Cryptocurrency mining feasibility using low-cost hardware

Factibilidad de minería de criptomonedas mediante el uso hardware de bajo costo

William R. Navas, Mg.[1], Víctor H. Garofalo, Mg.[1], Roger D. Campoverde, Mg.[1], Dennis H. Zambrano, Mg, Freddy S. Pincay, Msc.[1], Raquel N. Vera[1], Angel M. Plaza, Msc.[1]

[1]Universidad de Guayaquil, Ecuador, william.navase@ug.edu.ec, victor.garofalol@ug.edu.ec, *roger.campoverdeb@ug.edu.ec*, dennis.zambranos@ug.edu.ec, freddy.pincayb@ug.edu.ec, *raquel.verao@ug.edu.ec*, angel.plazav@ug.edu.ec

***Abstract*– The development of prototypes with low-cost and environmentally friendly components are an important part of the characteristics of project proposals within the academic and technological area in the Faculty of Industrial Engineering of the University of Guayaquil, the present work carries out a feasibility evaluation of mining of cryptocurrency using the Raspberry Pi hardware, documenting the process and evaluating each of the parties involved, in search of a viable option that allows mining a cryptocurrency, taking into account the security of the network through the mining process, it is intended find an energetically sustainable without giving up the fundamental principles of cryptocurrencies**

***Keywords*-- Cryptocurrencies, Cryptography, Raspberry Pi, Mining, Hashrate, wallet.**

***Resumen*– El desarrollo de prototipos con componentes de bajo costo y amigables al medioambiente son parte importante de las característica de propuestas de proyectos dentro del área académica y tecnológica en la Facultad de Ingeniería Industrial de la Universidad de Guayaquil, el presente trabajo realiza una evaluación de factibilidad de la minería de criptodivisas mediante el hardware Raspberry Pi, documentando el proceso y evaluando cada uno de las partes implicadas, en busca de una opción viable que permita minar una criptodivisa, teniendo consideraciones a la seguridad de la red mediante el proceso de minería, se pretende encontrar una opción energéticamente sostenible de la misma sin renunciar a los principios fundamentales de las criptodivisas.**

***Keywords*-- Criptodivisas, Criptografía, Raspberry Pi, Minería, Hashrate, Monedero.**

I. Introducción

Dentro del crecimiento tecnológico mundial y los procesos de globalización, es imprescindible un sistema financiero en el cual las transacciones se realicen de forma inmediata, sin las intervención de terceros, apegada a los principios monetarios fundamentales de descentralización y eficiencia, para otorgar a los usuarios completo control sobre los activos, porque si bien el sistema financiero actual ha mejorado mucho desde sus inicios, sigue girando en torno a la confianza de los usuarios, sociedades y estados en una institución en específico que guarda los activos del usuario, es decir, las pruebas tangibles de que la institución guarda esos activos solo las tienen las dos partes creando dependencia en las instituciones.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2022.1.1.637
ISBN: 978-628-95207-0-5 **ISSN:** 2414-6390

La creación de las criptomonedas se planteó como una solución a los inconvenientes del sistema financiero tradicional, fundamentado en la primera criptomoneda bitcoin [1] la cual se presentó como una alternativa de intercambio mediante un sistema en el cual los usuarios son los encargados de verificar, validar y procesar las transacciones de los miembros de la red de intercambio, y la forma en la cual generar confianza seria mediante una cadena de bloques en la que cada transacción de la red se guardara y todos los demás usuarios tendrían esta cadena la cual se verificaría constantemente antes de agregar una nueva transacción, lo cual provocaría que los usuarios que modifiquen o borren alguna transacción tengan inconsistencias en la cadena de bloques y por ende recibirían un aviso y posterior expulsión de la red, esto dio lugar al primer sistema de criptomonedas conocido y hoy en día el más famoso. Además, el autor de bitcoin sin mencionarlo de forma directa cumplió con lo necesario para que algo sea considerado un activo o moneda y es que debe tener la capacidad de almacenar valor, debe además poder ser fácilmente intercambiado en transacciones entre partes y además ser una referencia de valor es decir dar un valor especifico a las cosas.[2]

Si bien el sistema cumple con los principios a lo largo del tiempo, y con el interés de cada vez más personas por las criptomonedas estos se han ido corrompiendo en ciertas partes, el proceso anterior que se menciono es la minería de criptodivisas, la cual hoy en día consume cantidades enormes de energía que ponen en peligro el futuro del sistema, debido a los centros de minería masivos, que además es contraria al concepto de descentralización del sistema. Debido a estos factores es que mediante este trabajo se plantea un análisis de una alternativa de minería que siga aportando a la seguridad

de la red, pero que sea energéticamente sostenible, así como cuál del amplio ámbito de criptomonedas que existen hoy en día es la más adecuada para este proyecto. [3]

II. ANTECEDENTES

Alrededor de las criptodivisas y la red blockchain, existe un sistema que permite mantener en principios la red y garantizar la seguridad de las transacciones, esta es la minería de criptodivisas, la cual a simples rasgos es la recompensa que entrega la red por la creación y validación de nuevos bloques en los cuales se encuentran las nuevas transacciones y aporta con la integridad de la red.

Muchas de las formas de validación requieren potencia computacional alta, ya que se ejecutan mediante la llamada proof-of-work o prueba de trabajo la cual es a breves rasgos resolver ciertos algoritmos matemáticos complejos para lograr la validación de transacciones, sin embargo existen un sinnúmero de criptomonedas basadas en este principio y nuevas formas de validación, lo cual deja la puerta para que la minería se ejecute en infinidad de equipos con todo tipo de prestaciones y características, por ende, al no conseguir cantidades significativas del activo presentan un importante punto de análisis a futuro, ya que en los últimos años el valor puede crecer de forma impredecible.

