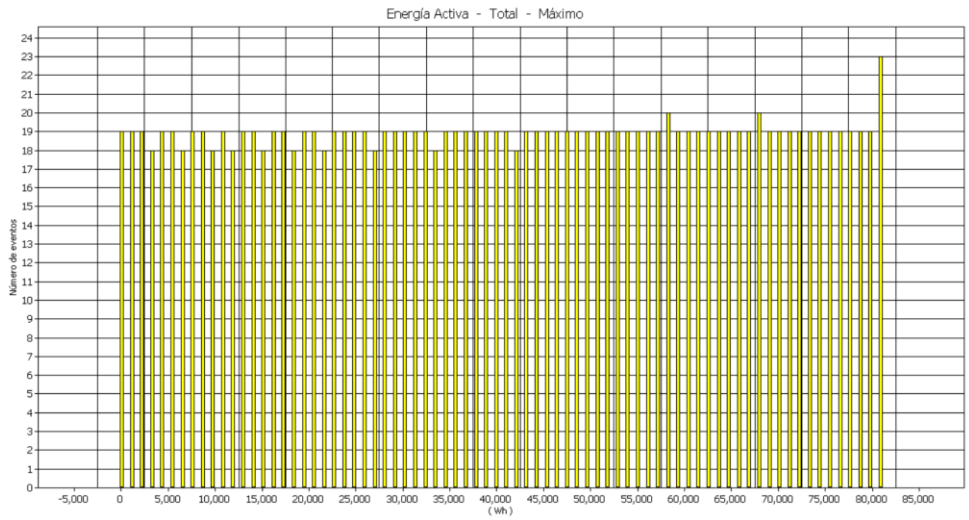


Figura 3.5 Energía total medida durante 24 horas

Una alternativa para representar gráficamente el consumo de energía es analizar su comportamiento en cada momento específico. La Figura 3.6 ilustra la cantidad de energía consumida por el sistema en intervalos de un minuto. Se identificaron periodos de mayor consumo entre las 13:00 y 15:00 horas, coincidiendo con las horas de mayor temperatura ambiente. También se identificó que el menor consumo se registró entre las 00:00 y 04:00 horas. Este fenómeno está relacionado nuevamente con el cambio en la velocidad de los ventiladores del equipo, que responden a la carga térmica interna, aumentando o disminuyendo el consumo eléctrico.

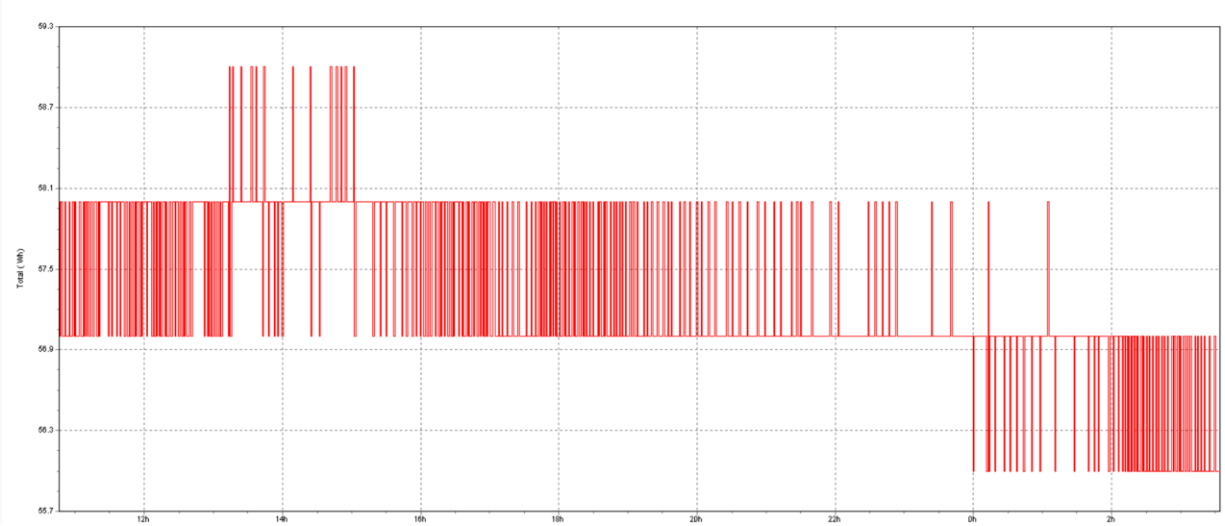


Figura 3.6 Energía activa registrada por analizador de redes

Es importante destacar que durante todo el período de monitoreo no se registraron interrupciones, desconexiones ni fluctuaciones significativas en la tensión, lo que confirma que la red de alimentación logró mantener condiciones estables para el funcionamiento continuo del ASIC. Este comportamiento es esencial para garantizar la continuidad del proceso de minado de forma segura. De lo contrario, sería necesario disponer de un UPS (Fuente de Alimentación Ininterrumpida, del inglés, *Uninterruptible Power Supply*) o un sistema de baterías de respaldo de gran capacidad, capaz de sostener durante varias horas la demanda de 3.5 kW del equipo ASIC.

3.2.3 Variación de la eficiencia durante el día de prueba

La eficiencia energética del equipo Antminer S19 Pro se define como la cantidad de energía eléctrica consumida por cada unidad de *hash*, comúnmente expresada en Joules por terahash (J/TH). Esta métrica es fundamental para evaluar el rendimiento operativo de dispositivos ASIC, ya que permite comparar el desempeño real, frente a las especificaciones dadas por el fabricante.

Durante el intervalo de 24 horas, se estimó una *tasa de hash* constante de 110 TH/s. Con base en el consumo total acumulado de 81,855 Wh, registrado por el analizador de redes, se calculó la eficiencia promedio de esas 24 horas de la siguiente manera.

Primero, se convirtió el valor de energía total a Joules:

$$E_{total} = 81{,}855\,Wh \times 3600\frac{J}{Wh} = 294{,}678{,}000\,J$$

Luego, se determinó la producción total de hashes durante las 24 horas (86,400 s):

$$110\,\frac{TH}{s} \times 86{,}400\,s = 9{,}504{,}000\,TH$$

Finalmente, la eficiencia promedio se obtuvo mediante:

$$Eficiencia = \frac{294{,}678{,}000\,J}{9{,}504{,}000\,TH} \approx 31\,J/TH$$

Este resultado refleja una eficiencia aproximada de 31 J/TH, ligeramente peor (mayor consumo por hash) que el valor nominal de 29.5 J/TH indicado por el fabricante, pero mejor que la eficiencia calculada en el instante puntual anteriormente (31.48 J/TH). La mejora relativa en la eficiencia

promedio puede explicarse por un comportamiento más estable durante las horas nocturnas, cuando la temperatura ambiente disminuyó y el sistema de ventilación no requirió operar a máxima capacidad.

Sin embargo, al examinar el comportamiento operativo en franjas horarias específicas, se identificaron mejoras puntuales en la eficiencia bajo ciertas condiciones. Entre las 00:00 y las 04:00 horas, cuando la temperatura ambiente fue más baja, se observó una disminución en el consumo eléctrico del sistema debido a la menor carga térmica. En consecuencia, los ventiladores no requirieron funcionar a toda su potencia, y la eficiencia energética mejoró alcanzando valores del orden de 29.97 J/TH. Este valor óptimo se registró en las horas de la madrugada y coincide con lo observado en la interfaz de monitoreo en tiempo real del dispositivo como se muestra en la Figura 3.7, proveniente del firmware Braiins OS, donde se evidencia una menor temperatura de los chips alrededor de las 3:00 a. m., contribuyendo a un desempeño más eficiente.

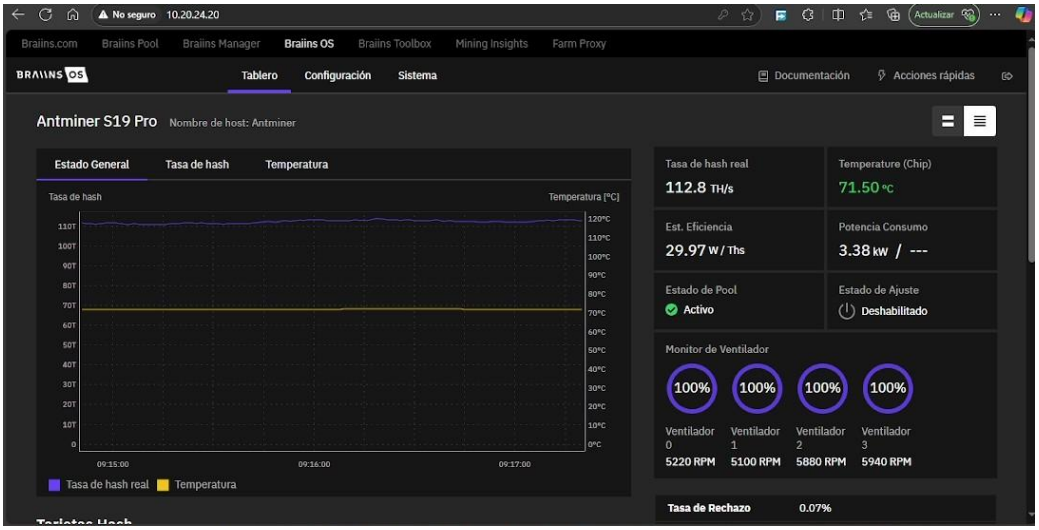


Figura 3.7 Temperatura de chip mínima registrado a las 3 am

3.2.4 Evaluación de distorsión armónica y calidad de energía

Uno de los efectos más relevantes en la operación de cargas no lineales como el Antminer S19 Pro es la generación de distorsión armónica en la red eléctrica llamado THD (*Total Harmonic Distortion*). Este fenómeno ocurre cuando el equipo absorbe corriente de forma no senoidal,

generando componentes adicionales a la frecuencia fundamental (60 Hz), lo que puede afectar tanto la eficiencia del sistema como la vida útil de otros dispositivos conectados.

Durante la medición continua de 24 horas, se registró el espectro de distorsión armónica de la tensión de suministro utilizando el analizador Fluke 435. En la Figura 3.8 se observa que los niveles de distorsión armónica en la tensión se mantuvieron bajos; por ejemplo, en la fase A el tercer armónico alcanzó un máximo de 4.231 % de la componente fundamental. Estos niveles se consideran aceptables dentro de estándares internacionales, lo que indica que la red de alimentación posee una adecuada capacidad de absorción o compensación frente a los armónicos inducidos por cargas no lineales como las de equipos de minería ASIC.

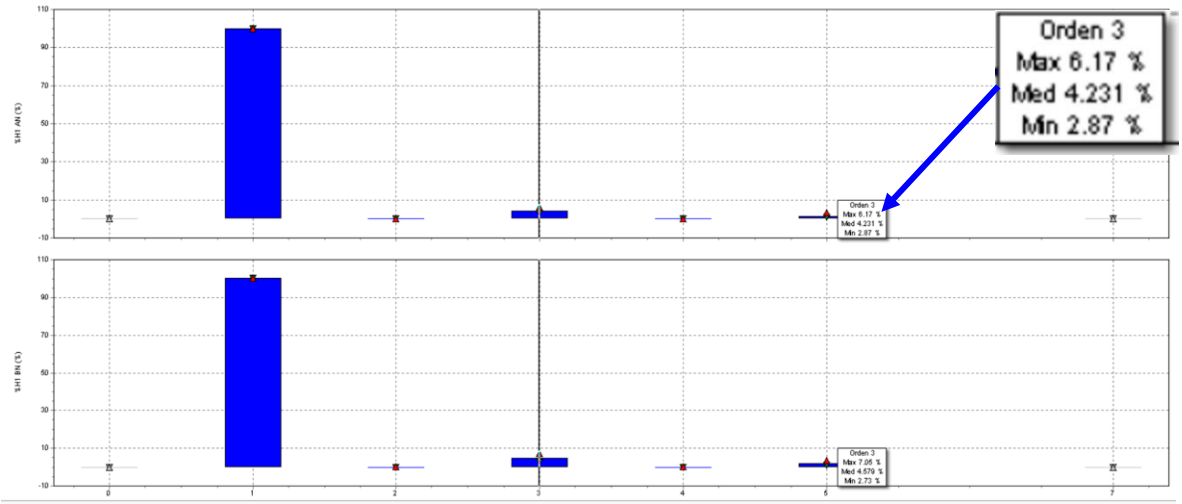


Figura 3.8 Espectro de armónicos en tensión THDv

En contraste con la tensión, la Figura 3.9 muestra el espectro armónico de corriente registrado en las mismas condiciones de operación. Se identifica una fuerte concentración de distorsión en el tercer armónico, con un valor máximo de 9.2 %, una media de 9.06 % y un valor mínimo de 8.93 %. Este comportamiento es típico en sistemas con cargas electrónicas con fuentes de alimentación conmutadas, como el Antminer S19 Pro, las cuales generan una forma de onda de corriente altamente distorsionada. Un nivel de distorsión de corriente de esta magnitud puede generar problemas en instalaciones eléctricas, tales como sobrecalentamiento de transformadores, resonancias indeseadas o el mal funcionamiento de dispositivos de protección, si no se implementan medidas de mitigación adecuadas.

