



**UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA DE INGENIERÍA EN TELEINFORMÁTICA**

**TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN TELEINFORMÁTICA**

**ÁREA
TECNOLOGÍA DE LOS ORDENADORES**

**TEMA
“EVALUACIÓN DE FACTIBILIDAD DE LA MINERÍA DE
CRIPTODIVISAS MEDIANTE RASPBERRY PI”**

**AUTORA
LOAYZA CORDOVA CRISTHIAN ALEXIS**

**DIRECTOR DEL TRABAJO
ING. PLAZA VARGAS ANGEL MARCEL, MG**

GUAYAQUIL, ABRIL 2021



ANEXO XI.- FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN



FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:			
Evaluación de factibilidad de la minería de criptodivisas mediante Raspberry Pi			
AUTOR(ES) (apellidos/nombres):		Loayza Córdova Cristhian Alexis	
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):		Ing. Castillo León Rosa Elizabeth, MG/ Ing. Plaza Vargas Ángel Marcel, MSC	
INSTITUCIÓN:		Universidad de Guayaquil	
UNIDAD/FACULTAD:		Facultad de Ingeniería Industrial	
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:		Ingeniería en Teleinformática	
FECHA DE PUBLICACIÓN:		28/09/2021	No. DE PÁGINAS: 129
ÁREAS TEMÁTICAS:		Tecnología de los ordenadores	
PALABRAS CLAVES/ KEYWORDS:		Criptodivisas, Cadena de bloques, Criptografía, Raspberry Pi, Minería, Hashrate, Monero, Sustentabilidad, Transacciones	
RESUMEN/ABSTRACT (100-150 palabras): Dentro del cambiante sistema financiero mundial, las criptodivisas se han posicionado como una opción interesante que entrega a sus usuarios diferentes opciones de uso, está basada en los principios de descentralización que el sistema tradicional no ha cumplido, pero este tipo de activos corre el riesgo de perder su integridad debido a los grandes intereses de centros de minería masiva de criptodivisas, además de que representan una amenaza ambiental debido a su alto consumo energético. Por lo cual el presente trabajo mediante la metodología cuasi experimental realizara 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, en la cual, aportando a la seguridad de la red mediante el proceso de minería, planteemos una opción energéticamente sostenible de la misma sin renunciar a los principios fundamentales de las criptodivisas.			
ADJUNTO PDF:		SI (X)	NO

CONTACTO CON AUTOR/ES:	Teléfono: 0997595501	E-mail: cristhian.loayzac@ug.edu.ec
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramón Maquilón Nicola	
	Teléfono: 593-2658128	
	E-mail: direccionTi@ug.edu.ec	



**ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE
AUTORIZACIÓN DE LICENCIA GRATUITA
INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO COMERCIAL DE LA
OBRA CON FINES NO ACADÉMICOS**

**FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA CON
FINES NO ACADÉMICOS

Yo, **LOAYZA CORDOVA CRISTHIAN ALEXIS**, con C.C. No. **070701265-4**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es “**EVALUACIÓN DE FACTIBILIDAD DE LA MINERÍA DE CRIPTODIVISAS MEDIANTE RASPBERRY PI**” son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.

A handwritten signature in black ink, appearing to read "Cristhian Alexis", written over a horizontal line.

LOAYZA CORDOVA CRISTHIAN ALEXIS
C.C. No. 094078567-8



**ANEXO VII.- CERTIFICADO PORCENTAJE DE
SIMILITUD
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Habiendo sido nombrado ING. ANGEL MARCEL PLAZA VARGAS, tutor del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por LOAYZA CORDOVA CRISTHIAN ALEXIS, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: EVALUACIÓN DE FACTIBILIDAD DE LA MINERÍA DE CRIPTODIVISAS MEDIANTE RASPBERRY PI, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio URKUND quedando el 1 % de coincidencia.

recompensas y demás cuestiones importantes por lo que se le conoce como democracia digital. Según Alsunaidi & Alhaidari (2019), el proceso que compone la prueba de participación delegada es el siguiente: • El comienzo del proceso inicia con la elección de delegados, el cual se cumple mediante un sistema de voto en tiempo real, de esta forma existe confianza en los usuarios o nodos elegidos. Un punto importante que toman en cuenta los usuarios es la cantidad de activo que tienen los usuarios a los que votan, lo cual brinda mayores oportunidades de ser elegido. • Acto seguido luego de la votación y elección de delegados, ocurre la creación de bloques en este proceso los elegidos tienen

<https://secure.orkund.com/old/view/107004389-735609-711932>



Firmado electrónicamente por:
**ANGEL MARCEL
PLAZA VARGAS**

ING. ANGEL MARCEL PLAZA VARGAS
DOCENTE TUTOR
C.C. 0915953665
FECHA: 10/9/2021



**ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR
DEL TRABAJO DE TITULACIÓN**

**FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN
TELEINFORMÁTICA**



Guayaquil, 13 de septiembre del 2021.

Sr (a).

Ing. Annabelle Lizaraburu Mora, MG.

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

**FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE
GUAYAQUIL**

Ciudad. -

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación **“EVALUACIÓN DE FACTIBILIDAD DE LA MINERÍA DE CRIPTODIVISAS MEDIANTE RASPBERRY PI”** del estudiante **LOAYZA CORDOVA CRISTHIAN ALEXIS**, indicando que ha cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, **CERTIFICO**, para los fines pertinentes, que la estudiante está apta para continuar con el proceso de revisión final.

Atentamente,



Firmado electrónicamente por:
**ANGEL MARCEL
PLAZA VARGAS**

ING. ANGEL MARCEL PLAZA VARGAS, MSC
CC: 0915953665

13 de septiembre del 2021



ANEXO VIII.- INFORME DEL DOCENTE REVISOR
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA



Guayaquil, 21 de septiembre de 2021

Sr (a).

Ing. Annabelle Lizarzaburu Mora, MG.

Director (a) de Carrera Ingeniería en Telemática / Telemática

FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL
 Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación **"EVALUACIÓN DE FACTIBILIDAD DE LA MINERÍA DE CRIPTODIVISAS MEDIANTE RASPBERRY PI"** del estudiante **LOAYZA CORDOVA CRISTHIAN ALEXIS**. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimiento de los siguientes aspectos:

Cumplimiento de requisitos de forma:

El título tiene un máximo de 11 palabras.

La memoria escrita se ajusta a la estructura establecida.

El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad.

La investigación es pertinente con la línea y sublíneas de investigación de la carrera.

Los soportes teóricos son de máximo 5 años.

La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:

El trabajo es el resultado de una investigación.

El estudiante demuestra conocimiento profesional integral.

El trabajo presenta una propuesta en el área de conocimiento.

El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica el que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,



Resado digitalmente por:

ROSA

ELIZABETH

CASTILLO LEON

ING. ROSA ELIZABETH CASTILLO LEÓN, MG.

C.C: 0922372610

FECHA: 21 DE SEPTIEMBRE DE 2021

Dedicatoria

Dedico el presente trabajo de titulación a mi familia, en especial a mi querida madre María Córdova que nunca dejo de creer en mí y me apoyo durante todos estos años para poder lograr este objetivo, a mis hermanos Steven, Jean Pierre y Anthony que me han brindado su apoyo en los momentos más duros, sin ellos nada hubiera sido posible, gracias por su apoyo incondicional, este logro también es de ustedes.

Agradecimiento

Agradezco a todas las personas que me han brindado palabras de aliento en estos años, que de una u otra forma me entregaron la motivación para seguir adelante, a mi familia que a pesar de las dificultades estuvieron siempre pendientes de mí y no dejaron de creer en mi capacidad, a mis abuelos, tíos y primos que siempre tuvieron sabios consejos para mí, a cada uno de los docentes a lo largo de la carrera por los conocimientos que me impartieron y sus experiencias, a mis compañeros que a lo largo de los años se volvieron amigos entrañables por sus consejos y momentos compartidos, a mi tutor de este trabajo por la oportunidad de trabajar juntos en él, a mi novia por sus palabras de aliento y apoyo, y a mí un recordatorio de no darse por vencido a pesar de las dificultades, gracias infinitas a todos.