Según Perlman [4], Miembro del Consejo de Forbes revista especializada en el mundo de los negocios y las finanzas menciona "La pandemia catapultó aún más los pagos digitales y la tecnología blockchain al centro de atención y demostró los beneficios de resiliencia de la infraestructura digital. Con empresas como Square, Tesla y MicroStrategy invirtiendo en Bitcoin como parte de la estrategia de gestión del tesoro" lo cual muestra el alcance que tiene hoy en día en el mundo este sistema que permite intercambios entre personas de todas partes del planeta sin las complicaciones actuales y altos estándares de seguridad, además cabe mencionar que cada vez más empresas tecnológicas ya las aceptan como método de pago e incluso tienen una criptodivisa propia.

Según Alikkal, C.G, Gopakumar, & K [3], el incremento exponencial de los mineros de criptomonedas conduce al establecimiento de una nueva forma de abordar económicamente el proceso de minería actual, dentro de estas alternativas la introducción de Raspberry pi puede ser una solución viable para disminuir los costos de los actuales sistemas, además proporcionar rentabilidad y ser energéticamente eficiente.

De esta forma se mostrará que se puede minar este tipo de activos mediante equipos de precio accesible, en el cual se opta por la Raspberry Pi, se realizará el proceso de instalación y las diferentes técnicas, programas y métodos para lograr que este dispositivo logre aportar a la seguridad de la red mediante la creación y validación de nuevos bloques, donde se escriben las nuevas transacciones, y de esta forma recibir una recompensa en forma del activo que se está validando.

A. Criptodivisas

Una criptodivisa o criptomoneda es un activo digital o virtual que utiliza criptografía como método de seguridad para realizar transacciones, esta característica presenta una fuerte dificultad de falsificación. Uno de los puntos que hacen más atractivos este tipo de activos es la naturaleza orgánica, lo cual, no es emitido por ningún organismo o autoridad central, esto en teoría lo hace inmune a la intervención o manipulación del gobierno o entidades de este tipo. Se manejan mediante información pública y claves privadas, y con tarifas de procesamiento mínimas. [5]

Desde el punto de vista de Lansky [6], establece que las criptodivisas cumplen con 6 condiciones:

- Las criptodivisas no necesitan de una jerarquía centralizada, debe lograr un consenso sobre sí misma.
- Existe un detalle universal sobre el número de criptodivisas en la red, y a quien pertenecen.
- El sistema determina la posibilidad de la creación de nuevas criptodivisas, además define la forma de la creación y como se otorga la propiedad.
- La pertenencia de las cantidades de criptodivisas de un usuario se verifica únicamente mediante sistemas criptográficos.
- Existe la posibilidad de que la propiedad de las criptodivisas se intercambie entre usuarios mediante un consenso de ambas partes, el registro de estas transacciones se guarda en la cadena de bloques.
- En caso de existir dos peticiones de intercambio de propiedad al mismo tiempo de una misma unidad de criptodivisa, solo podrá procesarse uno de ellos.

B. Minería de Criptodivisas

"Minar criptomonedas o Minería, se define como el proceso de realización de cálculos matemáticos para confirmar transacciones en la red, elevar la seguridad, y de ser posible, crear nuevas criptomonedas. El objetivo de los "mineros" es recopilar las últimas transacciones en bloques (es decir, conjuntos de transacciones verificadas) y encontrar una solución a un complejo algoritmo. Haciendo esto se obtiene una recompensa: una cantidad fija de criptomoneda. Esta cantidad varía según la criptomoneda en la que se trabaje. La solución a este algoritmo supone un proceso continuo y depende de los resultados de algoritmos anteriores para poder realizar el siguiente cálculo. Del mismo modo, la dificultad del algoritmo puede ser (y es) ajustada frecuentemente, con el fin de hacer que el trabajo de los mineros sea constante. El minero agrupa transacciones de criptomoneda nuevas en un "bloque". El bloque se codifica y se vincula a la cadena de bloques o blockchain existente. El minero obtiene su recompensa, que puede inyectar directamente de nuevo en el mercado." [7]

La minería se basa en un principio de intercambio, los mineros prestan el poder de cómputo para validar las transacciones, con el fin de obtener una recompensa económica en forma de la criptomoneda, de esta forma ambas partes reciben una recompensa la comunidad al mantener segura la red con la validación de transacciones, la creación de nuevos bloques en la blockchain y los mineros con el activo.

Los mineros son miembros críticos de la comunidad bitcoin que tienen un lugar indispensable en el proceso de verificación, los definen como individuos con un poder computacional limitado, y dentro del conjunto se incluye a las grandes empresas con un poder de cómputo en escalas mayores a los mineros individuales. Esencialmente es un esfuerzo competitivo y arriesgado, ya que los mineros tienen la labor de esperar por extensos periodos para confirmar un bloque, por ende, resulta en la recompensa esperada por verificar ese bloque. Cabe recalcar que los procesos que se realizan para la minería no solamente involucran el poder computacional, que implica el consumo de energía si no que muchas veces adicionalmente usan sistemas de refrigeración y otros servicios web para monitorización. [1]

C. Minería de Criptodivisas

"La Cadena de Bloques o Blockchain es un registro permanente, inmutable y público en el que se recogen todas y cada una de las transacciones que se han realizado con la moneda Bitcoin desde su creación, mediante bloques encadenados entre sí. Con esto se pretende poder verificar que el flujo de bitcoins ha sido correcto y no se ha quebrantado ese encadenamiento, desde el bloque génesis (el primer bloque) hasta el último generado. Con la Blockchain se supera el problema del doble gasto o "double spending". Será muy difícil utilizar un mismo bitcoin para más de una transacción ya que los bloques están perfectamente conectados y la más mínima separación a esa cadena produciría la no confirmación por parte de los participantes en la red, no llevándose a cabo nunca." [8]

El modelo de la cadena de bloques de bitcoin se usa en la mayoría de las criptomonedas con un nivel de seguridad elevado, porque la más mínima incongruencia en un bloque con los demás usuarios produce que se excluya de los demás bloques validos que se confirmaron entre los miles de usuarios que ejecutan esta labor.