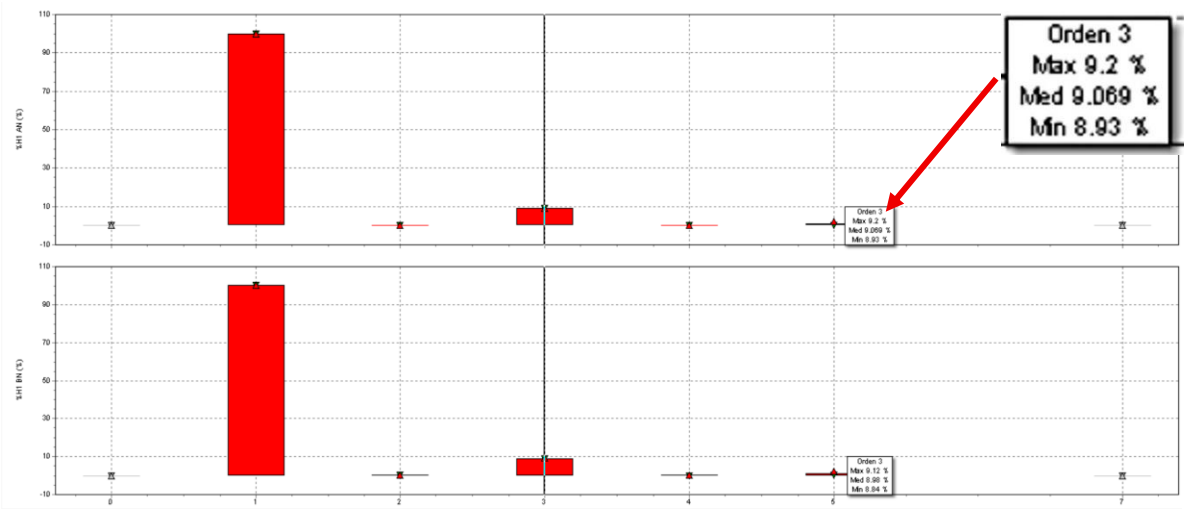


Figura 3.9 Espectro de armónicos en corriente THDi

Según la norma *IEEE 519-2014*, los límites recomendados para THD de tensión en sistemas de distribución de baja tensión deben mantenerse por debajo del 5 % para evitar problemas en la operación de equipos sensibles. En el presente estudio, se verificó que los niveles de distorsión armónica en la tensión de suministro no superaron el rango permitido, garantizando una calidad de energía adecuada para una operación segura del ASIC (IEEE, 2014).

Sin embargo, los elevados valores de THD en corriente son característicos de cargas como los ASIC, que emplean fuentes conmutadas con un bajo factor de cresta. El análisis espectral reveló la presencia predominante de armónicos de 3º, 5º y 7º orden, siendo estos los de mayor intensidad, como se observa en la Figura 3.8 y Figura 3.9. Estos armónicos, aunque no afectaron directamente al equipo durante el período de prueba, pueden representar un riesgo si existen otras cargas conectadas en paralelo.

Este análisis confirma que, si bien el THDv fue conforme a norma, el THDi requiere atención técnica específica en la etapa de planificación eléctrica. Un THDi elevado puede generar efectos adversos como el sobrecalentamiento de neutros y conductores, pérdida de eficiencia en transformadores, disparos erráticos en protecciones diferenciales y térmicas, así como una mayor susceptibilidad a interferencias electromagnéticas.

3.2.5 Impacto de la temperatura ambiente en el rendimiento

La temperatura ambiente es un factor crítico en el rendimiento operativo de equipos ASIC, ya que afecta directamente el comportamiento térmico interno, el régimen de funcionamiento de los ventiladores y, en consecuencia, la eficiencia energética del proceso de minería. Durante las 24 horas de monitoreo continuo del Antminer S19 Pro, no se utilizaron sistemas de climatización externa, lo que permitió evaluar la capacidad del equipo para operar bajo condiciones térmicamente exigentes.

Las mediciones infrarrojas realizadas con la cámara FLIR mostraron temperaturas superficiales de hasta 45.1 °C en zonas cercanas a los ventiladores y disipadores, mientras que las temperaturas internas del equipo, obtenidas a través del software de monitoreo, alcanzaron picos de 90 °C en los chips de Antminer S19 Pro. Estos valores, si bien se encuentran dentro del rango tolerado por el fabricante, indican una carga térmica significativa que condiciona el comportamiento eléctrico del sistema.

Durante las horas de mayor temperatura ambiente (entre las 13:00 y las 17:00), se observó un aumento significativo en la velocidad de los ventiladores integrados, los cuales ajustan su funcionamiento de manera automática para mantener la integridad térmica del equipo. Este incremento en el caudal de aire conlleva un mayor consumo eléctrico, dado que los ventiladores representan una carga auxiliar que, aunque esencial, no contribuye directamente al proceso de cálculo criptográfico.

En contraste, durante las horas nocturnas (a partir de las 20:00), la temperatura ambiente descendió considerablemente, reduciendo el trabajo de los ventiladores y permitiendo una operación más eficiente, pues alcanza los 112.8 TH/s, como se mostró en la Figura 3.6. Por tanto, se concluye que la temperatura ambiente afecta directamente el rendimiento energético del equipo, y que una adecuada gestión térmica del entorno es crucial para lograr un equilibrio óptimo entre rendimiento, eficiencia y la vida útil del hardware.

3.3 Comparación entre valores medidos y valores dados por el fabricante

Este apartado tiene como objetivo evaluar las diferencias entre el comportamiento operativo real del equipo Antminer S19 Pro y los valores nominales establecidos por el fabricante. La

comparación permite identificar diferencias, validar el rendimiento técnico en condiciones locales y establecer recomendaciones para la implementación eficiente de este tipo de equipos en entornos distintos al de laboratorio.

Se analizan variables clave como la *tasa de hash*, el consumo eléctrico, la eficiencia energética, el comportamiento térmico, la calidad del suministro eléctrico y la distorsión armónica de la red. Estos factores son determinantes para evaluar si el equipo cumple con su desempeño esperado o si requiere ajustes en su entorno operativo para alcanzar niveles óptimos de eficiencia y estabilidad.

3.3.1 Parámetros eléctricos medidos y del fabricante

Según la ficha técnica oficial proporcionada por Bitmain, el equipo ASIC Antminer S19 Pro presenta los siguientes valores operativos bajo condiciones de diseño estándar, esto es, en un entorno controlado a 25 °C, alimentación eléctrica estable, buena ventilación y sin perturbaciones eléctricas significativas:

- Tasa de hash: 110 TH/s
- Consumo eléctrico: 3,250 W ±5 %
- Eficiencia energética: 29.5 J/TH
- Temperatura de operación: 0 °C a 40 °C
- Nivel de ruido: 82 dB
- Factor de potencia: ≥ 0.95
- Distorsión armónica (THD): no indicado por el fabricante

Estos parámetros están diseñados para ser alcanzados en entornos ideales y, por lo tanto, constituyen un punto de referencia para el análisis de rendimiento en condiciones reales de operación. Durante la evaluación del Antminer S19 Pro bajo condiciones reales en El Salvador, se registraron los siguientes datos, que se comparan en la Tabla 3.1 con los valores nominales proporcionados por el fabricante.

Parámetro	Valor nominal (Bitmain)	Valor medido (real)	Desviación estimada
Tasa de hash	110 TH/s	110.3 TH/s	0.27%
Consumo eléctrico	3,250 W	3,465 – 3,487 W	6.90%
Eficiencia energética promedio	29.5 J/TH	31 J/TH	−9.1 %
Temperatura interna (máx.)	≤ 80 °C	75 °C	Dentro de rango
THD de tensión	≤ 5 % (IEEE 519-2014)	1.3 – 2.1 %	Conforme
THD de corriente	≤ 18 %	Hasta 9 %	Alto

Tabla 3.1 Tabla comparativa de valores reales con valores medidos durante 24 horas

Los valores presentados evidencian un comportamiento muy cercano a lo esperado, según especificaciones del fabricante. Aunque el consumo eléctrico fue superior al teórico, la eficiencia global fue mejor. Esto se puede atribuir a las condiciones particulares de operación y a la estabilidad eléctrica observada durante el monitoreo.

3.3.2 Parámetros térmicos medidos y del fabricante

Durante el periodo de monitoreo continuo de 24 horas, se evaluó la estabilidad operativa del equipo Antminer S19 Pro en condiciones reales, enfocándose en su capacidad para mantener una operación ininterrumpida, sin pérdidas de rendimiento ni eventos de desconexión eléctrica. La evaluación se facilitó gracias a los registros horarios proporcionados por el analizador de redes Fluke 435, lo que permitió observar el comportamiento eléctrico de manera detallada, minuto a minuto.

Entre el 1 de marzo a las 10:45 a. m. y el 2 de marzo a las 10:44 a. m., el equipo operó de manera continua, sin reinicios ni anomalías. La frecuencia de suministro se mantuvo estable en torno a 60.01 Hz, y la tensión osciló entre 223.4 V y 224.1 V, sin caídas ni sobrevoltajes significativos. Esto confirma que el sistema eléctrico local es adecuado para soportar la operación del ASIC sin

necesidad de reguladores ni UPS. No se registraron disparos de protecciones ni desconexiones, lo que demuestra la capacidad del sistema para alimentar cargas constantes de aproximadamente 3.4 kW.

El análisis horario permitió identificar tres periodos diferenciados en el comportamiento del equipo:

- **Periodo diurno crítico** (13:00–17:00): Se registró el mayor incremento en la demanda energética, correlacionado con las horas de mayor temperatura ambiental. Durante este periodo, el sistema de ventilación operó a máxima capacidad, lo que aumentó el consumo eléctrico, aunque sin afectar la estabilidad de la *tasa de hash*.
- **Periodo nocturno** (20:00–6:00): Las condiciones térmicas se estabilizaron, lo que redujo la carga de los ventiladores. Durante estas horas, se observó la mayor eficiencia energética, con un consumo estable y sin perturbaciones armónicas significativas.
- **Periodo de transición** (10:45–13:00 y 6:00–10:45): En estos periodos, se detectó un comportamiento progresivo tanto en el aumento como en la disminución del consumo, lo que reflejó la respuesta térmica gradual del sistema conforme variaba la temperatura ambiental.

La corriente absorbida por el equipo se mantuvo entre 15.2 A y 15.7 A, lo que confirma la estabilidad operativa durante todo el ciclo de prueba. Este comportamiento estable es fundamental para asegurar la rentabilidad de las operaciones de minería, ya que previene penalizaciones por desconexión en *pools de minería* y maximiza la productividad diaria del equipo.

Desde el punto de vista térmico, las mediciones registraron temperaturas superficiales de hasta 45.1 °C y temperaturas internas máximas de 90 °C en los chips. Aunque no se superaron los umbrales de seguridad, la operación a altas temperaturas incrementó el consumo energético, lo que demuestra que, para periodos superiores a 24 horas, es imprescindible diseñar un sistema de refrigeración o aislamiento térmico que asegure el funcionamiento a largo plazo.

Finalmente, se comprobó que el equipo fue capaz de operar de manera autónoma durante todo el ciclo de prueba sin intervención externa, sin reinicios, y manteniendo una *tasa de hash* constante de 110 TH/s. Este comportamiento refuerza la viabilidad técnica del uso de equipos ASIC en el contexto salvadoreño, incluso en condiciones no climatizadas.