Índice General

N°	Descripción	Pág.
	Introducción	1

Capítulo I

El Problema

N°	Descripción	Pág.
1.1	Planteamiento del problema	3
1.2	Justificación	4
1.3	Objetivos de la investigación	5
1.3.1	Objetivo general.	5
1.3.2	Objetivos específicos.	5
1.4	Formulación del problema	5
1.5	Variables	6
1.5.1	Variable independiente	6
1.5.2	Variable dependiente	6
1.6	Conceptualización y operacionalización de las variables	6
1.7	Alcance	6

Capítulo II

Marco Teórico

N°	Descripción	Pág.
2.1	Antecedentes del estudio	8
2.1	Antecedentes internacionales	8
2.1	Antecedentes nacionales	11
2.2	Fundamentación teórica	14
2.2.1	Criptodivisas	14
2.2.2	Minería de Criptodivisas	15
2.2.3	Cadena de bloques o Blockchain	16
2.2.3.1	Cadena de bloques publica	17
2.2.3.2	Cadena de bloques privada	17
2.2.3.3	Cadena de bloques de consorcio	18
2.2.4	Red Peer-to-Peer	18

N°	Descripción	Pág
2.2.5	Algoritmos de consenso	19
2.2.5.1	Prueba de trabajo o Proof of work (PoW)	20
2.2.5.2	Prueba de participación o Proof of Stake (PoS)	21
2.2.5.3	Prueba de participación delegada o Delegated Proof of Stake (DPoS)	23
2.2.5.4	Prueba de actividad o Proof of Activity (PoA)	25
2.2.5.5	Prueba de quemado o Proof of Burn (PoB)	26
2.2.5.6	Prueba de capacidad o Proof of Capacity (PoC)	27
2.2.5.7	Prueba de tiempo transcurrido o Proof of Elapsed Time (PoET)	28
2.2.5.8	Prueba de asignación o Proof of Assignment (PoA)	29
2.2.5.9	Algoritmo de consenso del protocolo Ripple (RPCA)	30
2.2.5.10	Prueba de Autoridad o Proof of Authority (PoA)	31
2.2.6	Criptografía	31
2.2.6	Clave única o métodos simétricos	33
2.2.6	Clave publica o métodos asimétricos	33
2.2.7	Sistemas criptográficos hash	34
2.2.7.1	Secure Hash Algorithm SHA-256	36
2.2.7.2	Ethash	37
2.2.7.3	Scrypt	39
2.2.7.4	X11	40
2.2.7.5	CryptoNight	41
2.2.7.6	RandomX	42
2.2.8	Raspberry Pi	44
2.2.9	CPU	45
2.2.10	GPU	46
2.2.11	ASIC	47
2.2.12	AES	47
2.2.13	Arquitectura ARM	48
2.2.14	Hashrate	49
2.2.15	Pool de minería	49
2.2.16	Crypto Wallet o Monedero de criptomonedas	49

N°	Descripción	Pág.
2.3	Fundamentación legal	50
2.3.1	Constitución de la Republica del Ecuador	50
2.3.2	Código Orgánico Integral Penal (COIP)	50
2.3.3	Banco Central del Ecuador	52

Capítulo III

Propuesta

N°	Descripción	Pág.
3.1	Métodos de investigación	53
3.1.1	Metodología cuasi Experimental	53
3.1.2	Metodo Descriptivo	53
3.1.3	Metodología Evaluativa	54
3.2.	Población y muestra	55
3.3	Técnica de recolección de datos	55
3.3.1	Encuesta	55
3.3.2	Análisis global de resultados	62
3.4	Elementos utilizados para el diseño de la propuesta	63
3.4.1	Algoritmos de consenso	63
3.4.2	Algoritmos criptográficos hash	67
3.4.3	Criptodivisa o Criptomoneda	69
3.4.4	Pool de minería	69
3.4.5	Modelo Raspberry Pi	70
3.4.6	Sistema operativo	70
3.5	Diseño de la propuesta	71
3.5.1	Conexión del hardware e instalación del sistema operativo	71
3.5.1.1	Conexión del hardware	71
3.5.1.2	Instalación de sistema operativo	73
3.5.2	Configuración del wallet para criptomonedas	77
3.5.3	Configuración del software minador	80
3.5.4	Ejecución de la minería de criptodivisas y pruebas de uso	83
3.5.4.1	Ejecución de la minería de criptodivisas	83

Nº	Descripción	Pág.
3.5.4.2	Pruebas de uso	86
3.5.4.2.1	Pruebas en Raspberry Pi	86
3.5.4.2.2	Pruebas en equipo secundario	90
3.5.5	Factibilidad de la minería de criptodivisas mediante Raspberry Pi	91
3.5.5	Factibilidad de la minería de criptodivisas mediante Raspberry Pi	91
3.5.5.1	Factibilidad del hardware	91
3.5.5.2	Factibilidad económica	92
3.5.5.3	Factibilidad energética	93
3.5.5.3	Factibilidad general	93
3.6	Conclusiones y Recomendaciones	94
3.6.1	Conclusiones	94
3.6.2	Recomendaciones	94
	Anexos	96
	Bibliografía	102

Índice de Tablas

Nº	Descripción	Pág.
1	Definición de las variables	6
2	Trabajos internacionales sobre Factibilidad de Minería de Criptodivisas	10
3	Trabajos nacionales sobre Factibilidad de Minería de Criptodivisas	12
4	Principales criptodivisas que usan el algoritmo SHA-256	38
5	Principales criptodivisas que usan el algoritmo Ethash	39
6	Principales criptodivisas que usan el algoritmo Scrypt	40
7	Principales criptodivisas que usan el algoritmo X11	41
8	Principales criptodivisas que usan el algoritmo CryptoNight	42
9	Principales criptodivisas que usan el algoritmo RandomX	44
10	Modelos de raspberry pi y sus características	45
11	Cantidad de alumnos que conocen que es una criptodivisa	56
12	Que criptodivisa se encuentra más difundida entre los alumnos	57
13	Cantidad de alumnos que conocen sobre el proceso de minería de criptodivisas	58
14	Algoritmo criptográfico más difundido	58
15	Ordenador de bajo costo y tamaño reducido más difundido	59
16	Cantidad de alumnos que conocen que se puede minar criptodivisas ...	60
17	Cualidad de Raspberry Pi más favorable	61
18	Cantidad de alumnos que conocen que para minar criptomonedas se ...	62
19	Comparativa de algoritmos de consenso y características	64
20	Comparativa de algoritmos de consenso y características	65
21	Comparativa de algoritmos criptográficos y características	68
22	Comparativa pools de minería y características	71
23	Características de equipo Raspberry Pi	87
24	Minería en equipo Raspberry Pi	90
25	Características de equipo secundario	91
26	Minería en equipo secundario	91
27	Comparativa del hardware	92
28	Factores económicos	93

Nº	Descripción	Pág.
29	Comparativa económica	93
30	Comparativa energética	94

Índice de Figuras

Nº	Descripción	Pág.
1	Como funciona una blockchain	17
2	Estructura de una red peer to peer	18
3	Prueba de Trabajo	21
4	Prueba de Participación	24
5	Proceso criptográfico	33
6	Proceso criptográfico Simétrico	34
7	Proceso criptográfico Asimétrico	35
8	Proceso Sistema criptográfico hash	36
9	Algoritmo SHA-256	37
10	Raspberry Pi 4 modelo B	46
11	CPU	47
12	GPU	48
13	ASIC	48
14	AES	49
15	Procesador con arquitectura ARM	50
16	Cantidad de alumnos que conocen que es una criptodivisa	57
17	Que criptodivisas se encuentra más difundida entre los alumnos	58
18	Cantidad de alumnos que conocen sobre el proceso de minería de cripto...	59
19	Algoritmo criptográfico más difundido	60
20	Ordenador de bajo costo y tamaño reducido más difundido	61
21	Cantidad de alumnos que conocen que se puede minar criptodivisas con R...	62
22	Cualidad de Raspberry Pi más favorable	63
23	Cantidad de alumnos que conocen que para minar criptomonedas ...	64
24	Logotipo de Monero (XMR)	71
25	Caja Raspberry Pi 4 Model B versión 4GB RAM	74
26	Raspberry Pi Raspberry Pi 4 Model B y disipadores	74
27	Raspberry Pi y conexiones	75
28	Raspberrypi.org/software	75
29	Raspberry Pi imager instalado	76

Nº	Descripción	Pág.
30	Raspberry Pi imager- Operating System	76
31	Raspberry Pi imager- Storage	77
32	Raspberry Pi imager- Listo para el proceso	77
33	Raspberry Pi imager- Proceso iniciado	77
34	Raspberry Pi OS- Guia de inicio	78
35	Raspberry Pi OS- Clave del equipo	78
36	Página oficial del wallet de Monero	79
37	Oxygen Orion GUI Wallet	80
38	Monero Wallet	80
39	Monero Wallet – Datos del monedero	81
40	Monero Wallet – Wallet listo	81
41	Terminal Raspberry Pi OS mediante Windows – Conexión mediante SSH	82
42	Terminal Raspberry Pi OS mediante Windows – Máquina virtual de 64 bits	82
43	Terminal Raspberry Pi OS mediante Windows – Comandos de actualización	83
44	Terminal Raspberry Pi OS mediante Windows – Comandos de clonación	83
45	Terminal Raspberry Pi OS mediante Windows – Mlonando repositorio de	84
46	Terminal Raspberry Pi OS mediante Windows – Creando ejecutable del ...	84
47	Terminal Raspberry Pi OS mediante Windows – Compilando ejecutable	85
48	Terminal Raspberry Pi OS mediante Windows – Ingreso al software	85
49	Página oficial xmrig – Guía de ingreso	86
50	Terminal Raspberry Pi OS mediante Windows	86
51	Terminal Raspberry Pi OS mediante Windows – minería de criptodivisas	86
52	Terminal Raspberry Pi OS mediante Windows – comando hashrate del ...	87
53	Terminal Raspberry Pi OS mediante Windows – comando connection del...	88
54	Terminal Raspberry Pi OS mediante Windows – comando resultas del ...	88
55	Terminal Raspberry Pi OS mediante Windows – Minería de criptodivisas...	89
56	Tablero de información de xmrpool.eu – Información de criptomonedas ...	89
57	Terminal Raspberry Pi OS mediante Windows – Minería de criptodivisas fin	90
58	Terminal Raspberry Pi OS mediante Windows – Minería de criptodivisas...	90
59	Tablero de información de xmrpool.eu – Información de criptomonedas...	91