D. Prueba de participación

La prueba de participación nació como respuesta a los inconvenientes presentados por la prueba de trabajo, debido a que presenta claras soluciones a desventajas en el ámbito de gasto energético elevado y la escalabilidad de las redes que lo utilicen, pero a la vez plantea nuevos desafíos desde la forma de funcionamiento.

"La base de funcionamiento del algoritmo PoS es que cada nodo se gana el derecho de crear un nuevo bloque, y por tanto a la toma de decisión, de acuerdo con el compromiso que haya demostrado tener con la red por el número de participaciones y el tiempo de permanencia en la misma. Además de esto, existe un factor aleatorio para que todos los compromisarios tengan la posibilidad de crear un bloque" [9]. Esta definición implica que los usuarios o nodos que realizan la prueba de participación validan un bloque que se les ha otorgado, pero este no se ha entregado en forma proporcional al poder computacional si no de forma aleatoria, pero entregando mayor posibilidad a aquellos que cumplan con ciertos requisitos dentro de la misma red que pueden variar dependiendo de la forma en que esta se concibió.

E. Raspberry Pi

Raspberry Pi es una serie de equipos de cómputo de bajo costo, al ser placa única cuenta con todos los componentes necesarios para el funcionamiento, fue creada por la Raspberry Pi Foundation, en el año 2009 lanzaron la primera versión, con la finalidad de incentivar y apoyar el uso de la informática y la programación para personas con recursos limitados. Raspberry Pi incluye en todas las versiones una CPU, memoria RAM, entrada y salida de audio y video, tarjetas de red (wifi y ethernet en últimos modelos), ranura microSD para almacenamiento, Puertos USB, Pines GPIO, Conexión para cámara. El procesador del equipo es de arquitectura ARM y de software libre es decir cualquier sistema que sea adaptable a esta arquitectura, además, cuenta con sistema operativo proprio llamado Raspberry Pi OS basado en Debian. En la Tabla 1 se presenta un resumen de los diferentes modelos con sus características principales. [10] [11]

Tabla 1 - Tipos de Raspberry Pi

Modelo	Características
Modelo A+	CPU BCM2835 700Mhz, RAM 512 MB, Puertos USB 1
Modelo B+	CPU BCM2835 700Mhz, RAM 512 MB, Puertos USB 4, Puerto Ethernet
2 Modelo B	CPU BCM2836 900Mhz, RAM 1 GB, Puertos USB 4, Puerto Ethernet
3 Modelo B	CPU BCM2837 1200Mhz, RAM 1 GB, Puertos USB 4, Puerto Ethernet, Bluetooth
3 Modelo B+	CPU BCM2837 1200Mhz, RAM 1 GB, Puertos USB 4, Puerto Ethernet, Bluetooth
Zero	CPU BCM2835 1000Mhz, RAM 512 MB, Puertos USB 1
4 Modelo B	CPU BCM2711 1500Mhz 64 bits, RAM 2,4,8 GB, Puertos USB 4, Puerto Ethernet Gygabit, Wifi, Bluetooth, Salida mini-hdmi 2

F. Crypto Wallet o Monedero de criptomonedas

Un monedero de criptomonedas es un software o hardware que permite gestionar los activos digitales, es decir guardar las claves públicas y privadas de diferentes criptomonedas con el fin de mantenerlas protegidas, pero también permite realizar intercambios, compras o ventas de

forma fluida de criptomonedas. Lo que se guarda en el monedero es la transacción y los diferentes cambios en ellas, estos presentan elevados estándares de seguridad para los usuarios, existen propios de cada criptomoneda e independientes con opciones de guardar multitud de criptomonedas a la vez. [12]

III. METODOLOGÍA

Dentro del presente trabajo de investigación donde se evaluará la factibilidad de la minería de criptodivisas mediante el hardware Raspberry Pi, existen varios factores claves que determinaran un mejor o peor rendimiento del hardware, por lo cual se analizara cada una de ellas antes de elegir la criptomoneda que se minara en el hardware.

A. Algoritmos de consenso

Es de enorme importancia la elección de una criptomoneda que use un algoritmo o método de consenso que permita obtener el máximo rendimiento del hardware en cuestión, por eso se planteó una cantidad considerable de ellos para elegir el idóneo para el proyecto. El algoritmo de consenso adecuado permitirá que los nodos o usuarios de la red puedan elegir sobre lo principios fundamentales de la misma, entre estas la cadena de bloques, transacciones, validación y la característica de interés del estudio minería de criptodivisas, por lo cual evaluaremos las diferentes opciones. En la tabla 2 se muestra una comparativa sobre algunas características importantes de los algoritmos de consenso.[13] [14] [15]

Tabla 2 - Comparativa de algoritmos de consenso y características [11]