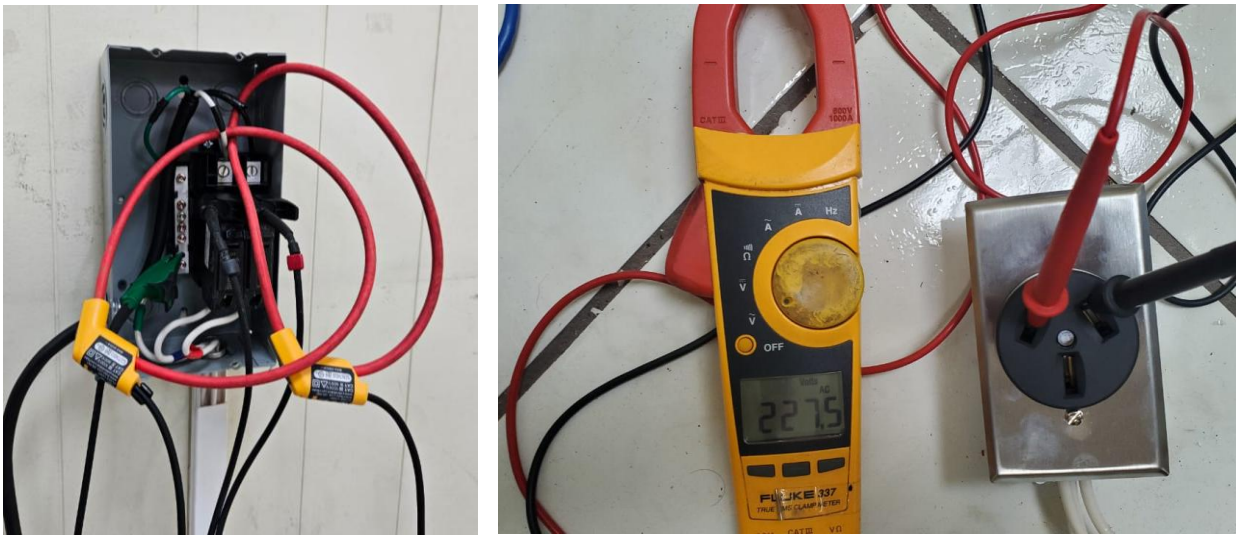
3.4 Condiciones de prueba y desafíos en la instalación

Para el desarrollo de este proyecto de investigación, fue necesario ejecutar varios ciclos de prueba, los cuales resultaron exitosos. Los resultados obtenidos coincidieron con los datos técnicos proporcionados por el fabricante del ASIC Antminer S19 Pro, confirmando que tanto el comportamiento eléctrico como térmico del equipo se mantuvieron dentro de los márgenes esperados. Esto valida el desempeño del dispositivo bajo las condiciones climáticas de El Salvador.

Sin embargo, antes de realizar las pruebas bajo condiciones ambientales reales, se presentaron diversas limitaciones que afectaron la precisión de las mediciones. Una de las principales dificultades fue la falta de climatización en el local destinado a las pruebas, lo que dificultó el control de la temperatura. Esto generó picos térmicos que podrían haber alterado el comportamiento del equipo.

A pesar de no contar con un sistema de climatización, se aprovechó la ventilación natural abriendo puertas y ventanas, lo que permitió una circulación de aire suficiente para prevenir el sobrecalentamiento. Durante la noche, las temperaturas más bajas favorecieron el rendimiento eléctrico al facilitar la disipación del calor, lo que redujo el riesgo de sobrecalentamiento y mejoró la eficiencia operativa.

En el proceso de poner en marcha el equipo ASIC, surgieron dificultades adicionales relacionadas con la conexión eléctrica. Al tratarse de un dispositivo de segunda mano, el Antminer S19 Pro no incluía el alimentador eléctrico original, y estaba diseñado para operar a 220 V mediante un conector específico. Para resolver esta limitación, fue necesario construir y adaptar un alimentador con el cable de calibre adecuado para soportar la corriente nominal del equipo, tal como se muestra en la Figura 3.10. Debido a la incompatibilidad del conector original, se realizó una instalación eléctrica alternativa.



(a) (b)

Figura 3.10 Adaptación de la instalación eléctrica para el ASIC

Esta adaptación requirió de una supervisión constante para asegurar que no ocurrieran sobrecalentamientos en la infraestructura eléctrica, incluyendo, el subtablero con su interruptor térmico, cables, tomacorrientes. Así se garantizó la seguridad y estabilidad de la conexión durante las pruebas. A continuación, se destacan cuatro factores clave para una adecuada instalación y operación del equipo ASIC:

1. **Acceso a una línea eléctrica de 220 VAC**: La mayoría de los hogares en El Salvador no cuentan con instalaciones a 220 V Finalmente, se utilizó un espacio con acceso a una tensión eléctrica de 220 V monofásico y un regulador de alta potencia, lo cual fue esencial para el funcionamiento del ASIC.
2. **Disponibilidad de un regulador de voltaje adecuado**: El regulador fue esencial para proteger al equipo contra variaciones de voltaje, evitando picos o caídas inesperadas que podrían haber dañado el hardware. Este dispositivo garantizó la estabilidad del suministro eléctrico durante las pruebas.
3. **Suficiente ventilación del espacio**: Aunque no se disponía de sistemas de ventilación forzada, como extractores o aire acondicionado, el espacio contaba con ventanas que permitieron un flujo de aire natural a temperatura ambiente. Aunque no era la opción ideal, esta ventilación fue suficiente para mantener una temperatura interna aceptable durante las pruebas, evitando que el equipo alcanzara temperaturas peligrosas.

4. **Nivel de ruido generado durante la operación:** El ruido emitido supera los niveles tolerables en espacios cerrados sin aislamiento acústico, convirtiéndose en una molestia y un factor intrusivo en entornos concurridos. Por esta razón, se decidió realizar ciclos de prueba de 24 horas durante un fin de semana. Esta consideración sería relevante para instalaciones domésticas, con mayor afluencia de personas.

A pesar de los desafíos presentados, las condiciones de prueba ofrecieron una valiosa oportunidad para evaluar el comportamiento del Antminer S19 Pro en un entorno bastante adverso, especialmente por la falta de control para mantener la temperatura baja durante el día. La experiencia obtenida demostró que, con ajustes mínimos y bajo ciertas condiciones, el equipo puede operar correctamente incluso en espacios sometidos a temperatura ambiente no completamente controladas.

CAPÍTULO 4. ANÁLISIS ECONÓMICO Y DE RENTABILIDAD PARA LA MINERÍA DE CRIPTOMONEDAS

En este capítulo se presenta un análisis técnico y financiero que permite determinar la viabilidad de un proyecto de minería de criptomonedas en El Salvador. Se consideran escenarios con diferentes modelos de hardware, tarifas eléctricas y proyecciones de precio de Bitcoin. Además, se evalúa el impacto del *halving*, el crecimiento estimado del valor de BTC y la dificultad de la red. El estudio incluye indicadores como ROI, VAN y TIR. Finalmente, se incorporan comparaciones internacionales y consideraciones del marco regulatorio local.

4.1 Análisis de costos: inversión, operación y mantenimiento

En un proyecto de minería de Bitcoin es imprescindible un análisis detallado de costos para evaluar su viabilidad económica. La minería de Bitcoin con equipos ASIC (*Application-Specific Integrated Circuit*) conlleva costos iniciales elevados y gastos operativos continuos, principalmente por consumo eléctrico. Asimismo, un análisis completo debe contemplar la inversión en hardware, la infraestructura eléctrica necesaria, los costos operativos de energía eléctrica consumida tanto por los equipos ASIC como por el sistema de enfriamiento.

A continuación, se presenta el desglose de la inversión inicial y los costos de operación estimados para el uso de un ASIC Bitmain Antminer S19 Pro en El Salvador, con énfasis en el costo de la energía eléctrica bajo el esquema tarifario local.

4.1.1 Costo de inversión inicial

La inversión inicial corresponde principalmente a la adquisición del equipo de minería ASIC. En este caso se emplea un Bitmain Antminer S19 Pro, un dispositivo de alta gama capaz de lograr alrededor de 110 TH/s de potencia de cómputo con un consumo eléctrico aproximado de 3.25 kW (3,250 W). La tabla 4.1 muestra los gastos más importantes para la implementación de las pruebas de un equipo ASIC en El Salvador. Cabe señalar que los costos estimados podrían incrementarse significativamente en un escenario real de implementación, ya que no se ha contemplado el

arrendamiento del espacio físico. En caso de requerirse el alquiler del local, el costo inicial sería considerablemente mayor.

El equipo fue adquirido en condición de segunda mano, razón por la cual fue necesario someterlo a un proceso de reacondicionamiento técnico. Esto implicó limpieza interna y mantenimiento preventivo. Si bien estos costos no se incluyen en la Tabla 4.1, deben considerarse en un proyecto de mayor escala. En cuanto al costo de adquisición del ASIC, el precio estimado de compra, al tratarse de un equipo usado, fue de US$ 500.00, más los costos de manejo, envío e importación aduanera, por un total de US$ 930.00.

Es importante señalar que el costo del regulador de voltaje no fue incluido en la estimación de inversión, dado que este equipo fue facilitado en calidad de préstamo exclusivamente para las pruebas experimentales, por lo que no representó un gasto para el proyecto. No obstante, su costo ha sido incorporado en la Tabla 4.1 a modo de referencia, ya que en proyectos de mayor magnitud debe considerarse como un elemento indispensable de protección frente a variaciones en el suministro eléctrico.

Componente	**Costo estimado (US$)**
Antminer S19 Pro (equipo usado)	$930.00
Regulador de voltaje (ya instalado)	$0.00
Cableado eléctrico	$50.00
Térmico (protección de sobrecarga)	$20.00
Adecuación del espacio	$0.00
Mano de obra e instalación eléctrica	$0.00
Total de inversión	$1,000.00

Tabla 4.1 Costos de inversión inicial para el funcionamiento de un Antminer S19 Pro

Adicional a la compra del equipo, fue necesario adecuar la instalación eléctrica del lugar de operación. El Antminer S19 Pro requiere una alimentación de 220-240 VAC para funcionar de manera segura y estable, debido a su alto consumo de potencia. En entornos residenciales típicos de El Salvador, la tensión eléctrica por fase es 120 V, por lo que se tuvo que implementar una conexión dedicada de 220 VAC para alimentar el ASIC.

Esta condición representa un aspecto crítico a considerar en proyectos de instalación de equipos ASIC en entornos domésticos, ya que, en ausencia de una red de 220 V, sería necesario solicitar a la compañía distribuidora de energía la reconfiguración del servicio eléctrico, lo cual conllevaría costos adicionales por modificación de la acometida. En el presente caso, dicho costo no fue contemplado, ya que el lugar seleccionado ya disponía de dicho nivel de tensión.

4.1.2 Costos operativos eléctricos mensuales

El principal costo operativo es el consumo energético, dado que el Antminer S19 Pro se utiliza para minar Bitcoin mediante el protocolo de consenso *Proof of Work*, que demanda mucha potencia de cómputo para su ejecución. Por lo tanto, la medición del consumo de energía fue fundamental en este estudio y se utilizó el analizador de red Fluke 435 para registrar el funcionamiento real del sistema durante 24 horas de funcionamiento continuo.

Dado que en El Salvador el costo de la electricidad es relativamente alto para usuarios comerciales/residenciales, este rubro influye significativamente en la viabilidad del proyecto. Según el pliego tarifario vigente a la fecha del estudio (enero-abril de 2025), el cual se muestra en la Figura 4.1, el cargo por energía es de 0.192553 $US\$/kWh$ esta tarifa de la distribuidora CAESS no incluye los costos de comercialización ni cargos de distribución ni el IVA. En base a este costo unitario de la energía, se determinó el gasto eléctrico diario y mensual del Antminer, como se detalla a continuación.