Nº	Descripción	Pág.
60	Página web xmrig download – selección de sistema operativo	100
61	Xmrig software – Descomprimir carpeta	100
62	Xmrig carpeta – recursos y ejecutable del software minador	101
63	Página web xmrig wizard– archivo config.json	101
64	Xmrig ejecutado en Windows– minería iniciada	102
65	Xmrig ejecutado en Windows– minería finalizada	102
66	Xmrig ejecutado en Windows– Comando hashrate	103
67	Tablero de información de xmrigpool.eu – Información de criptomonedas...	103
68	Tablero de información de xmrigpool.eu – Información de criptomoneda ...	103

Índice de Anexos

Nº	Descripción	Pág.
1	Preguntas de la encuesta	98
2	Minería de criptodivisas en equipo Windows y prueba de uso:	99



**ANEXO XIII.- RESUMEN DEL TRABAJO DE
TITULACIÓN (ESPAÑOL)
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



**“EVALUACIÓN DE FACTIBILIDAD DE LA MINERÍA DE CRIPTODIVISAS
MEDIANTE RASPBERRY PI”**

Autor: Loayza Cordova Cristhian Alexis

Tutor: Ing. Plaza Vargas Ángel Marcel, MSC

Resumen

Dentro del cambiante sistema financiero mundial, las criptodivisas se han posicionado como una opción interesante que entrega a sus usuarios diferentes opciones de uso, está basada en los principios de descentralización que el sistema tradicional no ha cumplido, pero este tipo de activos corre el riesgo de perder su integridad debido a los grandes intereses de centros de minería masiva de criptodivisas, además de que representan una amenaza ambiental debido a su alto consumo energético. Por lo cual el presente trabajo mediante la metodología cuasi experimental realizara 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, en la cual, aportando a la seguridad de la red mediante el proceso de minería, planteemos una opción energéticamente sostenible de la misma sin renunciar a los principios fundamentales de las criptodivisas.

Palabras Claves: Criptodivisas, Cadena de bloques, Criptografía, Raspberry Pi, Minería, Hashrate, Monero, Sustentabilidad, Transacciones



**ANEXO XIV.- RESUMEN DEL TRABAJO DE
TITULACIÓN (INGLÉS)
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



**‘FEASIBILITY ASSESSMENT OF CRYPTOCURRENCY MINING USING
RASPBERRY PI**

Author: Loayza Cordova Cristhian Alexis

Advisor: Ing. Plaza Vargas Ángel Marcel, MSC

Abstract

Within the changing global financial system, cryptocurrencies have positioned themselves as an interesting option that gives their users different options of use, it is based on the principles of decentralization that the traditional system has not fulfilled, but this type of assets runs the risk of losing its integrity due to the large interests of massive cryptocurrency mining centers, in addition to representing an environmental threat due to their high energy consumption. Therefore, the present work through the quasi-experimental methodology will carry out a feasibility evaluation of cryptocurrency mining using Raspberry Pi hardware, documenting the process and evaluating each of the parties involved, in search of a viable option that allows mining a cryptocurrency, in which, contributing to the security of the network through the mining process, let's propose an energy-sustainable option of the same without renouncing the fundamental principles of cryptocurrencies.

Keywords: Cryptocurrencies, Blockchain, Cryptography, Raspberry Pi, Mining, Hashrate, Monero, Sustainability, Transactions

Introducción

Debido a la creciente globalización es cada vez más indispensable un sistema financiero en el cual las transacciones se realicen de forma inmediata, sin la 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 .

En base esto se produjo la creación de las criptomonedas como una solución a los inconvenientes del sistema financiero tradicional, fundamentado en la primera criptomoneda bitcoin la cual (Nakamoto, Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer, 2008) 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 sería 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 (Domingo, 2018) 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 específico a las cosas.

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 Alikkal, C.G, Gopakumar, & Shahil (2019) consume cantidades enormes de energía que ponen en peligro el futuro del sistema, debido a los centros de minería masivos, que además provocan pérdida en la 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. A continuación, se detalla el contenido del trabajo que está estructurado por capítulos, para lograr los objetivos.

En el primer capítulo se detalla la forma en que el problema se origina, los puntos que justifican la creación de este trabajo, los objetivos a cumplir y el alcance del proyecto.

El segundo capítulo se detalla los trabajos de ámbito internacional y nacional que sirven de punto de partida y guía del tema a tratar, además se entrega conceptos de los diferentes componentes del proyecto, fundamentación teórica, conceptual y el marco legal que se apegue al proyecto. En el tercer capítulo se desarrolla la propuesta de investigación del proyecto, se detalla la metodología que será utilizada, la técnica de recolección de datos, y los diferentes procesos de evaluación al que se someterá a los procesos implicados, los resultados y por último las conclusiones y recomendaciones.

Capítulo I

El Problema

1.1. Planteamiento del problema

“Las criptomonedas son activos financieros digitales, para los cuales la propiedad y las transferencias de propiedad están garantizadas por una tecnología descentralizada criptográfica”. (Giudici, Milne, & Vinogradov, 2020)

En medio del cambiante e impredecible mercado financiero mundial se erige una nueva tendencia transaccional como son las criptodivisas, las cuales, presentan ventajas inimaginables por encima de los sistemas financieros actuales que, a pesar de la continua mejora, mantienen problemas de fondo en la estructura y en especial en los sectores menos desarrollados de la sociedad.

“Es necesario, por tanto, un sistema de pago electrónico basado en prueba criptográfica en lugar de confianza, permitiendo que dos partes interesadas realicen transacciones directamente entre ellas, sin necesidad de un tercero de confianza. Si las transacciones son computacionalmente imposibles de revertir, protegerán a los vendedores del fraude, y cualquier mecanismo de depósito de garantía se puede implementar fácilmente para proteger al comprador”. (Nakamoto, 2008)

De esta premisa nace el principio de la red blockchain, el cual es usado por la mayoría de las criptodivisas, los principales fundamentos son ser distribuida, segura e inmutable apegadas a los fundamentos financieros que en la mayoría no han cumplido los sistemas financieros tradicionales, en especial el de descentralización.

Dentro de este enorme mundo que plantean 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. por lo cual se plantea evaluar la factibilidad de la minería de criptodivisas mediante Raspberry Pi, ya que el hardware además de ser de bajo coste presenta múltiples ventajas de consumo energético y automatización. Además, el consumo energético en la minería de criptodivisas se ha vuelto un punto de discusión debido al elevado nivel y al crecimiento de los mineros con equipos de alto consumo que lo provoca, a la cual la minería en equipos como Raspberry Pi podría plantearse como una solución sostenible.

1.2. Justificación

“Como consecuencia de la explosiva aparición de criptomonedas, ha crecido el interés por parte de la academia en estudiar sus características, en particular el desempeño y el riesgo del mercado que presentan, pues además de facilitar las operaciones cambiarias y la obtención de financiamiento para las empresas, han alcanzado una gran popularidad por haberse convertido en novedosos vehículos de inversión”. (López-Herrera, Macías Trejo, & de la Torre Torre, 2020)

Dadas las circunstancias del panorama mundial en el sector financiero es más que una necesidad el buscar alternativas de intercambio monetarias más justas, descentralizadas y con opciones de crecimiento con inversiones más modestas, dentro de este contexto, se busca enseñar y facilitar los conocimientos de las distintas alternativas de intercambio monetario entregando conceptos claros con indicaciones precisas de los diferentes tipos de criptodivisas, minería, validación, intercambio y las ventajas sobre el sistema financiero actual.

Según Perlman (2021), 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 (2019), 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.

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Evaluar la factibilidad de la minería de criptodivisas mediante Raspberry Pi.