Algoritmo	Seguridad	Implementación	Compatibilidad
Prueba de trabajo	Elevado nivel de seguridad, en especial en redes grandes	Fácil, variedad de software para minería	Alta, adaptable a todo tipo de hardware
Prueba de participación	Alta en la red, menor en los usuarios por requisito de conexión	Regular, poco software	Regular, hardware comercial
Prueba de participación delegada	Alta en la red, menor en los usuarios por requisito de conexión	Regular, poco software	Regular, hardware comercial
Prueba de actividad	Elevado, sobre todo a ataques (DoS)	Regular, poco software	Regular, hardware comercial
Prueba de quemado	Elevado nivel de seguridad, redes comprometidas	Regular, software propio de la blockchain	Regular, hardware comercial
Prueba de capacidad	Regular, algoritmo sin mucha difusión	Regular, poco software	Alta, cualquier hardware con unidad de almacenamiento
Prueba de tiempo transcurrido	Regular, peligro de ataques a procesadores Intel	Regular, software propio de la blockchain	Regular, hardware Intel
Prueba de asignación	Regular, algoritmo sin mucha difusión	Regular, software propio de la blockchain	Alta, se usa equipos IoT para minar de forma pasiva
Protocolo Ripple	Alta, usuarios deben verificar para ingresar a red	Regular, software propio de la blockchain	Regular, servidores propios de empresas
Prueba de autoridad	Alta, usuarios deben verificar para ingresar a red	Regular, software propio de la blockchain	Regular, hardware comercial

Debido a que el equipo minador ejecutara la minería desde cero se deben descartar los algoritmos que tengan como requisito una cantidad de activo para ser elegido para el proceso, estos algoritmos podrían considerarse a futuro una vez que se cuente con alguna criptomoneda, estos son:

- Prueba de participación, Prueba de participación delegada, Prueba de actividad, Prueba de quemado.
- De la misma forma, se descarta el algoritmo de Prueba de tiempo transcurrido debido a que es usable únicamente en procesadores de la marca Intel por ende de arquitectura x86, debido a que el prototipo del hardware minador está basado en la arquitectura ARM y es de la marca Broadcom.
- El protocolo Ripple queda descartado debido a que el uso del algoritmo está condicionado a autorización de privados en mayoría bancos.
- Otro de los algoritmos que a pesar de ser muy interesante se debe descartar es la Prueba de asignación, la cual utiliza pequeños dispositivos como cámaras, parlantes para minar de forma pasiva, y no entra en los lineamientos del proyecto debido a que se pretende evaluar el rendimiento independiente del hardware elegido.
- El algoritmo de Prueba de Capacidad necesita una unidad de almacenamiento masivo lo cual no entra en los lineamientos del proyecto, Raspberry usa una Micro-SD para albergar el sistema operativo y archivos, pero para este algoritmo se necesita un disco duro o SSD de gran almacenamiento.

Luego de estas consideraciones los algoritmos que presentan las condiciones para aprovechar de forma ideal el hardware seria: Prueba de trabajo y Prueba de autoridad, de los cuales Prueba de trabajo fue el elegido debido a la amplia adaptabilidad a diferentes sistemas operativos, hardware, en lo cual Prueba de autoridad está limitado y además la posibilidad de minar depende no del hardware si no de la capacidad del usuario de aportar a la red con proyectos e ideas, además

Prueba de trabajo ofrece altos niveles de seguridad en las cadenas de bloques.

B. Algoritmos criptográficos hash

La elección de un algoritmo criptográfico que se adapte de forma óptima al proyecto es indispensable, debido a que este proporcionara la dificultad con la que se encontrara el hardware a la hora de minar las criptomonedas y dependiendo de cuan rentable sea de minarlo mediante sistemas ASIC más complicado será para el hardware que usa CPU para minar Además, el algoritmo presentara el estándar de seguridad para poder enfrentar posibles ataques y proporciona confianza a los usuarios de la cadena de bloques, a continuación, en la tabla 3 se muestra una comparativa con las opciones más representativas en la actualidad. [16]

Tabla 3 - Comparativa de algoritmos criptográficos y características

Algoritmo	Hardware de uso	Seguridad	Principales Criptodivisas
SHA-256	ASIC, CPU, GPU	Alta, codificación 32 bytes, desarrollado NSA	Bitcoin (BTC), Bitcoin Cash (BCH)
Ethash	ASIC, CPU, GPU	Alta, basado en SHA-3, varios algoritmos a la vez	Ethereum (ETH), Ethereum Clasic(ETC)
Scrypt	ASIC, CPU, GPU	Alta, requiere mucha memoria, resistente ataques fuerza bruta	Dogecoin (DOGE), Litecoin (LTC)
X11	ASIC no eficiente, CPU, GPU	Alta, 11 algoritmos hash a la vez	Dash (DASH), EUNO (EUNO)
CryptoNight	ASIC no eficiente, CPU, GPU	Alta, codificación de 256 bits, encriptación AES	Monero Classic (XMC), Dero (DERO)
RandomX	ASIC no disponible, CPU, GPU no eficiente	Alta, aleatoriedad impredecible, encriptación AES	Monero (XMR)