SUPERINTENDENCIA GENERAL DE ELECTRICIDAD Y TELECOMUNICACIONES

PLIEGO TARIFARIO

PRECIOS MÁXIMOS PARA EL SUMINISTRO ELÉCTRICO

VIGENTES A PARTIR DEL 15 DE ENERO AL 14 DE ABRIL DE 2025

I. PEQUEÑAS DEMANDAS (0 < kW ≤ 10)

BAJA TENSION

a) Tarifa Residencial para consumos menores de 99 kWh/mes - BT

Bloque 1: Primeros 99 kWh/mes

		CAESS	DEL SUR	CLESA	EEO	DEUSEM	EDESAL	B&D	DEC
Cargo de Comercialización:									
Cargo Fijo	US$/Usuario-mes	0.867998	1.015107	0.786919	0.923566	0.821532	1.566566	0.867936	1.031851
Cargo de Energía:									
Cargo Variable	US$/kWh	0.192553	0.184249	0.193040	0.192012	0.204809	0.171224	0.178283	0.146958
Cargo de Distribución:									
Cargo Variable	US$/kWh	0.032119	0.051952	0.065141	0.069640	0.081671	0.066055	0.040568	0.039656

Figura 4.1 Pliego tarifario del mes de enero a abril de 2025

$$Consumo\ eléctrico\ diario: 81{,}855\ Wh/día$$

$$Consumo\ eléctrico\ mensual: 81{,}855\ Wh/día\ \times 30\ dias = 2{,}455.65\ kWh$$

$$Costo\ diario\ =\ 81.855\ kWh\ /dia\ \times US\$\ 0.192553\ =\ 15.76\ US\$/día$$

$$Costo\ mensual\ = US\$\ 15.76 \times\ 30\ dias =\ \ 472.84\ US\$/mes$$

Como se observa, el costo mensual de electricidad para operar un Antminer S19 Pro en El Salvador es significativo, alcanzando casi los US$ 500. Este valor equivale a un consumo de 2,455.65 kWh al mes. Esta cifra es superior al consumo promedio de electricidad de un hogar en El Salvador, que la mayoría de los casos no superan los 99 kWh al mes, lo que refleja la alta demanda energética de la minería de Bitcoin. Además, esta tarifa es válida para pequeñas demandas, como se muestra en la Tabla 4.1. por lo tanto, con 3 equipos ASIC se debería cambiar a media o alta demanda. Por consiguiente, la rentabilidad del proyecto depende en gran medida del costo de la electricidad, por lo que pequeñas fluctuaciones en las tarifas eléctricas pueden afectar significativamente la rentabilidad.

4.1.3 Costos de mantenimiento

En lo que respecta al mantenimiento del equipo, para este estudio no se han considerado costos iniciales específicos, dado que únicamente se realizó una intervención de mantenimiento preventivo puntual previo a la prueba experimental, la cual no implicó reemplazo de componentes ni acciones correctivas. Sin embargo, en proyectos de mayor escala, con múltiples unidades ASIC operando de forma continua durante periodos prolongados potencialmente varios años, es necesario establecer un plan de mantenimiento programado que contemple tanto acciones preventivas como correctivas.

Las labores típicas de un mantenimiento incluyen la limpieza periódica de ventiladores, disipadores de calor, así como el eventual reemplazo de ventiladores, fuentes de alimentación o módulos de control en caso de fallas. Si bien estos costos de mantenimiento tienden a ser relativamente bajos en comparación con el gasto energético mensual, deben ser considerados en el dimensionamiento económico total de un proyecto industrial, dado que influyen directamente en la eficiencia térmica y eléctrica del equipo, y, por ende, en su productividad y vida útil.

La Tabla 4.2 presenta una estimación comparativa de los costos iniciales para la instalación y puesta en marcha de un equipo ASIC Antminer S19 Pro bajo dos escenarios: el primero, operación en espacio propio sin costos de arrendamiento y el segundo, operación en espacio alquilado considerando un costo estimado de alquiler de US$ 250 mensuales para un local con infraestructura eléctrica básica.

Categoría	Escenario A: Espacio propio (US$)	Escenario B: Espacio alquilado (US$)
Antminer S19 Pro (usado)	930.00	930.00
Regulador de voltaje	150.00	150.00
Cableado eléctrico	50.00	50.00
Protección térmica	20.00	20.00
Adecuación de espacio	0.00	150.00
Mano de obra instalación	0.00	0.00
Alquiler anual	0.00	3,000.00
Total de inversión primer año	**1,150.00**	**4,300.00**

Tabla 4.2 Estimación comparativa de los costos iniciales

En un escenario de ampliación a cinco unidades del Antminer S19 Pro, tanto la inversión inicial como los requerimientos de infraestructura y el consumo energético se incrementan proporcionalmente. La Tabla 4.3 muestra el impacto económico directo bajo dos condiciones: utilizando la tarifa eléctrica residencial vigente (0.192553 US$/kWh) o aplicando una tarifa hipotética de 0.095 US$/kWh.

Cálculo del consumo mensual con las tarifas vigentes:

- Consumo de 1 equipo: 2,455.65 kWh/mes.
- Consumo de 5 equipos: 12,278.25 kWh/mes.

Escenario energético	Consumo mensual (kWh)	Costo mensual (US$)	Costo anual (US$)
Tarifa residencial	12,278.25	2,364.17	28,370.40
Tarifa hipotética	12,278.25	1,166.43	13,997.21

Tabla 4.3 Consumo energético de 5 equipos ASIC

Con la operación de cinco equipos, el consumo energético supera considerablemente el límite de pequeña demanda, lo que requiere migrar a un contrato de media demanda. Este cambio conlleva requisitos técnicos adicionales, como la instalación de acometida trifásica, transformador y protecciones de mayor capacidad, en caso de que el lugar no cuente con la infraestructura eléctrica adecuada.

4.1.4 Factores técnicos que influyen en la durabilidad de un ASIC

La vida útil de un equipo ASIC como el Antminer S19 Pro está determinada por una combinación de factores técnicos y operativos, incluyendo el diseño electrónico, la calidad de los componentes, las condiciones ambientales, el régimen de carga, la estabilidad del suministro eléctrico, las rutinas de mantenimiento y la rapidez de la obsolescencia tecnológica.

Cuando un equipo ASIC se opera bajo condiciones ideales, como una temperatura controlada por debajo de los 25 °C, una humedad relativa entre el 40 % y el 60 %, un suministro eléctrico estable y un mantenimiento preventivo regular, los fabricantes y los usuarios experimentados en foros especializados han reportado que un ASIC de gama alta puede seguir funcionando de manera eficiente durante 3 a 5 años (Konyseva, 2023).

Sin embargo, si el equipo opera en un entorno con temperaturas elevadas, alta presencia de polvo o un suministro eléctrico inestable, su vida útil puede reducirse considerablemente. En tales condiciones, componentes clave como los ventiladores, las tarjetas madre con microprocesadores integrados y las fuentes de alimentación se desgastan más rápidamente, lo que puede acortar la vida del equipo a tan solo 2 o 3 años (Minería, 2023).

Depreciación del equipo ASIC

Para efectos del análisis económico, se considera la depreciación como la pérdida de valor del activo a lo largo del tiempo, debido tanto al desgaste físico como a la obsolescencia. Existen distintos métodos de cálculo, pero el más común en evaluaciones preliminares es el método lineal, que distribuye la pérdida de valor de manera uniforme durante la vida útil estimada.

Caso con el ASIC Antminer S19 Pro:

- Costo de adquisición: US$ 930.00
- Vida útil base considerada: 3 años
- Valor residual al final de los 3 años = US$ 100.00
- Depreciación anual (método lineal): US$ (930 – 100)/3 = US$ 276.67/ año

La depreciación del ASIC tiene un impacto directo en la rentabilidad del proyecto, ya que significa que el valor del equipo disminuye con el tiempo. En el caso del Antminer S19 Pro, esta pérdida es de aproximadamente US$ 276.67 al año, por lo que es importante tenerla en cuenta al calcular los ingresos netos para los próximos tres años. Considerar la depreciación al hacer el análisis financiero ayuda a ajustar las expectativas y a tomar decisiones más informadas sobre cuándo actualizar o reemplazar el equipo.

4.2 Ingresos esperados por minería de Bitcoin

En el contexto de la minería de criptomonedas, los ingresos esperados dependen de una combinación de factores técnicos y económicos, la eficiencia energética, el precio de mercado del Bitcoin, la dificultad de la red y los costos asociados a la operación. Estos ingresos representan el valor bruto generado por la actividad minera antes de descontar los gastos de energía eléctrica y de mantenimiento. Estos cálculos son un elemento clave para evaluar la viabilidad financiera de un proyecto de minería. En esta sección se presenta el análisis de las ganancias o pérdidas reales obtenidas con un equipo ASIC Antminer S19 Pro bajo condiciones controladas en El Salvador,

comparando dichos resultados con estimaciones teóricas y calculadoras de rentabilidad que se encuentran en el Internet.

4.2.1 Ingreso real generado por minería de criptomonedas

En condiciones reales de operación, se hicieron mediciones durante 24 horas utilizando un ASIC Antminer S19 Pro. Se registró un ingreso diario en bitcoin de 0.00006151 BTC como se muestra en la Figura 4.2. Este valor proviene de mediciones directas en *Braiins Pool* durante el período de estudio realizado, en este caso específicamente el 2 de marzo de 2025, el cual representa la recompensa para ese día obtenida con un solo minero Antminer S19 Pro.

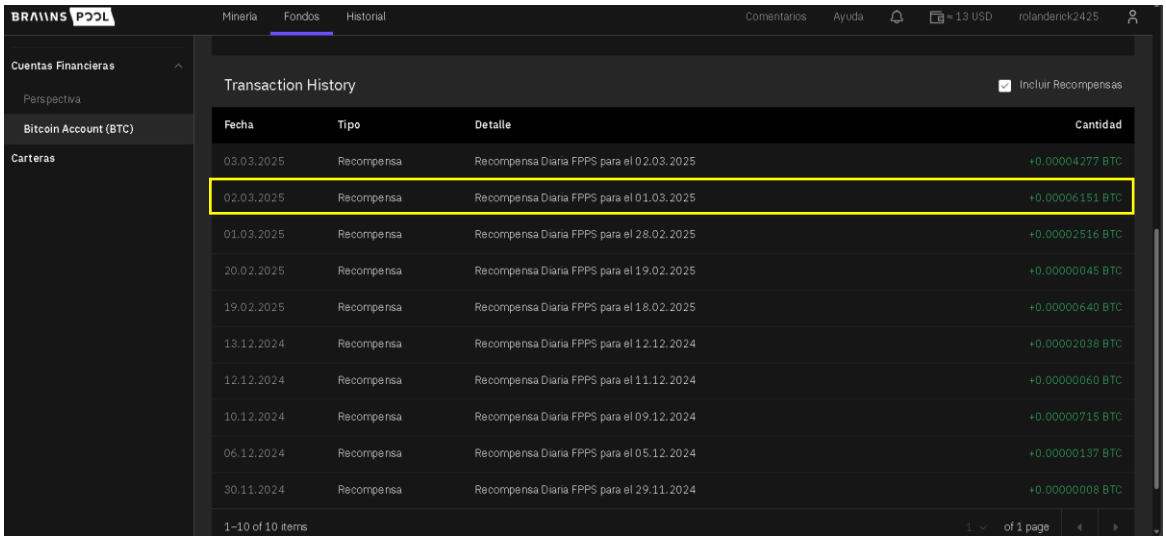


Figura 4.2 Recompensa obtenida del minado de Bitcoin

Convertido a dólares, esto equivale aproximadamente a US$ 5.17 por día, basado en el precio promedio de Bitcoin de US$ 84,000.00 en marzo de 2025 (0.00006151 BTC x 84,000.00 US$/BTC = US$ 5.17). Lo anterior significa que este equipo generaría US$ 155.10 al mes o US$ 1,861.20. Es importante entender que esta ganancia en dólares podría ser menor debido a la volatilidad del precio de Bitcoin, a la creciente dificultad de la red minera y al evento *halving*, que reduce progresivamente las recompensas de los mineros.

Este ingreso real 0.00006151 BTC/día (61.51×10^{-6} BTC /dia) es coherente con el dato esperado para un Antminer S19 Pro. De acuerdo con especificaciones y calculadoras de rentabilidad, este equipo de 110 TH/s, debería minar en el orden de 50×10^{-6} BTC/dia. Por ejemplo, el sitio *ASIC*

MinerValue estima un ingreso de 0.0000525 BTC/día para este ASIC bajo las condiciones actuales de dificultad de la red y recompensas.

En términos monetarios, varios sitios web coinciden en que un Antminer S19 Pro suele generar entre 5 y 7 dólares estadounidenses al día. Por ejemplo, una calculadora de *ASIC MinerValue* reportó unos US$ 5.22 en ingresos diarios. Sin embargo, con una tarifa eléctrica de 0.19 US$/kWh y asumiendo el consumo declarado por el fabricante de 3.25 kW, el costo energético generaría pérdidas, como se ilustra en la Figura 4.3. Los ingresos diarios reales medidos coinciden con los cálculos teóricos y confirman la capacidad productiva de este ASIC (ASICMinerValue, 2025).