1.3.2. Objetivos Específicos

- Recopilar información teórica referente para el estudio del estado del arte.
- Determinar el algoritmo de consenso y el algoritmo criptográfico de minería que mejor se ajuste a la infraestructura tecnológica escogida.
- Determinar la criptodivisa que se ajuste a la capacidad del proyecto y el impacto futuro.
- Ejecutar las diferentes pruebas de minería en la infraestructura.
- Evaluar la factibilidad del proceso, consumo y alcance.

1.4. Formulación del problema

Tomando como referencia el planeamiento del problema surge la interrogante:

¿Es factible ejecutar la minería de criptodivisas en un hardware de dimensiones reducidas como es Raspberry pi, cuál sería la criptomoneda más adecuada para el proceso?

1.5. Variables

1.5.1. Variable independiente

- Evaluación de Raspberry pi

1.5.2. Variable dependiente

- Minería de criptodivisas

1.6. Conceptualización y Operacionalización de las variables

Tabla 1.

Definición de las variables

	Independiente	Dependiente
Variable	Evaluación de Raspberry pi	Minería de criptodivisas
Definición	Es la forma de monitorizar el rendimiento de los diferentes factores, en un hardware determinado de características modestas y evaluar las capacidades.	Se compone de una lista de procesos, informáticos, criptográficos y matemáticos que permiten a un equipo demostrar el compromiso con la red, donde cada uno de estos factores pueden variar dependiendo de la red, en recompensa se le otorga un redito económico al usuario.

Información adaptada de los repositorios y artículos investigados. Elaborado por Crithian Loayza

1.7. Alcance

La finalidad del presente trabajo de titulación es evaluar la factibilidad de la minería de criptodivisas mediante Raspberry Pi, analizando cada de unas de las variables involucradas en el proceso:

- Algoritmo de consenso
- Algoritmo criptográfico de minería
- Criptodivisa
- Software minador y Capacidad del hardware

Una vez definida la criptodivisa a implementar con los diversos recursos tecnológicos en el hardware para que llegue a minar una criptodivisa, con el objetivo de evaluar la factibilidad del minado, ventajas, desventajas, costes, beneficios, dificultad y de esta forma definir una conclusión sobre la situación actual y la tendencia.

Capítulo II

Marco Teórico

2.1. Antecedentes del estudio

En el inicio de los fundamentos de las criptodivisas más en específico bitcoin como la principal referente que fue fundamentada por Satoshi Nakamoto en el artículo “Bitcoin A Peer-to-Peer Electronic Cash System”, expresa que la mayoría pensaba que el futuro era realmente incierto o una idea de paso, en la actualidad, la aceptación de las criptomonedas ha sido sumamente elevado y existe un punto de crecimiento importante durante la pandemia del SARS-CoV debido diversos factores favorables en el sistema monetario digital, como la ausencia de contacto físico o de presencia del titular para diversos fines, transacciones internacionales entre otras. Además de todas las ventajas que los sistemas de minería actuales de las criptomonedas de mayor demanda presentan grandes inconvenientes en el sector de la sustentabilidad, haciendo imperativo el uso de nuevos protocolos y de hardware más eficiente. (Nakamoto, Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer, 2008)

A continuación, se describen algunos estudios como antecedentes bibliográficos que fundamentan el presente trabajo y aportan conocimiento al mismo.

2.1.1. Antecedentes Internacionales

Alikkal, C.G, Gopakumar Raji y Shahil, K del Departamento de Tecnologías de la información del MEA Engineering College de la India, en el artículo “Implementation of Bitcoin Mining using Raspberry Pi”, expresa sobre cómo aprovechar el hardware Raspberry Pi para minar Bitcoin, además de como las criptomonedas se han desarrollado en un gran sistema financiero mediante las computadoras y que la minería permite obtener un consentimiento valido y seguro de cada transacción. Este trabajo propone la implementación de un minero de criptodivisas en este caso bitcoin usando el hardware Raspberry pi en combinación con un dispositivo Hash USB, más el software CG-Miner para la extracción de criptomonedas con bajo consumo de energía y costos, además de integración de un pool de minería el cual es servicio donde varios mineros se agrupan y así pueden prestar el poder computacional en conjunto para de esta forma ser recompensados, ya que de forma independiente seria casi imposible minar un bloque con la potencia del hardware, cabe recalcar que la recompensa es menor ya que se

dividirá entre el número de participantes y el poder de cómputo que prestaron, además los pool permiten una monitorización más llevadera siendo posible revisar nuestras estadísticas incluso desde un smartphone. Todo esto apuntando a la naturaleza compacta y eficiente energéticamente que presenta Raspberry pi que ayuda a mitigar el costo de los procesos actuales los cuales consumen grandes cantidades de energía, además del elevado costo. (Alikkal, C.G, Gopakumar, & Shahil, 2019)

Oriol Val Gangonells en el año 2020, en la tesis “LA MINERÍA EN CRIPTOMONEDAS” analiza las diferentes criptodivisas con mayor capitalización de mercado, y los aspectos comunes entre ellas privacidad, minería, ventajas y desventajas, que las diferencian del resto, así como el comportamiento de diferentes hardware del mercado en el momento de ejecutar la minería en estos entre ellos el de importancia para este estudio Raspberry pi, y una de las conclusiones más importantes es que el gasto computacional hoy en día en termino de consumo energético esta alcanzo niveles preocupantes, por lo cual, el tamaño del gasto energético puede compararse con el de grandes ciudades e incluso estados por lo cual es más que una necesidad el buscar algoritmos de consenso amigables que demanden menor consumo energético, pero que a la vez sigan presentando niveles de seguridad elevados que brindan confianza en las diferentes criptomonedas. (Gangonells, 2020)

Siguiendo en la línea de los desafíos actuales de las criptomonedas se encuentra la demanda de hardware en especial de GPU que debido a la minería técnicamente se encuentran agotadas, esto además está provocando altos niveles de contaminación lo cual no se apega a la filosofía inicial de las criptomonedas de ofrecer una alternativa más eficiente de intercambio monetario, y debido a los costos elevados del hardware para minería el principio de prueba de trabajo solo otorga a los usuarios con mayor poder adquisitivo lo cual va en contra de la filosofía al crear barreras para los nuevos usuarios, por lo cual, provoca que desistan del afán de minar creando una especie de oligopolio que está creando una centralización de la blockchain. (Gangonells, 2020)

El trabajo desarrollado por Harald Vranken en 2017, en el artículo “Sustainability of bitcoin and blockchains”, expone que el enfoque está en la sostenibilidad en el contexto del medio ambiente y los aspectos económicos e intentan responder si en este caso el bitcoin es sostenible a largo plazo, ya que actualmente el consumo de energía de la minería de bitcoin representa valores elevados tanto en los costos de adquisición de hardware para la minería, y aún más

elevado en el consumo energético de los mismos, el cual no se encuentra bien definido y se presentan varias estimaciones que van desde la producción de una central eléctrica en el rango de 10 MW, a extremos como el consumo de países pequeños como Irlanda o Dinamarca en el rango de 3 a 6 GW y todo esto depende de la eficiencia del hardware a la hora de minar ya que las estimaciones de menos consumo se realizan en los supuestos de equipos de mayor eficiencia y así mismo los de mayor consumo con equipos ineficientes. (Vranken, 2017)

Otro trabajo muy interesante respecto a la sustentabilidad energética de la minería de criptodivisas es el de Julieta Sanchez en 2019, en el artículo “El bitcoin y su demanda exponencial de energía: economía versus sostenibilidad”, menciona que para crear una criptomoneda se necesitan cantidades elevadas de energía en especial si son de las más demandadas, ya que la minería provoca una enorme cantidad de computadoras conectadas a la red, que en conjunto consumen elevadas cantidades de energía. Todo este panorama ha aumentado de forma elevada debido al aumento de los precios de las principales criptomonedas, porque en consecuencia si una criptomoneda eleva el valor es porque hay una mayor demanda detrás y por ende más mineros interesados en obtenerla. (Sánchez Cano, 2019)

Teniendo en cuenta estos factores de la minería, se suman varios sistemas para este tipo de transacciones en la cual cada equipo de cómputo busca respuestas a un algoritmo matemático de alta complejidad, lo cual conlleva un alto procesamiento y por ende alto consumo energético. Todo esto apunta a que la sostenibilidad y ser amigable con el ambiente debe ser tratado de forma urgente en los procesos de minería actuales para ajustarse a la realidad que vive el planeta, y que se acabe imponiendo un modelo que no dependa de la capacidad computacional para asegurar la seguridad de la red. (Sánchez Cano, 2019)

Tabla 2.