Tomando solo en consideración las características que interesan de acuerdo con el análisis previo, los algoritmos más idóneos serian X11, Cryptonight y RandomX de los cuales los dos primeros tienen límites en la minería ASIC provocando que no sea rentable alejando a este tipo de mineros, y RandomX que en cambio no permite de forma estricta la minería ASIC debido a mantiene características que solo se consiguen mediante CPU. Además este algoritmo actualmente solo es utilizado por una criptodivisa llamada Monero (XMR) y su comunidad fue la desarrolladora del mismo buscando elevar su seguridad y mantener un minería sostenible solo ejecutable en CPU, otro punto importante es que Monero (XMR) frente a la principal criptomoneda de los otros algoritmos Dash (DASH) y Monero Classic (XMC) según [17] tiene una capitalización de mercado mucho mayor es decir el valor de su moneda por el número de criptodivisas en circulación, ubicándose respectivamente Monero (XMR) en el puesto número 28, Dash (DASH) en el puesto 51 y Monero Classic (XMC) que se encuentra fuera de las 100 principales criptodivisas. Aportándonos considerablemente más valor la cantidad de activo que logremos minar con Monero (XMR) que con las otras opciones. Debido a lo anteriormente expuesto este trabajo utilizara el algoritmo criptográfico RandomX y por ende la única criptomoneda a la fecha Monero (XMR) dentro de su portafolio.

C. Criptodivisa o Criptomoneda

La criptodivisa elegida para ejecutar la minería es Monero el cual es un proyecto de código abierto que fue creado en 2014, con un enfoque en la descentralización, privacidad y el anonimato. Monero a lo largo de su desarrollo se ha mantenido en constante mejora, incluyendo diferentes algoritmos o procesos en su sistema para mejorar su eficiencia. [19]

Su enfoque en el anonimato le ha permitido posicionarse como una de las opciones predominantes de los miles que existen, ubicándose en el puesto número 28 del mundo, con un valor por unidad de $305.54, existen un total de 17,978,392.96 XMR unidades del activo dando como resultado una capitalización de mercado de $5,509,855,887. Actualmente el redito económico por minar Monero es de 3 XMR por cada bloque minado. [18]

Monero utiliza el método de consenso Prueba de trabajo dentro de su cadena de bloques, y su algoritmo criptográfico es RandomX por lo cual es minable únicamente mediante CPU, su adaptabilidad en cuanto a sistemas operativos es elevado pudiendo ejecutarse en sistemas Windows, macOS, Linux o Android.

D. Pool de minería

Un pool de minería permite que un grupo de mineros ejecuten la minería de forma simultánea, entregando la recompensa sobre la base del poder de cómputo de cada una de las partes, esto permite que equipos con potencia baja puedan recibir recompensas, que de forma independiente podrían obtener solo luego de tiempos prolongados o en ciertos casos nunca, a continuación en la tabla 4 se detallan algunos de los pool más difundidos de la criptomoneda elegida y sus características para elegir la opción idónea.[20]

Tabla 4 - Comparativa pools de minería y características

Pool	Comisión	Pago mínimo	Servidores
xmrpool.eu	0.9%	0,07 XMR	USA, Asia, Canadá
xmr.nanopool.org	1%	1 XMR	USA, Asia, EU
supportxmr.com	0.9%	0,1 XMR	USA, EU

E. Diseño de la propuesta

Una vez determinados los diferentes elementos relevantes para la propuesta es de importancia establecer un esquema que defina en que orden se ejecutarán los procesos para la minería de criptomonedas en Raspberry Pi, comenzando por temas de configuración del equipo hasta la evaluación de factibilidad del proceso, el proceso se desarrollará de la siguiente forma:

- Conexión del hardware e instalación del sistema operativo
- Configuración del wallet para criptomonedas
- Configuración del software minador
- Ejecución de la minería de criptodivisas y pruebas de uso
- Factibilidad de la minería de criptodivisas mediante Raspberry Pi

F. Configuración del software minador

Cumpliendo con los pasos previos, los requerimientos externos para ejecutar la minería están cubiertos, ahora se ejecutan los diferentes comandos en Raspberry Pi OS mediante línea de comando para agregar los componentes necesarios. Una vez inicializada la Raspberry Pi se tiene varias opciones para manejar el hardware y ejecutar la minería, pero en este caso se usará de forma remota mediante SSH. Primero, se debe conocer la dirección ip con la que esté conectada el equipo, ejecutar el comando ssh pi@"direccion ip del equipo minador" dentro del terminal del equipo Windows, enviara un hash de seguridad que se debe confirmar y por último ingresar la clave que se asigna al equipo. [21]

Una vez establecida la conexión con el equipo minador se debe instalar varias dependencias y repositorios, pero además se debe tener en cuenta que el algoritmo criptográfico RandomX que usa Monero requiere que el sistema donde se ejecute la minería debe ser de 64 bits y Raspberry Pi OS es de 32 bits, lo cual no es un inconveniente debido a que el sistema operativo cuenta con una máquina virtual de 64 bits de alto rendimiento llamada "Debian Stretch of 64 bits" la cual se ejecuta con el comando ds64-shell, con lo cual el equipo estará adaptado para los requerimientos del algoritmo. (figura 1)

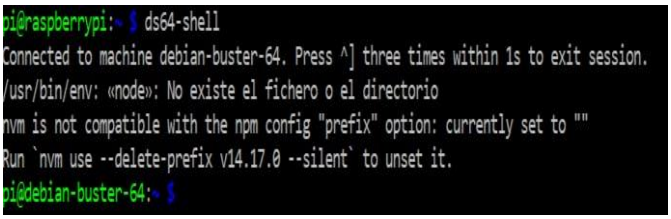

Fig. 1 Terminal Raspberry Pi OS / Windows – máquina virtual de 64 bits

En este punto se requiere ejecutar un comando que va a permitir clonar repositorios desde github, que es en donde se encuentran las dependencias del software minador. El comando es **sudo apt-get install git build-essential cmake libuv1-dev libssl-devlibhwloc-dev**.