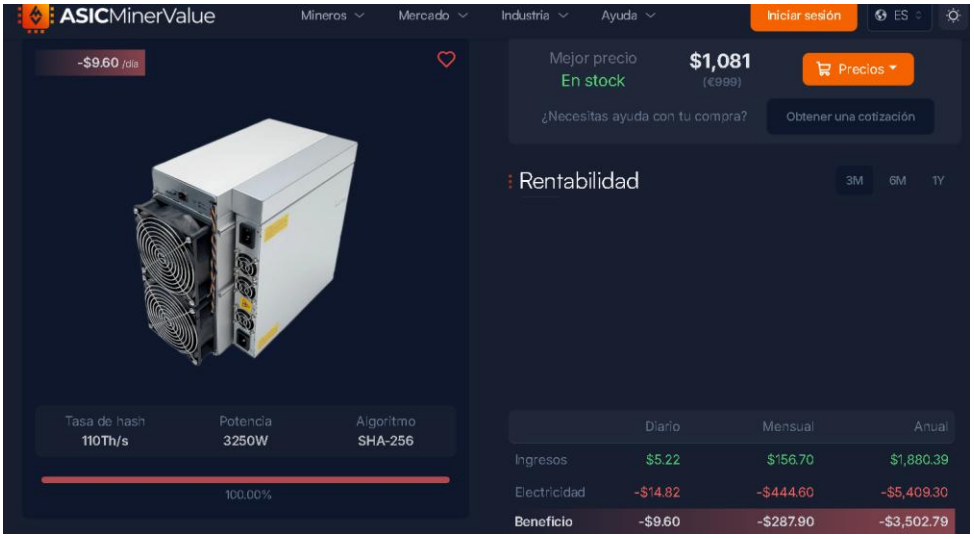


Figura 4.3 Estimación de ganancias con ASIC Antminer S19 Pro

Realizando el mismo ejercicio de este sitio web, pero utilizando los datos obtenidos directamente de las mediciones, se considera la tarifa eléctrica residencial vigente en El Salvador para el primer trimestre de 2025, que es de 0.192553 US$/kWh. Esto da como resultado un costo diario de energía para operar el Antminer S19 Pro de aproximadamente US$ 15.76. Este valor se obtiene multiplicando el consumo eléctrico registrado en un día de operación, que fue de 81,855 Wh. Este cálculo es fundamental para dimensionar correctamente los costos asociados a la operación continua del equipo en condiciones reales.

En resumen, durante el periodo de prueba del Antminer S19 Pro, se obtuvo un ingreso de aproximadamente de US$ 5.17 diarios, basado en el precio del bitcoin en ese momento. Al mismo tiempo, el costo diario de energía eléctrica fue de alrededor de US$ 15.76, lo que refleja una diferencia considerable entre los ingresos y los costos operativos.

Al restar el costo energético diario del ingreso generado, se obtiene una utilidad neta diaria de:

$$\text{Utilidad neta diaria} = \text{US\$ } 5.17 - \text{US\$ } 15.76 = -10.59\ US\$/dia$$

Esto implica una pérdida mensual aproximada de:

$$\text{Pérdida mensual} = -10.59\ \text{US\$/dias} \times 30\ dias = -317.70\ US\$/mes$$

Los datos obtenidos confirman que, bajo el esquema tarifario residencial vigente en El Salvador, el Antminer S19 Pro genera una rentabilidad negativa, incluso con un precio relativamente alto de Bitcoin como el de marzo de 2025. Esta situación se explica por el alto costo energético asociado al algoritmo *Proof of Work*, así como por la baja eficiencia relativa del equipo en comparación con modelos más recientes.

4.2.2 Comparación técnica del Antminer S19 Pro con el Antminer S21 Pro

Dado que, con el precio actual de la electricidad en El Salvador, la utilidad neta del Antminer S19 Pro resulta negativa, es pertinente comparar sus características con las de la nueva generación de mineros ASIC, en particular el modelo Antminer S21 Pro, lanzado por Bitmain en 2024. Esta comparación permite evaluar los avances en eficiencia energética y potencia de cómputo, así como su impacto en la rentabilidad operativa. A continuación, se detallan las especificaciones técnicas más relevantes de ambos equipos.

Parámetro	Antminer S19 Pro	Antminer S21 Pro
Tasa de hash (TH/s)	110 TH/s	234 TH/s
Consumo eléctrico	3,250 W	3,510 W
Consumo diario estimado	81.75 kWh/día	84.24 kWh/día
Eficiencia energética	29.5 J/TH	15.0 J/TH
Precio estimado (marzo 2025)	US$ 930 (usado)	US$ 4,500 (nuevo)

Tabla 4.4 Especificaciones técnicas de dos tipos de ASIC

En base a la Tabla 4.4 se puede realizar el siguiente análisis de cada parámetro a considerar para comprar el ASIC Antminer S21 Pro.

- **Tasa de hash:** El Antminer S21 Pro ofrece una potencia de cómputo de 234 TH/s, lo cual representa un aumento del 112.73 % respecto al Antminer S19 Pro. Esta mejora se traduce directamente en una mayor producción de bitcoin por día.
- **Consumo eléctrico:** Aunque el Antminer S21 Pro presenta un consumo de energía apenas un 7.41 % superior al del S19 Pro (3,510 W frente a 3,250 W), su relación potencia/consumo es significativamente más favorable, lo que optimiza el rendimiento general del equipo.
- **Eficiencia energética:** El Antminer S21 Pro alcanza una eficiencia de 15.0 J/TH, mientras que el Antminer S19 Pro opera a 29.5 J/TH. Esto representa una mejora del 49.1 % en eficiencia, lo que implica un menor consumo energético por hash calculado, reduciendo así el impacto del costo eléctrico sobre la rentabilidad.
- **Costo de adquisición:** Aunque el Antminer S21 Pro tiene un costo de aproximadamente US$ 4,500, su alta tasa de hash permite recuperar con rapidez la inversión, especialmente en proyectos con tarifas eléctricas preferenciales o acceso a energía renovable de bajo costo.

El Antminer S21 Pro representa una mejora significativa en eficiencia y potencia de minado en comparación con modelos anteriores. Aunque su costo inicial es elevado y la electricidad en países como El Salvador es costosa, el rendimiento superior de este equipo podría justificar la inversión. A pesar de requerir un desembolso mayor, su consumo energético por unidad de potencia de cómputo es considerablemente más bajo, lo que lo hace más eficiente y permite una mayor rentabilidad a largo plazo.

Para ilustrar mejor este punto, a continuación, se presentan las utilidades que se obtendrían de ambos ASIC con el precio de Bitcoin promedio de US$ 84,000. Los cálculos se realizaron utilizando los datos del Antminer S19 Pro, mientras que para el Antminer S21 Pro se emplearon las especificaciones del fabricante y una calculadora en línea con un ingreso de 0.00011 BTC. También se utilizaron las tarifas eléctricas de 0.192553 US$/kWh, proporcionadas por la SIGET, y un precio de electricidad hipotético de 0.095 US$/kWh para la comparación.

Equipo	Consumo diario (kWh)	Tarifa eléctrica (US$/kWh)	Ingreso bruto mensual (US$)	Costo eléctrico mensual (US$)	Ganancia neta mensual (US$)
S19 Pro	81.855	0.192553	155.10	472.84	−317.74
S19 Pro	81.855	0.095	155.10	233.29	−78.19
S21 Pro	84.240	0.192553	277.20	486.61	−209.41
S21 Pro	84.240	0.095	277.20	240.08	37.12

Tabla 4.5 Estimación de la rentabilidad mensual de los modelos ASIC

La viabilidad económica de la minería de Bitcoin con equipos ASIC, como el Antminer S19 Pro y el S21 Pro, depende en gran medida de eventos como el *halving* y la dificultad de la red. El *halving*, que ocurre cada cuatro años, reduce a la mitad la recompensa por bloque, afectando directamente los ingresos. En El Salvador, la tarifa eléctrica residencial ronda los 0.20 US$/kWh. Esta disminución en la recompensa hace que la minería solo sea rentable si el precio de Bitcoin sube, la dificultad de la red baja, o si se utilizan equipos más potentes como el Antminer S21 Pro.

4.3 Análisis de rentabilidad

La evaluación económica de un proyecto de minería de criptomonedas no puede limitarse al cálculo de ingresos brutos y costos operativos. Es necesario determinar si la inversión inicial se recuperará en un plazo razonable y si el proyecto generará utilidades sostenibles a lo largo de su vida útil. Para ello, se emplean indicadores financieros como la rentabilidad y el *Retorno sobre la Inversión* (ROI), complementados con métricas como el *Valor Actual Neto* (VAN) y la *Tasa Interna de Retorno* (TIR), abordadas más adelante en este capítulo.

En el contexto de la minería de Bitcoin, donde intervienen variables altamente volátiles como el precio de la criptomoneda y la dificultad de la red para minar, la estimación de la rentabilidad requiere un enfoque dinámico y basado en escenarios. El presente análisis parte de los resultados obtenidos con el Antminer S19 Pro y otros datos vistos en el panel de control de *Braiins Pool* durante marzo de 2025 y se compararon con los datos del fabricante de un equipo más reciente, el Antminer S21 Pro.

4.3.1 Retorno de la Inversión (ROI)

El Retorno de la Inversión (ROI, por sus siglas en inglés *Return on Investment*) es un indicador financiero que expresa, en términos porcentuales, la relación entre el beneficio neto obtenido y el capital invertido. Su finalidad es evaluar la eficiencia y rentabilidad de una inversión para un periodo definido, permitiendo comparar diferentes alternativas bajo un mismo criterio. En el presente estudio, el ROI se calcula para los modelos de equipos ASIC Antminer S19 Pro y Antminer S21 Pro, considerando su precio de adquisición en el mercado y el ingreso neto diario proyectado bajo condiciones ideales de operación continua y estabilidad de la red. El cálculo del ROI se realiza utilizando la siguiente fórmula.

$$ROI = \frac{Ganancia\ neta\ total(US\$)}{Inversion\ inicial(US\$)} \times 100$$

En el ámbito de la minería de criptomonedas, es habitual emplear el concepto de *flujo de caja,* entendido como el registro sistemático de las entradas y salidas de dinero asociadas a un proyecto, empresa o inversión durante un período determinado y bajo condiciones operativas constantes. Este indicador permite evaluar la liquidez generada y la capacidad del proyecto para sostenerse financieramente.

En la minería de Bitcoin, ambas métricas deben evaluarse juntas, ya que un ROI positivo no siempre implica una recuperación rápida de la inversión. Para efectos del análisis de Retorno de Inversión, se consideró un escenario alcista con precio del Bitcoin de US$ 150,000 dado que se espera que alcance este precio para finales del año 2025 y asumiendo que el precio de energía podría obtenerse a 0.095 US$/kWh si se hace un contrato a largo plazo.

- ***Escenario* 1: *Antminer S19 Pro operando un a*ño**

$$Precio\ del\ bitcoin\ US\$\ 150{,}000\ y\ tarifa\ electrica\ de\ 0.095\ US\$\ /kWh$$

$$Ganancia\ de\ la\ mineria\colon 0.00006151\ BTC/dia$$

$$Ingresos\colon 0.00006151 \times 150{,}000 = 9.23\ US\$/dia$$

$$Consumo\ electrico\ medido\colon 81{,}855\ Wh$$

$$Consumo\ electrico\ diario: 81.855\ kWh \times 0.095\ US\$/kWh = 7.77\ US\$/dia$$

$$Ingreso\ neto\ diario:\ 9.23\ US\$/dia - 7.77 US\$/dia = 1.46\ US\$/dia$$

Con el valor del ingreso neto diario ya se puede realizar el cálculo del ROI para un año.

$$Ganancia\ neta\ para\ un\ año = US\$\ (1.46 \times 30 \times 12) - US\$\ 930.00 = -US\$\ 404.4$$

$$ROI = \frac{-US\$\ 404.4}{US\$\ 930.00} \times 100 = -43.48\ \%$$

Este valor de $ROI = -43.48\ \%$ significa que en un año no se recupera la inversión inicial, más bien se tiene una pérdida del 43.48 %.