Trabajos internacionales sobre Factibilidad de Minería de Criptodivisas

Referencia	Tema	Objetivo	Herramientas
(Alikkal, C.G, 2019) (Gopakumar, & K, 2019)	Implementation of Bitcoin Mining using Raspberry Pi	Implementar la minería de bitcoin mediante Raspberry pi, y software adicional	Raspberry Pi, CG-miner, Hash usb

(Gangonells, 2020)	La minería de criptomonedas	en evaluar las diferentes criptomonedas de mayor capitalización, y evaluar la minería en distintos hardware entre estos Raspberry pi	Orange Pi, Raspberry pi, PC, Software minero
(Vranken, 2017)	Sustainability of bitcoin and blockchains	Exponer las razones por las cuales la minería de bitcoin no es sostenible a largo plazo, y es necesario el uso de hardware más eficiente	Creada y desarrollada por el autor
(Sánchez Cano, 2019)	El bitcoin y su demanda exponencial de energía versus sostenibilidad	Informar sobre las enormes cantidades de energía que consume la minería de criptodivisas	Creada y desarrollada por el autor

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

2.1.2. Antecedentes Nacionales

Dentro del ámbito nacional existen algunos trabajos relacionados como el realizado por Orrala Cajas y Chompol Pincay en 2017, con el tema “ANÁLISIS DE LAS VENTAJAS DEL USO DEL BITCOIN EN EL ECUADOR COMO UNA CRIPTOMONEDA ALTERNATIVA A LAS TRANSACCIONES COMERCIALES”, el proyecto busca una alternativa al intercambio monetario tradicional mediante criptodivisas en concreto bitcoin al ser la criptomoneda de mayor aceptación, además enumera las medidas de protección con el que cuentan los usuarios al usar una red P2P, entre las cuales están el denominado pseudo-anonimato que brindan las transacciones con este tipo de activos, ya que cifran el origen de estas con la finalidad de proteger la información de los participantes. Así mismo la cadena de bloques como

parte fundamental de la veracidad de las transacciones efectuadas, registrando cada una de ellas y llevando el control respectivo. (Orrala Cajas & Chompol Pincay, 2017)

Dentro de este mismo proyecto se nombra un tipo específico de hardware para minería de criptomonedas, ANTMINER S9 que se define como un prototipo diseñado para la minería de criptomonedas en este caso bitcoin, los cuales se conectan a la red P2P para comenzar a adquirir las criptodivisas. Además, dentro del análisis de factibilidad menciona la posibilidad de efectuar la minería de bitcoin mediante el hardware de estudio “Raspberry pi”, y que luego de ciertas configuraciones es totalmente operativo para efectuar la minería de criptodivisas, mencionando también la diferencia enorme de precios y consumo energético en comparación con otros hardware. (Orrala Cajas & Chompol Pincay, 2017)

Tomando en cuenta el punto de la familiarización de las criptodivisas en el país, Martha Caizapanta, Elisa Borja, y María González en 2018, presentan la publicación “Desarrollo de las criptomonedas en Ecuador, responsabilidad y riesgo”, en la cual expresan que el sistema monetario ecuatoriano es más tradicional que en otros sectores del mundo, pero las criptomonedas se encuentran en el mercado y cada vez se vuelven más habituales las personas que optan por este tipo de activos dentro de la sociedad, en la mayoría de casos debido a la descentralización y que no existe un organismo gubernamental que la controle. A pesar de que uno de los principales inconvenientes de las criptomonedas es la volatilidad, también es uno de los principales atractivos ya que puede generar ganancias en tiempos relativamente cortos. (Caizapanta, Borja, & González, 2018)

Además, indican algunas de las normativas legales del Ecuador en el manejo de criptomonedas, en principal el Banco Central del Ecuador menciona que las mismas no son legales dentro del país, pero que los ecuatorianos tienen la libertad de realizar las transacciones que deseen mediante internet. Dejando en claro que en el medio es importante una campaña de información al respecto para que los ciudadanos se enteren de los beneficios y riesgos, para evitar también ser víctimas de estafas. (Caizapanta, Borja, & González, 2018)

Además de los antecedentes anteriormente expuestos, uno de los puntos más importantes dentro de nuestro proyecto es la comparativa de diferentes factores para elegir la criptodivisa que mejor beneficio producirá con el hardware Raspberry pi, uno de estos factores son los algoritmos de consenso que son los encargados de registrar, validar y realizar transacciones dentro de la tecnología Blockchain.

Ximena Campaña y Washington Zumba, presentan la tesis “Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo”, en la cual demuestran una comparativa exhaustiva de la mayoría de los protocolos que se usan actualmente, muchos de ellos usados en las criptomonedas más populares, además, las principales propiedades de estas que se consideran esenciales para el funcionamiento. Dentro de este ámbito se involucra la aplicabilidad y eficiencia en como logran resolver los grandes retos dentro de las diferentes blockchain como son la seguridad y la escalabilidad, y presentan cierta ponderación dependiendo de cómo se comporte el protocolo frente a estos desafíos para poder presentar a los más eficientes actualmente. Este proyecto presenta una enorme guía a la hora de evaluar cuál de las criptodivisas se usará a futuro. (Campaña Iza & Zumba Sampedro, 2020)

Tabla 3.

Trabajos nacionales sobre Factibilidad de Minería de Criptodivisas

Referencia	Tema	Objetivo	Herramientas
(Orrala Cajas & Chompol Pincay, 2017)	Análisis de las ventajas del uso del bitcoin en el ecuador como una criptomoneda alternativa a las transacciones comerciales	Informar a la población ecuatoriana sobre las alternativas digitales de intercambio monetario, referencia a minería en Raspberry Pi	Raspberry Pi, Software minero
(Caizapanta, Borja, & González, 2018)	Desarrollo de las criptomonedas en Ecuador, responsabilidad y riesgo	Analizar el nivel de aceptación actual de las criptodivisas en el país, y el impacto a futuro	Creada y desarrollada por el autor
(Campaña Iza & Zumba Sampedro, 2020)	Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo	Analizar los diferentes métodos de consenso y presentar las alternativas más eficientes	Creada y desarrollada por el autor

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

2.2. Fundamentación Teórica

2.2.1. 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. (Flamur, Olivera, & Emilija, 2017)

Desde el punto de vista de Lansky (2018), 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.

Hoy en día existen un sinnúmero de criptomonedas, que funcionan bajo los principios fundamentales anteriormente expuestos, pero ejecutados de diferentes formas que los hacen únicos frente a los demás, además, comparten el principio de la minería como forma de forma para poner en circulación nuevas unidades de criptomonedas en forma de compensación como recompensa de prestar el poder de cómputo de la computadora del usuario y la validación de las

transacciones. La escritura de las transacciones se hace en una cadena de bloques llamada “Blockchain”, de esta forma se puede observar los principios fundamentales de las criptomonedas donde existen diversas formas de lograr un mismo fin, lo cual aumenta la diversidad de formas en que puede funcionar una criptodivisa.

2.2.2. 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.” (Buzzi, Cittadini, & De Oliveira, 2018)

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. (Alikkal, C.G, Gopakumar, & Shahil, 2019)

2.2.3. Cadena de bloques o blockchain

“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.” (Romero, 2020)

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.

Según Amores Martinez (2020), la blockchain está basada en las redes P2P, con los principios fundamentales en ser descentralizada y distribuida, formada por un gran número de nodos que intercambian información entre sí, en este caso las diferentes transacciones que se efectúan en la red. El siguiente paso es guardar la información en los bloques, los cuales para ser creados e insertados en la cadena deben pasar por un consenso entre los nodos que conforman la red, este consenso se realiza mediante un algoritmo que se define en la misma creación de la red. Cuando la información se ha registrado dentro de la cadena de bloques es técnicamente inmutable debido a que lleva consigo un código criptográfico que se une a la información del bloque.

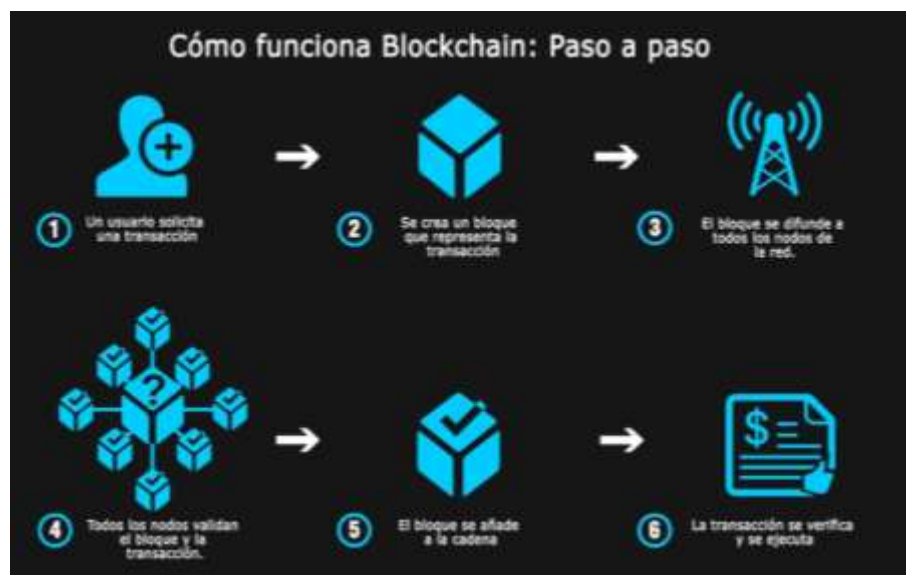


Figura 1. Como funciona una blockchain. Información tomada de 101blockchains.com. Elaborado por Nelson Rodríguez