Con el comando anterior ejecutado el siguiente paso es copiar del repositorio el software minador oficial de Monero desde https://github.com/xmrig/xmrig.git.

En este punto se tiene el minador en el equipo con todas las dependencias que necesita (figura 2), se debe ingresar al directorio del minador mediante el comando cd xmrig, y crear un nuevo directorio llamada build, mediante el comando mkdir cuya función es crear un directorio nuevo, se entra al directorio mediante cd build. En este punto se ejecuta un comando muy importante cmake que es el encargado de crear un ejecutable con toda la información del repositorio que se clono del software minador.

Para el mejoramiento de la lectura, se ha presentado una versión simplificada del proceso de instalación y configuración de cada uno de los componentes.

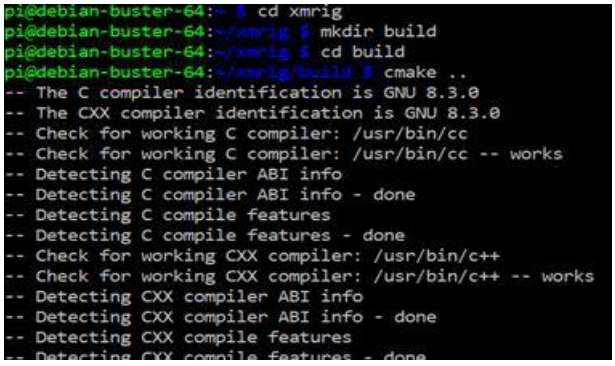

Fig. 2 Creando ejecutable del software minador.

IV. RESULTADOS

Una vez que el software minador ha sido instalado correctamente, se procede a ejecutar la máquina virtual de 64 bits de Raspberry Pi OS, ingresar al directorio del programa mediante cd xmrig, y de igual manera al directorio build mediante cd build.

En este punto, solo falta ingresar los datos al software minador para que se ejecute, estos deben ser ingresados en un orden especifico, se pueden obtener desde la página oficial del software minador, se debe ingresar la dirección del wallet, elegir el pool y en el apartado de línea de comando Linux aparecerá la información que se debe ingresar, los datos de la siguiente forma:./xmrig -o xmrpool.eu:9999 -u *dirección del wallet* -k –tls (figura 3). El único cambio que se efectuara es el puerto 5555 en el cual la dificultad del minado se ajustara a la capacidad del hardware.

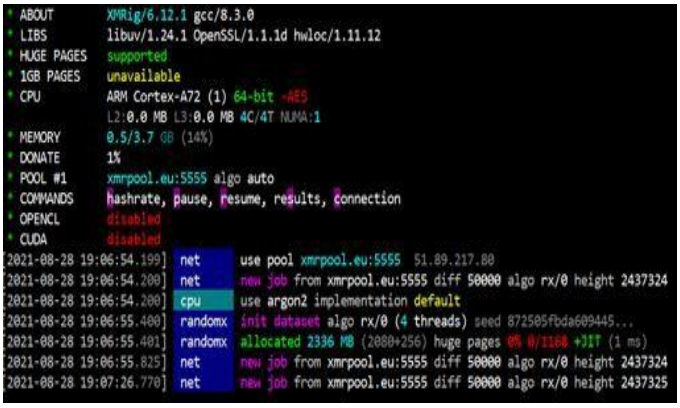

Fig. 3 Ejecución de la minería de criptodivisas.

Como muestra la figura 4, el comando connection entregara información detallada de la conexión, el pool de minería que se está usando, el algoritmo en este caso es RandomX y varios detalles adicionales.

Fig. 4. Comando connection del software minador.

El comando results entregara diferentes valores que se han presentado durante el tiempo que lleva ejecutada la minería (figura 5), como accepted que son el número de hashes aceptados, el pool-side hashes que son el número de total de hashes que producen los usuarios del pool juntos, difficulty el nivel de dificultad de minado establecido por la criptomoneda y finalmente el avg result time que es la cantidad de tiempo en la cual se mina un bloque dentro de la blockchain, además se muestra en la parte inferior una tabla que indica los 10 hashes de mayor dificultad y su porcentaje de enfuerzo.

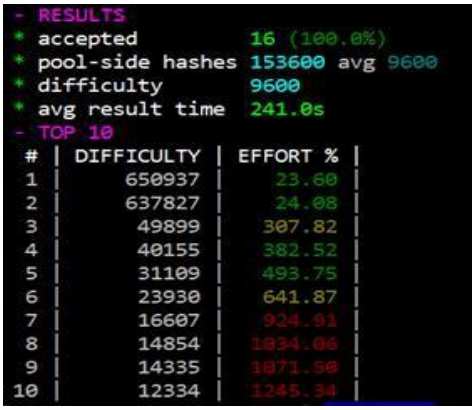

Fig. 5. Comando result del software minador.

Tabla 5 - Características de equipo Raspberry Pi.

Modelo	Raspberry Pi 4 Model B
Procesador	ARM Cortex-A72- 4 núcleos
Memoria RAM	4 GB
Memoria ROM	16 GB MicroSD
Consumo	6 watts/0.006 kW/h
Precio	$80.00 (precio local)

Luego de conocer los procesos y el entorno de minería de criptodivisas es momento de revisar la capacidad minera del hardware para lo cual se analiza cual es el hashrate que produce el equipo y la cantidad de criptodivisa que se logra minar, para posteriormente poder comparar con otros hardware de minería. Por ello es importante tener claro las características del hardware Raspberry Pi para la posterior comparativa, en la tabla 5 se detallan las características.

Para monitorizar las criptodivisas minadas se debe utilizar la página del pool de minería, e ingresando la dirección del wallet se visualizará esa información (figura 6).