- ***Escenario 2*: *Antminer S21 Pro operando un año***

$$Precio\ del\ bitcoin\ US\$\ 150{,}000\ y\ tarifa\ electrica\ de\ 0.095\ US\$/kWh$$

$$Ganancia\ de\ la\ mineria: 0.00011\ BTC/dia$$

$$Ingresos: 0.00011 \times 150{,}000 = 16.50\ US\$/dia$$

$$Consumo\ electrico\ medido: 84.24\ kWh$$

$$Consumo\ electrico\ diario: 84.24\ kWh \times 0.095\ US\$/kWh = 8.00\ US\$/dia$$

$$Ingreso\ neto\ diario:\ 16.50\ US\$/dia - 8.00\ US\$/dia = 8.50\ US\$/dia$$

Con el valor del ingreso neto diario ya se puede realizar el cálculo del ROI para un año.

$$Ganancia\ neta\ para\ un\ año = US\$\ (8.50 \times 30 \times 12) - US\$\ 4{,}500.00$$

$$= -US\$\ 1{,}440.00$$

$$ROI = \frac{-US\$\ 1{,}440.00}{US\$\ 4{,}500.00} \times 100 = -32.00\ \%$$

Este valor de $ROI = -32.00\ \%$ significa que en un año no se recupera la inversión inicial, más bien se tiene una pérdida del 32.00 %.

4.3.2 Tiempo de recuperación

Adicionalmente, se utiliza el tiempo de recuperación de la inversión (*payback period*), el cual determina el número de periodos necesarios para que las ganancias acumuladas igualen la inversión inicial. Su cálculo puede expresarse de forma general como:

$$Tiempo\ de\ recuperacion(dias) = \frac{Inversion\ inicial(US\$)}{Ingreso\ neto\ diario(US\$)}$$

En este caso ambos operando deben ser positivos pues es el resultado es un número de días, no es un porcentaje como en el caso de otros indicadores.

Diferencias clave:

- El ROI porcentual mide la relación entre ganancia e inversión en un periodo determinado.
- El tiempo de recuperación indica cuántos días o años se necesitan para recuperar el capital inicial.

$Escenario\ 1$: $Antminer\ S19\ Pro$

$$Tiempo\ de\ recuperacion(dias) = \frac{US\$\ 930.00}{US\$\ 1.46} = 636.98\ dias = 1.77\ años$$

$Escenario\ 2$: $Antminer\ S21\ Pro$

$$Tiempo\ de\ recuperacion(dias) = \frac{US\$\ 4{,}500.00}{US\$\ 8.50} = 529.41\ dias = 1.47\ años$$

Por lo tanto, en estos proyectos es posible recuperar la inversión inicial suponiendo que el bitcoin va a valer US$ 150,00.00 y la energía eléctrica se pudiera contratar a 0.095 US$/kWh, solo bajo estas condiciones es que en ambos escenarios se puede recuperar en 2 años. Sin tomar en cuenta los gastos de operación y para ambos casos esto puede ocurrir en casi dos años.

4.3.3 Cálculo de ROI para diversos escenarios

Siguiendo la misma metodología antes descrita, se han tabulado en una tabla los resultados para múltiples escenarios en donde se muestran dos valores de precio de bitcoin y dos valores de precio de la energía, dando ocho posibilidades. Los resultados se muestran en la Tabla 4.5, donde se observa con claridad cómo el acceso a energía más económica transforma completamente el panorama de recuperación del capital invertido.

Equipo	Precio de Bitcoin (US$)	Tarifa eléctrica (US$/kWh)	Ingreso neto diario (US$)	Tiempo recuperación (años)	ROI anual (%)
S19 Pro	84,000	0.192553	−10.59	No se recupera	Negativo
S19 Pro	84,000	0.095	−2.6	No se recupera	Negativo
S21 Pro	84,000	0.192553	−6.98	No se recupera	Negativo
S21 Pro	84,000	0.095	−1.24	No se recupera	Negativo
S19 Pro	150,000	0.192553	−6.52	No se recupera	Negativo
S19 Pro	150,000	0.095	1.46	1.77	−43.48 %
S21 Pro	150,000	0.192553	0.28	44.64	−97.76 %
S21 Pro	150,000	0.095	8.5	1.47	−32.00 %

Tabla 4.6 Comparación de rentabilidad en distintos escenarios

En los escenarios con un precio de Bitcoin de US$ 84,000 tanto el Antminer S19 Pro como el Antminer S21 Pro presentan pérdidas diarias en cualquier esquema tarifario. Esto lleva a que se tenga un ROI anual negativo y en un tiempo de recuperación indeterminado, lo que hace inviable la operación desde el punto de vista financiero.

Sin embargo, en un contexto altamente alcista, con un precio de bitcoin de US$ 150,000, se observan ingresos positivos en combinación con la tarifa hipotética de 0.095 US$/kWh. En este escenario, el Antminer S19 Pro logra un ROI anual de -43.48 % y un tiempo de recuperación de 1.77 años, mientras que el Antminer S21 Pro, gracias a su mayor eficiencia energética, alcanza un ROI de -32 % y un periodo de recuperación de apenas 1.47 años.

El análisis evidencia que la tarifa eléctrica es el factor más determinante para la viabilidad económica de la minería de criptomonedas en El Salvador. Sin embargo, esta ventaja no es suficiente para compensar un precio bajo de Bitcoin, ya que incluso con acceso a energía más barata, un valor de bitcoin igual o menor a US$ 84,000 mantiene los resultados en zona negativa para ambos modelos.

En este caso, la tabla anterior confirma que para lograr un retorno es imprescindible operar con equipos de alta eficiencia y bajos costos en la energía eléctrica, además de contar con un entorno de mercado favorable en términos de precio de Bitcoin. Sin estas condiciones, la minería resulta financieramente insostenible, independientemente del modelo de ASIC utilizado en este análisis.

4.3.4 Cálculo del VAN y TIR en la rentabilidad de equipos ASIC

La Tasa Interna de Retorno (TIR) y el Valor Actual Neto (VAN) son indicadores financieros esenciales para evaluar la viabilidad y rentabilidad de un proyecto de inversión. Su aplicación se basa en el análisis de los flujos de caja, que son los registros de las entradas y salidas de efectivo generados por el proyecto a lo largo de un periodo determinado. Evaluar estos flujos permite determinar si los ingresos generados serán suficientes para cubrir el capital inicial y los costos operativos. Estos parámetros también facilitan la comparación del desempeño esperado de diferentes opciones de inversión bajo condiciones definidas.

El Valor Actual Neto (VAN) se calcula aplicando una tasa de descuento a los flujos de ingresos y egresos proyectados, con el fin de considerar el costo de oportunidad del capital invertido, así como factores como el rendimiento mínimo esperado, la inflación y el riesgo. La tasa de descuento se determina utilizando criterios financieros establecidos, tales como el rendimiento promedio de inversiones similares, el costo de capital de la empresa o las referencias del mercado.

Una vez descontados los flujos de caja, se resta la inversión inicial. Entonces, un VAN positivo indica que el proyecto generará un excedente económico sobre el capital invertido, lo que señala viabilidad financiera. En cambio, un VAN negativo muestra que los ingresos proyectados no cubrirían el monto invertido, lo que refleja una rentabilidad limitada (Fernando, 2024).

La fórmula estándar para calcular el VAN es:

$$VAN = \sum_{t=1}^{n} \frac{F_t}{(1+r)^t} - I_0$$

Donde:

F_t: Flujo de caja en el periodo

r: Tasa de descuento aplicada

n: Número total de periodos en el análisis

I_o: Inversión inicial

Interpretación del resultado del VAN:

- Si VAN > 0: el proyecto es rentable
- Si VAN = 0: el proyecto ni gana ni pierde valor
- Si VAN < 0: el proyecto no es restable

La Tasa Interna de Retorno (TIR) es otro indicador clave que mide la rentabilidad potencial de un proyecto. Representa la tasa de descuento que hace que el VAN sea igual a cero, lo que significa que el valor presente de los flujos de ingresos proyectados es igual al valor presente de los flujos de egresos, incluyendo la inversión inicial.

Este valor, expresado en porcentaje, indica el rendimiento esperado del capital invertido bajo las condiciones proyectadas. Si la TIR es superior a la tasa de descuento definida, el proyecto sería rentable. En cambio, si la TIR es menor a la tasa de descuento, implicaría que el proyecto no es rentable (Sevilla, 2025).

La fórmula estándar para calcular el TIR es:

$$VAN = \sum_{t=1}^{n} \frac{F_t}{(1+r)^t} - I_0 = 0$$

Donde:

F_t: Flujo de caja en el periodo

r: TIR

n: Número de periodos

I_0: Inversión inicial

Interpretación del resultado del TIR.

- Si TIR > tasa de descuento requerida: el proyecto es viable
- Si TIR < tasa de descuento requerida: el proyecto no es viable

Con base en los parámetros previamente definidos, y utilizando los flujos de caja netos anuales calculados para cada modelo de equipo y tarifa eléctrica, se estimaron los valores de VAN y TIR para un análisis de tres años. Estos cálculos se realizaron bajo el supuesto de que los precios y costos permanecen constantes, con una tasa de descuento anual del 20 %, representativa del costo de oportunidad y riesgo del capital en inversiones tecnológicas en la región. Los resultados obtenidos se presentan en la Tabla 4.7.

Datos para el cálculo

- Escenarios de análisis: 3 años.
- Vida útil estimada: Antminer S19 Pro: 3 años. Antminer S21 Pro: 5 años.
- Tasa de descuento (r): 20 % anual.
- Los precios de la electricidad y de Bitcoin se considerarán constantes durante todo el período de análisis.

Escenario* 1: *Antminer S19 Pro para un periodo* $n = 3$ *años

$$Precio\ del\ bitcoin\ US\$\ 150{,}000\ y\ tarifa\ electrica\ de\ 0.095\ US\$/kWh$$

$$Ingreso\ neto\ anual: 1.46\ US\$/dia\ \times 360\ dia = US\$\ 525.60$$

$$VAN: \sum_{t=1}^{3} \frac{US\$\ 525.60}{(1+0.2)^t} - US\$\ 930.00$$

Equipo	Tarifa eléctrica (US$/kWh)	Ingreso anual (US$)	Periodo (años)	VAN (US$)	TIR (%)
S19 Pro	0.095	525.6	3	117.17	31.87 %
S21 Pro	0.095	3,060.00	3	1,945.83	46.27 %
S19 Pro	0.192553	−2,347.2	3	−5,874.33	No rentable
S21 Pro	0.192553	100.8	3	−4,287.67	−68.34 %

Tabla 4.7 Calculo del VAN y del TIR

La Tabla 4.7 presenta el análisis financiero de los equipos Antminer S19 Pro y Antminer S21 Pro, bajo dos escenarios tarifarios de energía eléctrica: una tarifa baja de 0.095 US$/kWh y una tarifa elevada de 0.192553 US$/kWh. Para cada caso se calcularon los indicadores de VAN y TIR considerando un periodo de evaluación de tres años.

En el primer escenario, correspondiente al Antminer S19 Pro con tarifa de 0.095 US$/kWh, se observa un ingreso anual neto de US$ 525.60, con un VAN positivo de US$ 117.17 y una TIR de 31.17 %. Esto indica que el proyecto es marginalmente rentable, ya que logra superar la tasa de descuento de referencia del 20 %. Sin embargo, el bajo valor VAN muestra que la rentabilidad está sujeta a fluctuaciones en el precio de Bitcoin o cambios en los costos de energía.

En contraste, el Antminer S21 Pro bajo la misma tarifa alcanza un ingreso anual neto de US$ 3,060.00, lo que se traduce en un VAN de US$ 3,445.83 y una TIR de 46.27 %. Este resultado confirma la alta eficiencia de este equipo comparado con el Antminer S19 Pro y la capacidad de recuperar la inversión en un tiempo considerablemente más corto. Bajo estas condiciones, el Antminer S21 Pro representa una opción atractiva para proyectos de minería de criptomonedas.

El escenario cambia de forma drástica en condiciones de tarifa elevada de 0.192553 US$/kWh. En el caso del Antminer S19 Pro, el ingreso anual neto es negativo con un valor de –US$ 2,347.20, generando un VAN de –US$ 5,874.33 y clasificando el proyecto como no rentable, ya que los costos de operación superan con amplitud los ingresos obtenidos. Por su parte, el Antminer S21 Pro con esta tarifa mantiene un ingreso anual positivo pero muy bajo de apenas US$ 100.8, y en cuanto al VAN y la TIR ambos son negativos, el primero es de –US$ 2,787.67 y el segundo es de –63.01 %, indicadores que reflejan que el proyecto no es rentable.