2.2.3.1. Cadena de bloques pública

Una blockchain publica se define como una red a la que puede acceder cualquier usuario, además de permitírsele la creación de bloques, tener participación en el proceso de consenso o validación. Una de las características principales de este tipo de blockchain es que se las considera totalmente descentralizada. Otra definición muy extendida es que son redes en la cual la información es publica, pero con los matices de que las transacciones están protegidas ya que no se puede saber quiénes son los participantes por el proceso de encriptación por criptografía. (Preukschat, Kuchkovsky, Gómez Lardies, Díez García, & Molero, 2017)

2.2.3.2. Cadena de bloques privada

Una blockchain privada solo permite que los usuarios autorizados o con los privilegios adecuados puedan obtener información de la cadena, o en ciertos caso participar en el proceso de consenso o validación. Este tipo de cadenas son usadas para usos internos privados donde es indispensable que la información se mantenga dentro de la empresa. (Preukschat, Kuchkovsky, Gómez Lardies, Díez García, & Molero, 2017)

2.2.3.3. Cadena de bloque de consorcio

Una blockchain de consorcio es una cadena en la cual el proceso de consenso se maneja por un grupo de nodos que fueron preseleccionados, es decir se debe tener la aprobación de estos nodos elegidos para que los nuevos bloques y transacciones sean agrupadas a la cadena, se puede definir este tipo de cadenas como semi-descentralizadas.

2.2.4. Red Peer-to-Peer

Una red peer to peer es una red informática que funciona entre iguales, es decir no como el modelo tradicional TCP/IP con servidores y clientes, aquí todos los clientes o nodos se comportan como clientes y servidores de forma paralela. De esta forma permite compartir, interactuar e intercambiar información sin necesidad de intervención de terceros, ya que todos los usuarios ya sean personas, dispositivo o entidad funcionan como nodos. (Gallardo, Gutiérrez, & Fuentes, 2008)

“Este concepto hace referencia a un sistema de transmisión de datos en red que basa su funcionamiento en un sistema sin jerarquías donde todas las máquinas son a la vez clientes y servidores. Todos los dispositivos y usuarios integrantes de una red P2P pueden comunicarse directamente entre sí sin la obligación de circular a través de un servidor. Este modelo cuenta con la ventaja de ser complementario, y no excluyente, del modelo cliente/servidor. Su implementación masiva se da sobre redes Ip, constituyéndose en redes virtuales que funcionan sobre la infraestructura técnica de internet, pero singularizadas porque la búsqueda de la información no se realiza en función de la ubicación del recurso sino de su descripción” (Pérez-Subías, 2003)



Figura 2. Estructura de una red peer to peer. Información tomada de diccionarioactual.com. Elaborado por diccionarioactual.com

2.2.5. Algoritmos de consenso

Según la REAL ACADEMIA ESPAÑOLA (2001), consenso es un acuerdo que se produce al obtener el consentimiento de todos los integrantes de un conjunto de individuos es decir un grupo o varios grupos, la parte fundamental del término se define como “Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema” con estas definiciones se puede entender mejor el significado de algoritmo de consenso, que según Amores Martínez (2020), son “las normas establecidas para llegar a acuerdos y así evitar discrepancias a pesar de poder existir intermediarios que quieran generar problemas en la toma de decisiones”.

De la forma en la cual se define a las criptomonedas, existen diferentes formas de cumplir con los principios fundamentales, y los algoritmos de consenso son la herramienta precisa para la toma de decisiones, ya que al ser un sistema descentralizado se debe buscar una forma de mantener un orden, y este se definió llevando al consenso a todos los nodos de la red mediante los diferentes algoritmos, que se definirán a continuación.

2.2.5.1. Prueba de trabajo o Proof of work (PoW)

El algoritmo de Prueba de trabajo fue con el que se inició la blockchain en este caso bitcoin y el funcionamiento está dada bajo el concepto de solicitar un trabajo a los usuarios, que luego se verifica mediante la red. El concepto más claro de los primeros trabajos que mencionan este algoritmo indica que “Este es un protocolo en cual un comprobante demuestra a un verificador que ha gastado un cierto nivel de esfuerzo computacional en un intervalo de tiempo específico. Aunque no se definieron como tales ni se trataron formalmente, las pruebas de trabajo se han propuesto como un mecanismo para varios objetivos de seguridad, incluida la medición del acceso al servidor, la construcción de cápsulas de tiempo digitales y la protección contra el envío de correo no deseado y otros ataques de denegación de servicio”. (Jakobsson & Juels, 1999)

Satoshi Nakamoto, quien fundamento bitcoin propuso la prueba de trabajo para gestionar las diferentes transacciones de la red bitcoin, la mayor ventaja era prevenir el doble gasto que podría

ocurrir en la red bitcoin. Según Nakamoto (2008), el proceso de prueba de trabajo se puede definir en los siguientes puntos:

- El nodo o usuario constituye un enlace con la red. Luego la red otorga un trabajo o labor computacional de complejidad elevada, y por consiguiente esta labor debe ser solucionada para que el nodo o usuario obtenga una recompensa económica.
- A continuación, se procede a descifrar el acertijo, lo cual implica el uso elevado de potencia computacional para lograr solventar el acertijo otorgado, este procedimiento es el denominado minería en este caso de criptomonedas.
- Cuando la labor computacional ha sido resuelta, el nodo o usuario distribuye esta información con la red para que pueda ser verificada, una vez en esta sección del proceso se constata que la labor satisface los requisitos que se solicitaban. En caso de que satisfaga lo anteriormente dicho se otorga apertura a los recursos de la red, en caso de ser negativa la verificación se deniega el acceso, luego de esta verificación además se procede a examinar los protocolos de doble gasto.

Una vez que se ha verificado que la labor se ha realizado de forma correcta, el nodo o usuario puede alcanzar la recompensa por la potencia computacional prestada.

El algoritmo prueba de trabajo presenta un elevado nivel de complejidad ya que cada vez que crece la cadena de la misma forma la dificultad del cálculo hash, este sistema puede estar expuesto a ataques de hasta el 50%, ya que una vez que la red sea corrompida más de ese porcentaje el atacante romperá el principio fundamental de descentralización de la blockchain, pero un ataque de esta magnitud es técnicamente imposible ya que debería controlar la mitad de todos los ordenadores que prestan el poder computacional para la minería del activo, sea este bitcoin o alguna de las varias criptomonedas que hoy en día usan este algoritmo de consenso. (Nakamoto, 2008)



Figura 3. Prueba de Trabajo. Información tomada de 101blockchains.com. Elaborado por Nelson Rodríguez

Algunas de las principales desventajas de este algoritmo es que a medida que crece la red, el nivel de dificultad aumenta y demanda un poder computacional mayor, lo cual no la hace adecuada para redes de crecimiento inmediato. Del artículo “Comparative Analysis of Blockchain Consensus Algorithms” de Bach, Mihaljevic, & Zagar (2018), se destacan las ventajas y desventajas más importantes de este algoritmo:

- Ventajas:
 - El algoritmo presenta un nivel elevado de seguridad, en especial si la red se forma de varios miles de nodos o usuarios, además el algoritmo presenta nivel de seguridad directamente proporcional al número de usuarios es decir más usuarios mayor seguridad, por la capacidad computacional para corromper el consenso seria técnicamente imposible de manejarse de forma independiente.
 - El algoritmo presenta facilidad de implementación, ya que los softwares presentan un fácil mantenimiento, así como los procesos.

- Se puede acoplar de forma sencilla a diferentes hardware, con potencias mínimas hasta equipos de potencia elevada.
- Presenta una alta resistencia a los ataques más comunes como son los de denegación de servicios (DDoS)
- Desventajas:
 - El algoritmo en redes con grandes cantidades de usuarios o nodos consumen grandes cantidades de energía, debido a la demanda de hardware de gran consumo.
 - Presenta una tendencia a la centralización para equipos especializados o de alta potencia.