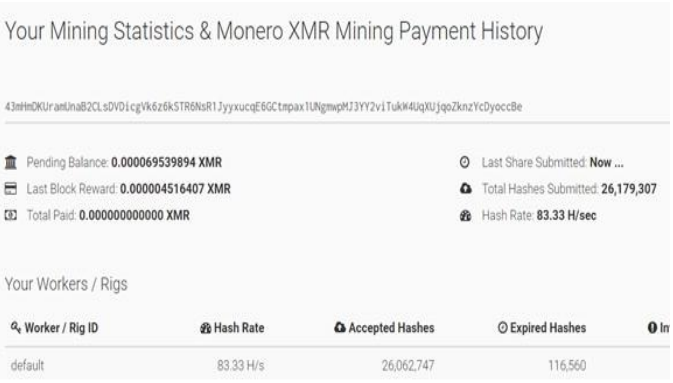

Fig. 6. Información de criptomonedas minadas.

Al observar el tablero de resultados del proceso de minado, se puede contrastar que el hashrate del equipo se encuentra en alrededor de 83.33 H/s cerca del valor que entrega el software minador que será el que se utilizará como referencia al ser calculado directamente del hardware, además muestra el total de hashes aceptados en el pool, y la cantidad XMR (figura 7), es decir lo que se ha minado hasta el momento, usando como base este valor menos la diferencia de lo que entregue el sistema luego de ejecutar la minería tendremos la cantidad que puede minar el equipo, el valor con el que comienza es de 0.000069539894 XMR. Las pruebas se ejecutarán en un tiempo de 3 horas para poder verificar un hashrate confiable que permita hacer estimaciones de la minería en tiempos prolongados, y poder realizar una evaluación fiable.

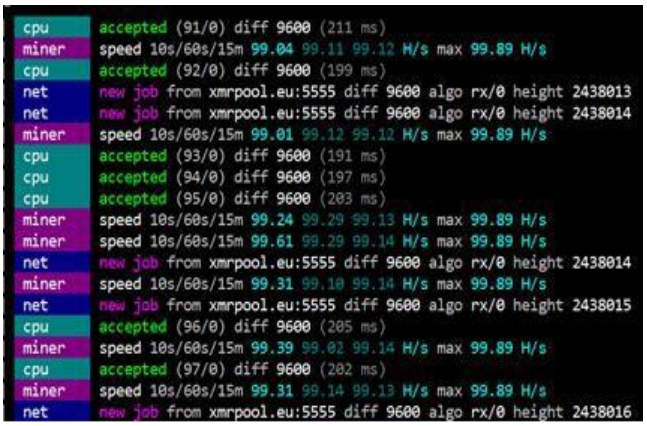

Fig. 7. Minería de criptodivisas fin.

Una vez finalizado el proceso se confirma que el ultimo hashrate que entrega el software es de 99.31 H/s de media y de 99.89 H/s de máximo, confirmando una cantidad estable muy parecida a la del inicio del proceso, durante el minado no es necesario monitorizar el equipo o el software ambos trabajaran de forma continua siempre y cuando no exista algún inconveniente en la fuente de alimentación o el acceso a la red (tabla 6).

Tabla 6 - Minería en equipo Raspberry Pi

Tiempo de actividad	3 horas (14:34:29 del 29/08/2021 - 17:34:41 del 29/08/2021)
Cantidad de XMR inicio	0.000069539894 XMR
Cantidad de XMR fin	0.000076851673 XMR
XMR minado	0.000007311779 XMR
Promedio de hashrate	99.14 H/s
Consumo	6 watts

Para obtener un punto de comparación verificable es importante establecer un proceso de minería de criptodivisas en otro hardware con diferentes características, tanto a nivel técnico como de usabilidad, por lo cual se ejecuta en un equipo secundario con sistema operativo Windows de uso común.

Luego de ejecutar la minería en Raspberry Pi y en un equipo de uso regular, se plantea en la Tabla 7 una comparativa de la diferencia de resultados entre ambos dispositivos, posteriormente se realiza una comparación relacionada con el costo energético de realizar el minado en cada equipo, que se muestra en la Tabla 8.

Tabla 7 - Comparativa de Procesador y Hashrate

Hardware	Características	Hashrate	XMR (3 horas)
Raspberry Pi	ARM Cortex-A72- 4 núcleos 1.5 GHz/ 4GB RAM	99.14 H/s	0.000007311779 XMR
Equipo secundario	AMD Ryzen 5 3500U 4 núcleos 8 hilos 3.7 GHz/ 12GB	544 H/s	0.000009600011 XMR

El apartado energético es de elevada importancia en el mundo de las criptodivisas, debido a que el enorme impacto del consumo para la minería actual está causando que muchos de los usuarios cuestionen sus principios, lo cual incluso produjo una disminución del valor de la mayoría de las criptodivisas debido a publicaciones que hablaban del impacto de la minería mundial. En este contexto es importante la aparición de minería en hardware de bajo consumo como Raspberry Pi que nos permita seguir validando las transacciones de la cadena de bloques con un gasto energético eficiente.