4.3.5 Conclusiones del análisis financiero

El análisis realizado demuestra que la rentabilidad de la minería de criptomonedas en El Salvador depende principalmente del costo de la energía eléctrica y del precio del Bitcoin. Con las tarifas residenciales vigentes, incluso en escenarios de precios altos de la criptomoneda, los indicadores financieros como ROI, VAN y TIR resultan negativos, se confirma que, bajo estas condiciones, el proyecto no recuperaría la inversión ni generaría ingresos.

Sin embargo, con acceso a tarifas eléctricas reducidas y el uso de equipos más eficientes, como el Antminer S21 Pro, la rentabilidad mejora de forma significativa, alcanzando valores positivos en escenarios de mercado favorables. En síntesis, la factibilidad financiera de la minería de Bitcoin solo es posible si convergen simultáneamente tres factores: energía de bajo costo, equipos de última generación y un precio de Bitcoin elevado.

4.4 Sostenibilidad de la minería en El Salvador

Una vez realizado el análisis anterior, queda en evidencia que en El Salvador la demanda eléctrica ya no proviene únicamente de hogares, comercios e industrias, sino que ahora se pretende incorporar a gran escala equipos de alta demanda energética, como los ASIC utilizados en la minería de criptomonedas. Esto plantea un desafío importante, dado que la matriz eléctrica del país no dispone de excedentes suficientes y depende de recursos limitados, lo que dificulta sostener esta actividad sin generar presiones adicionales sobre el sistema de generación nacional.

El estudio con equipos como el Antminer S19 Pro confirma que, bajo las tarifas actuales y la infraestructura existente, la minería de criptomonedas carece de rentabilidad y sostenibilidad. La viabilidad de esta tecnología sería posible únicamente mediante el acceso a energía renovable a bajo costo y un marco regulatorio que promueva el uso responsable de los recursos. El reto consiste en determinar si la minería puede ser una oportunidad de desarrollo económico o, por el contrario, un riesgo para la seguridad energética y la estabilidad de la matriz eléctrica.

4.4.1 Limitaciones de la matriz energética salvadoreña

El principal obstáculo para la sostenibilidad de la minería en El Salvador es la capacidad limitada de la matriz energética nacional. El sistema depende principalmente de recursos hídricos,

geotérmicos y termoeléctricos, pero no cuenta con excedentes suficientes para absorber la demanda masiva que implican los equipos ASIC.

Un solo Antminer S19 Pro consume alrededor de 2,454 kWh al mes, lo que equivale a más de 20 veces el consumo promedio de un hogar salvadoreño. Con decenas o cientos de equipos ASIC operando, la presión sobre las generadoras eléctricas del país sería considerable, pues consumirían energía destinada a sectores prioritarios como el residencial e industrial. Además, el alto costo de la electricidad de 0.192553 US$/kWh, hace que el gasto mensual alcance los US$ 472.84, un valor difícil de compensar frente a la volatilidad del Bitcoin y el aumento de la dificultad de la red.

Al comparar estos resultados con otros países que fomentan la minería de criptomonedas, se evidencia una brecha significativa. Por ejemplo, en Venezuela las tarifas industriales rondan los 0.05 US$/kWh, menos de una cuarta parte del costo local, lo que convierte a esos países en un destino atractivo para plantas de minería (Charani, 2024).

El Dr. Carlos Martínez, catedrático de la Universidad de El Salvador, ha señalado que el país "no tiene energía barata ni clima frío", condiciones esenciales para operaciones rentables y sostenibles en minería de criptomonedas. En caso de que este estudio propusiera el diseño de una planta minera, los factores climáticos, incluyendo los costos de refrigeración, incrementarían aún más los gastos operativos de los mineros locales. Por lo tanto, con los datos obtenidos en este estudio, se coincide con las observaciones hechas por el Dr. Martínez (Rauda, 2022).

La falta de excedentes energéticos y el alto costo de la electricidad hacen que la minería privada sea insostenible a menos que se utilicen exclusivamente fuentes renovables. Según datos oficiales publicados por El Diario de Hoy, durante los primeros días de prueba del proyecto estatal de minería de Bitcoin, se invirtieron alrededor de US$ 4,672.00 en electricidad para extraer tan solo US$ 269.00, según el precio de Bitcoin en ese momento. Esto significa que, por cada dólar gastado en electricidad, se generaron aproximadamente US$ 0.06, lo que demuestra la baja rentabilidad de la operación (Alvarado, 2025).

4.4.2 Proyectos estatales y sostenibilidad condicionada

A pesar de estas limitaciones, el Estado salvadoreño ha implementado modelos de minería sostenibles gracias a un enfoque energético diferenciado. Un ejemplo es la planta geotérmica de

Berlín, que destinó aproximadamente 1.5 MW de su capacidad a la minería de Bitcoin, utilizando energía al costo de generación sin sobrecargos de transmisión y distribución. Entre 2021 y 2024, esta estrategia permitió generar alrededor de 473.5 BTC (Latimedia, 2024).

Además, El Salvador ha apostado por proyectos de mayor escala, como *Volcano Energy*, que combinan inversión privada internacional con participación estatal cercana a US$ 1,000 millones, contemplando la instalación de 241 MW de capacidad renovable a partir de fuentes solar y eólica. Estos modelos permiten sostener la minería de criptomonedas sin afectar la demanda local, siempre y cuando se utilicen recursos energéticos específicamente asignados y con acuerdos regulatorios claros (Volcano Energy, 2023).

Sin embargo, estas iniciativas no son replicables para pequeños operadores privados, ya que requieren gran escala de inversión, acceso directo a energía renovable y condiciones especiales de negociación. Mientras los proyectos estatales pueden operar bajo un esquema planificado, la minería doméstica o a mediana escala sigue siendo insostenible con la infraestructura actual.

4.4.3 Conclusiones acerca de sostenibilidad

El análisis indica que la minería de criptomonedas en El Salvador enfrenta serias limitaciones de sostenibilidad en el ámbito privado. Los altos costos eléctricos y la falta de excedentes de la matriz energética del país hacen que la actividad no sea rentable y poco competitiva frente a países con tarifas más bajas o mayores reservas de fuentes de energía renovable. La operación intensiva de equipos ASIC podría generar una demanda de potencia excesiva, afectando la energía disponible para sectores prioritarios.

En contraste, los proyectos estatales o de gran escala con acceso directo a fuentes renovables dedicadas, como la geotermia o los futuros desarrollos solares y eólicos, han demostrado que la minería de criptomonedas puede sostenerse bajo condiciones específicas. Sin embargo, este modelo no se aplica a pequeños operadores ni a la economía nacional en general.

En síntesis, la sostenibilidad de la minería en El Salvador depende de equilibrar tres factores clave: el acceso a energía renovable de bajo costo, la regulación que garantice un uso responsable de la capacidad instalada y la disposición del Estado para orientar estos proyectos hacia un beneficio

económico colectivo. De no cumplirse estas condiciones, la minería no solo carecería de rentabilidad, sino que también podría comprometer la estabilidad de la matriz energética nacional.

CONCLUSIONES

- El análisis demuestra que la implementación de Antminer S19 Pro no es rentable en El Salvador bajo las tarifas eléctricas residenciales actuales, ya que el costo de producción de Bitcoin supera su valor de mercado, resultando en un ROI negativo, VAN negativo y TIR insuficiente. Esto resalta que la rentabilidad de la minería depende de tarifas eléctricas bajas, preferentemente provenientes de fuentes renovables.
- La rentabilidad futura de la minería en El Salvador está condicionada a la disponibilidad de energía eléctrica a bajo costo. La integración de fuentes de energía renovables, como la solar y geotérmica, en la matriz energética del país podría reducir los costos y hacer la minería más competitiva y sostenible a largo plazo.
- La minería de criptomonedas con equipos como el Antminer S19 Pro y Antminer S21 Pro enfrenta limitaciones técnicas y ambientales que afectan su sostenibilidad a corto y largo plazo. Estas limitaciones requieren condiciones regulatorias y energéticas favorables para asegurar su viabilidad económica.
- Para optimizar la potencia de minado y la eficiencia de los equipos, es crucial contar con un sistema de refrigeración adecuado. En las pruebas, la temperatura interna de los chips del Antminer S19 Pro aumentó considerablemente debido a un espacio poco ventilado y a la alta temperatura ambiente, lo que podría comprometer el rendimiento del equipo.
- El ruido generado por el Antminer S19 Pro puede resultar molesto en áreas cercanas. Las pruebas de funcionamiento continuo solo fueron posibles durante 24 horas, lo que resalta la importancia de ubicar los equipos en espacios aislados o zonas no habitadas para evitar molestias y mejorar el ambiente de operación.
- Se detectaron niveles elevados de Distorsión Total Armónica (THD), lo que podría afectar la estabilidad de los equipos en instalaciones sin filtrado adecuado. Esto impacta negativamente el rendimiento, por lo que es esencial contar con sistemas de corrección. Además, la alta temperatura durante la operación prolongada pone de manifiesto la necesidad de sistemas de refrigeración eficientes para prolongar la vida útil de los equipos.

RECOMENDACIONES

- Se recomienda que cualquier proyecto de minería de criptomonedas en El Salvador con equipos ASIC contemple un estudio previo exhaustivo de factibilidad energética y económica. Este estudio debe incluir no solo el costo de adquisición de los equipos, sino también los costos operativos derivados del consumo eléctrico, los sistemas de enfriamiento y el mantenimiento preventivo, para evaluar la rentabilidad a largo plazo del proyecto.
- Dado que la rentabilidad de la minería de criptomonedas está estrechamente vinculada al costo energético, es fundamental evaluar escenarios de rentabilidad únicamente bajo condiciones de acceso a tarifas preferenciales de energía, preferentemente provenientes de fuentes renovables. Las tarifas energéticas actuales limitan la rentabilidad económica de la minería, lo que hace imprescindible el uso de energías más limpias y a menor costo.
- Es necesario implementar soluciones de filtrado y corrección de calidad de energía para reducir la Distorsión Total Armónica (THD) generada por los equipos ASIC. Estas soluciones deben estar conforme a los estándares eléctricos internacionales, a fin de garantizar una operación segura y estable dentro de la red eléctrica local, evitando posibles sobrecargas o fallos en la infraestructura.
- Se recomienda diseñar e instalar sistemas de ventilación y climatización adecuados que aseguren la disipación térmica eficiente de los equipos de minería. Dado que la temperatura de operación es un factor crítico para prevenir fallas prematuras y prolongar la vida útil de los equipos, se recomiendan sistemas de enfriamiento eficientes, como refrigeración líquida o aire acondicionado de alta capacidad.
- Para reducir la huella ambiental de la minería de criptomonedas, se recomienda fomentar la integración de fuentes de energía renovable, como la solar, eólica y geotérmica, en proyectos mineros. Estas fuentes no solo contribuirán a la sostenibilidad, sino que también permitirán reducir costos energéticos a largo plazo, mejorando la rentabilidad y el impacto ambiental de las operaciones.

REFERENCIAS

Aaron, S. (24 de febrero de 2025). *BitDegree*. Obtenido de BitDegree: https://es.bitdegree.org/crypto/resena-cgminer

Aguilar, R. R. (2019). *ENTENDIENDO EL BLOCKCHAIN.* 27. Obtenido de https://www.secmca.org/wp-content/uploads/2019/12/Blockchain.pdf

Alemán, U. (Martes 22 de Noviembre de 2022). Obtenido de https://diario.elmundo.sv/economia/solo-la-mitad-de-la-poblacion-salvadorena-usa-el-internet

Alvarado, M. (13 de Mayo de 2025). Las mentiras que rodean los proyectos de minería Bitcoin en El Salvador. *El Diario de Hoy*. Obtenido de https://www.elsalvador.com/h-noticias/h-negocios/bitcoin-el-salvador-nayib-bukele-criptomonedas/1218619/2025/#:~:text=%22Esta%20es%20oficialmente%20la%20primera,0.00599179%20bitcoins%2C%20equivalente%20a%20$269.