2.2.5.2. Prueba de participación o Proof of Stake (PoS)

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, en base al 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” (Amores Martinez, 2020). 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 base 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. Algunos de los criterios a tener en cuenta son la cantidad de activo reservado que presente el usuario o el tiempo que se encuentra activo en la red, una vez que se han elegido a los validadores, los escogidos podrán proceder a validar las distintas transacciones o crear nuevos bloques. Según King & Nadal (2012), las ventajas y desventajas de la prueba de participación son:

- Ventajas:

- Este método de consenso es más amigable con el medioambiente, ya que no es necesario hardware potente y de alto consumo para ejecutar la minería, por lo cual presenta un consumo energético menor.
- Presenta de forma más clara las recompensas para los integrantes de la red, de esta forma los usuarios o nodos se comprometen a que la red perdure en el tiempo.
- El nivel de descentralización es más amplio, debido a que todos los usuarios o nodos pueden participar con la respectiva cuota de participación. Evitando la consolidación de poder en pocos usuarios con capacidad computacional elevada.
- Mayor capacidad de escalabilidad, ya que el sistema no demanda ningún poder computacional elevado para resolver problemas, si no el compromiso con la red.
- Nivel de seguridad alto, debido a que puede superar problemas de otros métodos de consenso.
- Desventajas:
 - Las credenciales de los usuarios o nodos deben ser verificadas por lo cual el anonimato es menor en este tipo de redes.
 - Debido a que los sistemas de prueba de trabajo deben estar permanentemente conectados a internet, se puede presentar ataques directo a los usuarios, por eso es recomendado usar contraseñas robustas.

Una blockchain que usa prueba de trabajo necesita de un ataque que tome más del 51% de la red para poder tener el consenso de la red, pero en la prueba de participación aun con ataque de ese nivel no sería suficiente para lograrlo debido a que la antigüedad de la moneda es un factor fundamental.

“Este diseño alivia algunas de las preocupaciones de la suposición del 51% de Bitcoin, donde el sistema solo se considera seguro cuando los buenos nodos controlan al menos el 51% de la red o el poder minero. Primero, el costo de controlar una participación significativa podría ser mayor que el costo de adquirir un poder minero significativo, aumentando así el costo de ataque para tan poderosas entidades. Además, la edad de la moneda del atacante se consume durante

el ataque, lo que puede hacer más difícil para el atacante continuar impidiendo que las transacciones ingresen a la cadena”. (King & Nadal, 2012)



Figura 4. Prueba de Participación. Información tomada de 101blockchains.com. Elaborado por Nelson Rodríguez.

2.2.5.3. Prueba de participación delegada o Delegated Proof of Stake (DPoS)

“Este algoritmo propuesto para mejorar la seguridad de PoS, donde la elección de productores de bloque o testigos (auditores) depende de los votos de las partes interesadas. Esto proporciona el beneficio del control semi-central de la red brindando eficiencia y velocidad manteniendo las características de descentralización. El testigo creará nuevos bloques uno por uno, luego obtiene algunas recompensas. Si un testigo no puede crear un nuevo bloque dentro de un tiempo específico, las partes interesadas votarán pues un nuevo testigo al que se le asignará la misión”. (Alsunaidi & Alhaidari, 2019)

La prueba de participación delegada presenta un mecanismo para que los usuarios o nodos de la red, eligen dependiendo de la participación en la red, propuestas o tiempo de antigüedad a los delegados, que serán los encargados de validar los bloques y a la vez recibirán una recompensa, este algoritmo al igual que la prueba de participación no presenta trabajo

computacional elevado, en cambio, cuenta con un nivel de confianza en usuarios o nodos destacados. Es común que este tipo de redes se sometan a votación por cuestiones fundamentales de la red como políticas, recompensas y demás cuestiones importantes por lo que se le conoce como democracia digital. Según Alsunaidi & Alhaidari (2019), el proceso que compone la prueba de participación delegada es el siguiente:

- El comienzo del proceso inicia con la elección de delegados, el cual se cumple mediante un sistema de voto en tiempo real, de esta forma existe confianza en los usuarios o nodos elegidos. Un punto importante que toman en cuenta los usuarios es la cantidad de activo que tienen los usuarios a los que votan, lo cual brinda mayores oportunidades de ser elegido.
- Acto seguido luego de la votación y elección de delegados, ocurre la creación de bloques en este proceso los elegidos tienen la labor de agregar nuevos bloques a la cadena de bloques, cada uno de los delegados elegidos tiene la capacidad de crear un bloque y luego dar paso al siguiente delegado.
- En la parte final del proceso se evalúa el comportamiento de los delegados, y en caso de ser necesario se puede vetar de futuros procesos o expulsarlo definitivamente de la red, de esta forma se regule la red

Este algoritmo presenta respuestas a varios fallos y desafíos por eso a continuación, se describen las ventajas y desventajas que se mencionan en el análisis de Bach, Mihaljevic, & Zagar (2018):

- Ventajas:
 - Mayor capacidad de escalabilidad, ya que el sistema no demanda ningún poder computacional elevado para resolver problemas, si no el compromiso con la red.
 - El proceso de elección de delegados se ejecuta de manera eficiente, y elige a los encargados de producir los nuevos bloques.
 - La labor de que la red obtenga un nivel de seguridad elevado es menor, debido a que los equipos de gran potencia no son requeridos.
 - Mayor capacidad de escalabilidad, ya que el sistema no demanda ningún poder computacional elevado para resolver problemas, si no el compromiso con la red.

- Desventajas:
 - Este algoritmo al necesitar de una comunidad comprometida y dedicada con la red, el éxito dependerá del compromiso de los nodos o usuarios.
 - Las credenciales de los usuarios o nodos deben ser verificadas por lo cual el anonimato es menor en este tipo de redes.
 - Usuarios con mayor número de activos tienden a ser los elegidos como delegados presentando cierta centralización.

2.2.5.4. Prueba de actividad o Proof of Activity (PoA)

La prueba de actividad presenta un esquema en el cual combina características de prueba de trabajo y prueba de participación, fue desarrollado por “International Association for Cryptologic Research” como respuesta a diferentes falencias de el algoritmo prueba de trabajo, el proceso es el presentar cierto problema que demande poder computacional para que el usuario o nodo que primero lo resuelva, pero en este caso los mineros únicamente obtienen plantilla del bloque que está compuesta por la información del encabezado y la dirección de la recompensa que se le otorgara al minero, es decir crean el bloque sin transacciones. (Seth S. , 2021)

Una vez que este proceso finalice se pasa a un proceso parecido al de prueba de participación en el cual, ciertos nodos o usuarios elegidos de forma aleatoria, que dependiendo del tiempo en la red y cantidad de activo que tengan tendrán mayores posibilidades realizaran un proceso de verificación de la plantilla del bloque y luego de la misma forma comenzaran a agregar las transacciones.

Finalmente, luego de este proceso el bloque es enviado la red, y la compensación por la creación, validación del bloque y las transacciones se dividirán entre los usuarios o nodos que participaron en ambas labores. De esta forma este algoritmo toma características y eleva las mayores fortalezas recompensando tanto a los mineros como a los validadores por el aporte realizado, según SETH (2021), estas son las ventajas y desventajas del algoritmo:

- Ventajas:
 - Alta resistencia a ataques de denegación de servicios, y los ataques del más del 51%.

- Este algoritmo otorga la compensación a ambos tipos de usuarios lo que prestaron el poder de cómputo y los que participaron agregando las transacciones.
- Difícil de monopolizar ya que requeriría un ataque de poder computacional enorme y además un número de activo muy alto.
- Desventajas:
 - Igual que en uno de los algoritmos de los que procede, el algoritmo de actividad no es amigable con el ambiente, al hacer uso de minería tradicional que necesita equipos de cómputo de alto consumo.

2.2.5.5. Prueba de quemado o Proof of Burn (PoB)

El algoritmo de prueba de quemado presenta una alternativa peculiar de llegar al consenso en diferencia a los métodos tradicionales de minado, en este sistema los usuarios o nodos consiguen la capacidad de minar en base a la cantidad de activo que se ha gastado en otras palabras quemado. Este algoritmo fue creado por Iain Stewart en diciembre de 2012 y la idea inicial fue que los mineros que quemaran las monedas obtendrían la capacidad para minar el activo, por ende, entre más activos el usuario queme más probabilidades tiene de crear nuevos bloques. A continuación, se presentan el proceso que compone la prueba de quemado:

- Para comenzar el proceso del protocolo de quemado se debe enviar a una dirección pública y verificable, proporcionada por la red a la cual enviarán los activos esta dirección es conocida como eater addresses, cabe recalcar que una vez enviados los activos no se puede recuperar, de esta forma los nodos o usuarios demuestran el compromiso con la red al invertir en la misma cadena de bloques. (Bonneau & Heninger, 2020)
- Acto seguido luego de la quema el usuario estará en la lista de elegidos para comenzar a minar, un proceso sencillo que otorga grandes prestaciones, debido a que desprenderse de los propios activos no es algo fácil, esto provoca que los usuarios que lo hacen tengan gran confianza en la red. (Bonneau & Heninger, 2020)

Además, Bonneau & Heninger (2020), especifican las ventajas y desventajas del algoritmo:

- Ventajas:

- Este método de consenso es más amigable con el medioambiente, ya que no es necesario hardware potente y de alto consumo para ejecutar la minería, por lo cual presenta un consumo energético menor.
- Este algoritmo proporciona una elevada estabilidad a los usuarios, al estimular a los usuarios a reinvertir activos en la misma red, y a la vez elevando la seguridad.
- Desventajas:
 - Peligro de que la red pierda la descentralización, si los usuarios con mayor cantidad de activos son lo que siempre realizan el quemado.
 - A pesar de no demandar equipos de cómputo que consuman altas cantidades de energía, las monedas que se quemen podrían provenir de intercambios con otras que si haciendo a la minería poco amigable con el ambiente.