Tabla 8 - Comparativa de uso energético promedio

Hardware	Consumo	Valor del consumo en un mes ($0.04 x kW/h)
Raspberry Pi	6 watts - 0.006 kW/h	$0.1728
Equipo secundario	65 watts - 0.065 kW/h	$1.872

V. CONCLUSIONES

- La evaluación de los diferentes algoritmos de consenso y criptográficos permitieron la elección de una criptodivisa adecuada para el proceso de minería en Raspberry Pi.
- La criptodivisa Monero elegida para el proceso de minería se ajusta a las capacidades del hardware, siendo minable únicamente mediante CPU lo cual evita la minería mediante dispositivos ASIC una comunidad que disminuye las recompensas para equipos modestos.
- Las pruebas de minería de Monero en Raspberry Pi se ejecutaron de forma satisfactoria logrando visibilizar la capacidad del equipo, y entregando una guía de los procesos necesarios para la misma.
- La comparativa con el hardware secundario permitió tener una idea clara de la capacidad de Raspberry Pi frente a otro equipo, visibilizando sus ventajas energéticas y de costes.
- La minería de criptodivisas en Raspberry Pi es una alternativa factible, y hace frente al problema del elevado consumo energético de la minería actual debido a su consumo menor, además gracias al coste del equipo entrega la posibilidad de la entrada de nuevos mineros a la red atraídos por minar en un equipo que no afecte significativamente sus finanzas en el momento de comprarlo.
- Hacer uso de otros algoritmos de consenso que requieran una cantidad de activo inicial, debido que estos tipos de

algoritmos no presentan carga de procesamiento para el equipo, lo cual podría hacer aún más eficiente el uso de Raspberry Pi, podría ser una alternativa de crecimiento del activo que se minó.

- Realizar un análisis de posibles crecimientos de criptodivisas, para ejecutar un minado en vista de rendimiento económico, debido a que el valor de estas puede crecer incluso varios cientos de veces en tiempos cortos, entregando un beneficio al usuario que realizo el análisis.

REFERENCES

[1] Vujičić, D., Jagodić, D., & Ranđić, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh) (pp. 1-6). IEEE.

[2] Kher, R., Terjesen, S., & Liu, C. (2021). Blockchain, Bitcoin, and ICOs: a review and research agenda. Small Business Economics, 56(4), 1699-1720.

[3] Alikkal, V., C.G, R., Gopakumar, G., & Shahil, K. (2019). Implementation of Bitcoin Mining using Raspberry Pi. Conference: 2019 International Conference on Smart Systems and Inventive Technology. India.

[4] Perlman, N. (Abril de 2021). How To Ensure The U.S. Leads In Cryptocurrency Now And In The Future. Obtenido de https://www.forbes.com/sites/forbesfinancecouncil/2021/04/20/how-to-ensure-the-us-leads-in-cryptocurrency-now-and-in-the-future/

[5] Badea, L., & Mungiu-Pupăzan, M. C. (2021). The economic and environmental impact of bitcoin. IEEE Access, 9, 48091-48104.

[6] Lansky, J. (2018). Possible State Approaches to Cryptocurrencies. Possible State Approaches to Cryptocurrencies. Czech Republic. doi:10.20470/jsi.v9i1.335

[7] Buzzi, A. M., Cittadini, M. E., & De Oliveira, M. (Octubre de 2018). Introducción a las criptomonedas. San Luis, Argentina. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/74074/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

[8] Náñez Alonso, S. L., Jorge-Vázquez, J., Echarte Fernández, M. Á., & Reier Forradellas, R. F. (2021). Cryptocurrency mining from an economic and environmental perspective. Analysis of the most and least sustainable countries. Energies, 14(14), 4254.

[9] Azbeg, K., Ouchetto, O., Jai Andaloussi, S., & Fetjah, L. (2021). An overview of blockchain consensus algorithms: comparison, challenges, and future directions. Advances on smart and soft computing, 357-369.

[10] [A] Varghese, L., Deepak, G., & Santhanavijayan, A. (2019, December). An IoT analytics approach for weather forecasting using raspberry Pi 3 Model B+. In 2019 fifteenth international conference on information processing (ICINPRO) (pp. 1-5). IEEE.

[11] [B] Khalifa, A. F., Badr, E., & Elmahdy, H. N. (2019). A survey on human detection surveillance systems for Raspberry Pi. Image and Vision Computing, 85, 1-13.

[12]Conway, L. (2021). Best Bitcoin Wallets. Obtenido de https://www.investopedia.com/best-bitcoin-wallets-5070283

[13] Fu, W., Wei, X., & Tong, S. (2021). An improved blockchain consensus algorithm based on raft. Arabian Journal for Science and Engineering, 46(9), 8137-8149.

[14] [C] B. P. Rankhambe and H. Kaur Khanuja, "A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum," 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), 2019, pp. 1-7, doi: 10.1109/ICCUBEA47591.2019.9129332.

[15][D] Yang, W., Garg, S., Huang, Z., & Kang, B. (2021). A decision model for blockchain applicability into knowledge-based conversation system. Knowledge-Based Systems, 220, 106791.

[16] [E] Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Materials Today: Proceedings, 37, 2653-2659.

[17] Alsunaidi, S., & Alhaidari, F. (2019). Una encuesta de algoritmos de consenso para Tecnología Blockchain. Arabia Saudita. doi: 10.1109/ICCISci.2019.8716424

[18] Coinmarketcap. (2021). Principales 100 Criptomonedas por capitalización de mercado. Obtenido de https://coinmarketcap.com/es/

[19] Li, Y., Yang, G., Susilo, W., Yu, Y., Ho Au, M., & Liu, D. (2019). Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. Obtenido de https://ieeexplore.ieee.org/abstract/document/8685178

[20] [F] Haghighat, A. T., & Shajari, M. (2019). Block withholding game among bitcoin mining pools. Future Generation Computer Systems, 97, 482-491.

[21] Gangonells, O. V. (2020). LA MINERÍA EN CRIPTOMONEDAS. Barcelona.