Antonopulos, A. (2010). *Mastering Bitcoin.* Obtenido de https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf

Asamblea Legislativa, d. E. (2021). Obtenido de https://www.asamblea.gob.sv/node/11282

ASICMinerValue. (15 de Mayo de 2025). *Bitmain Antminer S19 Pro.* Obtenido de ASICMinerValue: https://www.asicminervalue.com/es/miners/bitmain/antminer-s19-pro-110th

Banco Santander, B. (12 de agosto de 2021). *¿Qué son las criptomonedas y cómo funcionan?* Obtenido de Santander.com: https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas

BBC News Mundo. (7 de septiembre de 2021). Obtenido de https://www.bbc.com/mundo/noticias-america-latina-58441561

Binance Academy. (5 de Julio de 2020). *Raiz de merkle*. Obtenido de Binance: https://academy.binance.com/en/articles/merkle-trees-and-merkle-roots-explained

Bitpanda. (s.f.). *La segurida de las criptomonedas*. Recuperado el 25 de Mayo de 2025, de bitpanda: https://www.bitpanda.com/academy/es/lecciones/que-son-las-claves-publicas-las-claves-privadas-y-las-direcciones-de-monedero/

Braiins. (29 de diciembre de 2021). *Braiins Acquired Remaining Stake in Braiins Pool, Slush Focusing on SatoshiLabs.* Obtenido de Braiins: https://braiins.com/blog/braiins-acquires-remaining-stake-in-braiins-pool-slush-focusing-on-satoshilabs

Cade. (11 de septiembre de 2014). *Wired*. Obtenido de Overstok.com: https://www.wired.com/2014/09/overstock-com-becomes-first-major-retailer-accept-bitcoin-worldwide/#:~:text=Overstock,to%20Accept%20Bitcoin%20Worldwide

Cantizzano, I. (12 de Septiembre de 2022). Obtenido de La Prensa Grafica: https://www.laprensagrafica.com/economia/Las-remesas-que-llegan-por-la-Chivo-son-menos-del-2-20220911-0059.html

César Artiga & Meraris López, C. A. (Noviembre de 2021). *BITCOIN ADOPTION.* Obtenido de https://library.fes.de/pdf-files/bueros/fesamcentral/18743.pdf

Charani, M. (27 de Septiembre de 2024). Los 5 lugares más baratos para minar criptomonedas. *CriptoFácil Español*. Obtenido de https://www.criptofacil.com/es/los-5-lugares-mas-baratos-para-minar-criptomonedas/

Christine, K. (14 de septiembre de 2021). *El auge de los ASIC: una historia paso a paso de la minería de Bitcoin*. Obtenido de Coindesk: https://www.coindesk.com/es/tech/2020/04/26/the-rise-of-asics-a-step-by-step-history-of-bitcoin-mining

Cointelegraf, C. (4 de Octubre de 2023). *El Salvador launches first Bitcoin mining pool as Volcano Energy partners with Luxor*. Obtenido de El Salvador launches first Bitcoin mining pool as Volcano Energy partners with Luxor: https://cointelegraph.com/news/el-salvador-first-bitcoin-mining-pool-volcano-energy-luxor

Delton Rhodes, R. (16 de Julio de 2024). *What's a Merkle tree? A simple guide to Merkle trees*. Obtenido de Komodo Academy : https://komodoplatform.com/en/academy/whats-merkle-

tree/#:~:text=Merkle%20Trees%2C%20by%20design%2C%20always,a%20block%20of%20a%20blockchain.

Energy, V. E. (3 de Noviembre de 2023). *Launch of Volcano Energy, a bitcoin mining project in El Salvador with an initial investment of $250 million*. Obtenido de Volcano Energy: https://volcano.energy/en/launch-of-volcano-energy-a-bitcoin-mining-project-in-el-salvador-with-an-initial-investment-of-250-million/

Euny Hong, I. (05 de diciembre de 2024). *Como funciona la mineria de bitcoin*. Obtenido de Investopedia: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

Faster Capital, F. C. (s.f.). *De las CPU a los ASIC la evolucion del hardware de mineria de bitcoin*. Recuperado el 16 de Mayo de 2025, de Faster Capital: https://fastercapital.com/es/contenido/De-las-CPU-a-los-ASIC--la-evolucion-del-hardware-de-mineria-de-bitcoin.html#:~:text=ASIC,de%20la%20miner%C3%ADa%20de%20GPU

Fernando, J. (14 de agosto de 2024). *Net Present Value (NPV): what it means and steps to calculate it*. Obtenido de Investopedia: https://www.investopedia.com/terms/n/npv.asp

Flir Systems. (s.f.). *FLIR i7 infrared camera datasheet. Global Test Supply.* Recuperado el 22 de Mayo de 2025, de Flir i-series: https://www.globaltestsupply.com/pdfs/cache/www.globaltestsupply.com/flir_systems/thermal_imager/i7/datasheet/flir_systems_i7_thermal_imager_datasheet.pdf

Fluke. (s.f.). *Fluke 435*. Recuperado el 2 de Mayo de 2025, de https://www.fluke.com/es-sv/producto/comprobacion-electrica/calidad-electrica/434-435

Fordham, F. (23 de Febrero de 2022). *Follow the Leader? Legal Uncertainties Shape the Risk Perception of El Salvador's Adoption of Bitcoin as Legal Tender — Fordham International Law Journal*. Obtenido de Fordham International Law Journal: https://www.fordhamilj.org/iljonline/follow-the-leader-legal-uncertainties-shape-the-risk-perception-of-el-salvadors-adoption-of-bitcoin-as-legal-tender

Freeman Law, F. L. (11 de Noviembre de 2023). *Double-Spending Problem & Byzantine General's Problem in Relation to Cryptocurrency*. Obtenido de Double-Spending

Problem & Byzantine General's Problem in Relation to Cryptocurrency: https://freemanlaw.com/double-spending-problem-and-byzantine-generals-problem-in-relation-to-cryptocurrency-2/

Frumkin, D. (2022). *Bitcoin Mining Handbook.* Republica Checha: Braiins Insights. Obtenido de https://cdn.prod.website-files.com/5e5fcd39a7ed2643c8f70a6a/63ebadbe407c5bc4621f0d2a_Handbook%20I_web%20verze_3.pdf

García, N. (2023). *Analisis de las principales criptomonedas, pasado presente y futuro.* Valladolid. Obtenido de https://uvadoc.uva.es/bitstream/handle/10324/63446/TFG-J-503.pdf?sequence=1

Han Su. (19 de Febrero de 2025). *¿Qué es un ASIC Miner?* Obtenido de Crypto Miner Bros: https://www.cryptominerbros.com/es/blog/what-is-an-asic-miner/?srsltid=AfmBOoriJPR3BuFt-ypGDzBCPO5pllUNiREzG11s4wsWaMrQljT0QFYH

Hankin, A. (2024 de enero de 2025). *Investopedia*. Obtenido de Dia de la pizza de bitcoin: https://www.investopedia.com/news/bitcoin-pizza-day-celebrating-20-million-pizza-order/

Hashrate Index. (2 de Junio de 2025). *Bitcoin mining pool hashrate distribution*. Obtenido de Hashrate index: https://hashrateindex.com/hashrate/pools

IEEE. (2014). *IEEE 519-2014*. Obtenido de Estandares IEEE: https://standards.ieee.org/ieee/519/3710/

JeFreda R Brown, J. R. (05 de diciembre de 2024). *Investopedia*. Obtenido de Que es bitcoin: https://www.investopedia.com/terms/b/bitcoin-mining.asp

Jiongyu Song, Y. C. (2022). *Cryptocurrencies' Past, Present and Future* . doi:https://doi.org/10.2991/978-94-6463-036-7_208

Kanade, V. (28 de noviembre de 2023). *spiceworks*. Obtenido de spiceworks: https://www.spiceworks.com/tech/tech-general/articles/what-is-bitcoin)

Kenneth Proctor, K. (28 de Enero de 2024). *Decentralization, Immutability, and Integrity: The Role of Blockchain Technology in Enhancing Cybersecurity.* Obtenido de ResearchGate: https://www.researchgate.net/publication/377751048_Decentralization_Immutability_and_Integrity_The_Role_of_Blockchain_Technology_in_Enhancing_Cybersecurity

Konyseva. (18 de Agosto de 2023). *Cual es la vida util esperada de un ASIC.* Obtenido de PC PRAHA: https://pcpraha.cz/es/mining-wiki/jaka-je-predpokladana-zivotnost-asic-mineru/?srsltid=AfmBOoogj5byvNxF6W6w7bUHLBPyxBMCZd3oQR4NUy39FmdfHOmJdB1Q

Latimedia. (17 de mayo de 2024). *El Salvador Minó Casi 474 BTC Usando Energía Geotérmica*. Obtenido de Centroamerica y Caribe: https://www.centroamericaycaribeit.com/20519/el-salvador-mino-casi-474-btc-usando-energia-geotermica/

Legge. (24 de febrero de 2025). Obtenido de koinly: https://koinly.io/blog/best-bitcoin-mining-pools/

Legge1. (3 de junio de 2025). *Best crypto mining software in 2025*. Obtenido de https://koinly.io/blog/best-crypto-mining-software

Mining Bitcoin. (s.f.). *Bitcoin deloper, S.F*. Recuperado el 15 de Mayo de 2025, de Mining: https://developer.bitcoin.org/devguide/mining.html

NEC. (2008). *National Electrical Code (2008 ed.).* Quincy, MA: National Fire Protection Association.

Nelson Renteria, N. (14 de Mayo de 2024). *El Salvador mined nearly 474 bitcoins, adding to state crypto holding, in last three years*. Obtenido de Reuters: https://www.reuters.com/world/americas/el-salvador-mined-nearly-474-bitcoins-adding-state-crypto-holding-last-three-2024-05-14/

Ortiz, R. (24 de abril de 2023). *bitwage.com*. Obtenido de Transformacion de Ethereum un nuevo horizonte para la inversion: https://bitwage.com/es-ar/blog/la-transformacion-de-ethereum-un-nuevo-horizonte-para-la-inversion

Prensa grafica, P. (2021). FMI_PREOCUPACION. *La prensa grafica*. Obtenido de https://www.laprensagrafica.com/economia/El-FMI-advierte-a-El-Salvador-de-riesgos-al-adoptar-Bitcoin-20210611-0012.html

R. Brown, J. (16 de mayo de 2024). *Investopedia*. Obtenido de Que es un altcoin: https://www.investopedia.com/terms/a/altcoin.asp#:~:text=Altcoins%20attempt%20to%20improve%20upon,256%20PoW%20consensus%20mechanism

Rasuse, E. (26 de julio de 2024). *Investopedia*. Obtenido de Arbol de Merkle en blockchain: https://www.investopedia.com/terms/m/merkle-tree.asp#:~:text=A%20Merkle%20tree%20is%20a%20data%20encryption%20structure%20used%20in,the%20data%20in%20a%20file.

Rauda. (08 de febrero de 2022). Obtenido de El Faro: https://elfaro.net/es/202202/el_salvador/25983/Primer-minero-salvadore%C3%B1o-de-bitcoin-%E2%80%9Cbuscamos-electricidad-m%C3%A1s-barata%E2%80%9D.htm

Rivas. (2024). *EVALUACIÓN TÉCNICA Y ECONÓMICA PARA EL MONTAJE DE UNA PLANTA DE MINERIA DE BITCOIN EN EL SALVADOR.* Ciudad Universitaria. Obtenido de https://repositorio.ues.edu.sv/items/54233517-4f32-4897-ad83-70cc3b59ec51/full

Schneider Electric. (2017). *Breaker terminal temperature limits per UL 489.* Obtenido de https://www.se.com/ca/en/faqs/FA173839/

Seth, S. (31 de Octubre de 2024). *GPU Usage in Cryptocurrency Mining*. Obtenido de Investopedia: https://www.investopedia.com/tech/gpu-cryptocurrency-mining/

Sevilla, A. (21 de mayo de 2025). *Tasa Interna de Retorno (TIR)*. Obtenido de Economipedia: https://economipedia.com/definiciones/tasa-interna-de-retorno-tir.html

Tapscott, D. (2016). *Blockchain revolution.* Retrieved from https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf?

Vermaak, W. (2022). *Que es la mineria asic*. Obtenido de https://coinmarketcap.com/academy/article/what-is-asic-mining

Volcano Energy. (5 de Junio de 2023). *Lanzan Volcano Energy, un proyecto de minería bitcóin en El Salvador con una inversión inicial de $250 millones*. Obtenido de Volcano Energy: https://volcano.energy/lanzan-volcano-energy-un-proyecto-de-mineria-bitcoin-en-el-salvador-con-una-inversion-inicial-de-250-millones/

Zurdo, R. P. (12 de Junio de 2018). *Blockchain la descentralizacion del poder.* Obtenido de https://infolibros.org/pdfview/10983-blockchain-la-descentralizacion-del-poder-y-su-aplicacion-en-la-defensa-ricardo-palomo-zurdo/