2.2.5.6. Prueba de capacidad o Proof of Capacity (PoC)

El algoritmo de prueba de capacidad basado en el principio de almacenar información, en la mayoría dispositivos de almacenamiento convencionales, discos duro o de estado sólido. En el cual se almacenan partes importantes del nodo entre las cuales posibles respuestas a problemas de la red, por ende, a mayor capacidad para almacenar información mayor es la posibilidad de poder resolverlo. En este sistema el equipo minador debe poner a disposición la capacidad de cómputo, además, la capacidad de almacenamiento tiende a producir bloques de forma más rápida que algoritmos conocidos. (Hayes, 2021)

Se detalla las ventajas y desventajas:

- Ventajas:
 - Este método de consenso presenta una reducción considerable de desperdicios de recursos energéticos, a pesar de que consumo no tiende al mínimo como otros el considerablemente bajo en comparación a la prueba de trabajo.
 - Los dispositivos de almacenamiento pueden ser utilizados de forma repetida.
- Desventajas:
 - Peligro de ataques desconocidos, debido a que es un algoritmo muy poco difundido a la fecha.

2.2.5.7. Prueba de tiempo transcurrido o Proof of Elapsed Time (PoET)

El algoritmo de prueba de tiempo transcurrido es una forma muy llamativa de abordar el consenso, debido a que presenta una verdadera igualdad de condiciones entre todos los nodos o usuarios, además, es un algoritmo que no es probable verla en el mundo de criptomonedas, por que presenta una peculiaridad la cual es que todos los usuarios que quieran participar en la red deberán ser verificados y autorizados, es decir se usa para redes permissionadas. Fue creado por Intel en el año 2016 y presenta un principio en el cual se elige de forma aleatoria al nodo o usuario que procederá a crear un nuevo bloque, la diferencia con otros algoritmos es que aquí todos tienen las mismas posibilidades de ser elegidos para minar el bloque, de esta forma este algoritmo presenta una forma más justa de lograr minar un bloque, sin tener en cuenta la cantidad de activo, poder computacional o antigüedad en la red. (Chen, Xu, Shah, Gao, & Lu, 2017)

El principio de funcionamiento de este algoritmo otorga a los usuarios un denominado objeto de tiempo, el cual se puede describir como un cronometro con cierta cantidad de tiempo hacia atrás es decir una cuenta regresiva que, una vez terminado ese tiempo, emite una alarma de activación al usuario avisando que, al momento de volver a la actividad, se convierte en un generador de bloques. Este tipo de aleatoriedad se consigue con un nuevo algoritmo de generación de numero aleatorio de Intel llamado RDRAND el cual produce números aleatorios en forma muy veloz utilizando la entropía que se produce en los procesadores de la marca. (Chen, Xu, Shah, Gao, & Lu, 2017)

Una vez que el usuario obtiene el objeto de tiempo y además ha sido verificado de forma correcta este procede a agregar las diferentes transacciones al bloque, además debe producir un hash con el bloque y enviarlo a la red para que sea aceptado. Este hash no debe usar la denominada prueba de trabajo, si no uno cualquiera asociado a la información.

Según Chen, Xu, Shah, Gao, & Lu (2017), las diferentes ventajas y desventajas del algoritmo son:

- Ventajas:
 - Presenta una gran capacidad de escalabilidad, debido a la eficiencia en redes de alta capacidad.

- Disminución de consumo energético, al no depender de equipos computacionales de alto consumo.
- Algoritmo especialmente diseñado para redes privadas.
- Desventajas:
 - Las redes que usan este algoritmo están obligadas a llevar un control de los usuarios por lo cual no existe el anonimato.
 - Se podrían utilizar debilidades de los procesadores Intel para ejercer ataques a este tipo de redes.

2.2.5.8. Prueba de asignación o Proof of Assignment (PoA)

El algoritmo de prueba de asignación plantea un proceso de consenso mediante herramientas criptográficas, que usa características de otros algoritmos como prueba de trabajo y prueba de almacenamiento, pero con consumo energético menor y que puede usarse en equipos con prestaciones modestas. La idea fundamental de este algoritmo es el de usar diferentes dispositivos (IoT) que en la mayoría presentan consumo energético diminuto, para ejecutar diferentes procesos de encriptación, y también de minería en escala mínima. (Seth, 2021)

Esta idea nace de la alta demanda de equipos (IoT) como porteros, cámaras, asistentes, y muchos más que en la actualidad incluyen procesadores, estos se encuentran en los diferentes hogares, empresas, y sitios públicos con acceso a internet, lo cual abre una ventana de posibilidades muy grande. Este algoritmo aprovecha esta capacidad de interconexión para delegar pequeñas tareas de micro minado a cada de los dispositivos de la red del usuario y ponerlos a disposición de este. (Seth S. , 2021)

- Ventajas:
 - Consumo energético mínimo, ya que se ejecuta en equipos con prestaciones modestas.
 - Libertad de que el usuario puede elegir en qué momento los dispositivos ejecuten la minería.
- Desventajas:
 - Los equipos mencionados presentan un poder computacional limitado.

2.2.5.9. Algoritmo de consenso del protocolo Ripple (RPCA)

El algoritmo de consenso del protocolo ripple como el nombre lo indica es un protocolo exclusivo de la criptomoneda llamada ripple, la cual a diferencia de la mayoría de las criptomonedas que usan la tecnología blockchain, esta usa una tecnología denominada de ledger distribuido y este algoritmo anteriormente mencionado como método de consenso entre los usuarios, de esta forma el sistema de ripple tiene la capacidad de procesar y validar transacciones en servidores propios. (Chase & MacBrough, 2018)

La totalidad de las empresas que usan el sistema ripple son bancos que manejan un propio nodo, el cual presenta un alto nivel de centralización ya que cada usuario administra de forma independiente el servidor establecido, el proceso del algoritmo comienza cuando cada uno de los nodos o usuarios toma las transacciones como válidas. A continuación, se reúnen una cantidad de transacciones de cada uno de los servidores y se somete a una votación sobre la confianza, en este punto las transacciones que obtengan una votación mínima establecida pasaran y así de forma simultánea, si una de las transacciones no alcanza el mínimo será descartada. El porcentaje con el cual se aprueba una transacción es de mínimo 80% una vez que obtengan este número de votos esta transacción se agrega al ledger distribuido. (Chase & MacBrough, 2018)

Dentro del documento de creación de Ripple Chase & MacBrough (2018), mencionan las ventajas del algoritmo y se identificara sus desventajas:

- Ventajas:
 - Bajo consumo energético, ya que los servidores mantienen una conexión mínima entre si ahorrando recursos.
 - Posibilidad de escalabilidad a gran escala, dependiendo de la capacidad monetaria de la empresa.
- Desventajas:
 - Es un sistema con una tendencia a la centralización, al requerir que los nodos cuenten con servidor propio.
 - Es una red sin anonimato, los usuarios deben verificarse.

2.2.5.10. Prueba de Autoridad o Proof of Authority (PoA)

La prueba de autoridad presenta un consenso basado en la confianza de la reputación de ciertos nodos o usuarios, la forma inicial para lograr esta confianza es que esta prueba de consenso requiere identidades reales verificadas para poder ingresar al blockchain. Estos usuarios que presentan las credenciales se denominan validadores, y entran en un proceso que de forma aleatoria elige al usuario que validara cada bloque. Uno de los puntos fundamentales es que la cantidad de estos usuarios habilitados para validar las transacciones son limitados, esto ofrece una mejora sustancial en la velocidad a la hora de verificar las transacciones ya que con un número limitado de usuarios la aleatoriedad se logra de forma más sencilla. El siguiente paso para llegar a ser un validador luego de verificar las credenciales, es el de postularse a este título, elegido igualmente por otros usuarios verificados evitando que dentro de la red existan usuarios corruptos, una vez que se es elegido por los demás usuarios el validador puede verificar un bloque de un conjunto. (Valente, 2019)

Este tipo de métodos de consenso usan una característica de gran alcance como es la reputación frente a los demás, una vez que los usuarios saben quién es el responsable de cada acción dentro de la red proceden a cuidar de forma minuciosa los movimientos y de la misma forma preocupándose de cómo actúan los demás, para mantener una red confiable y robusta. (Valente, 2019)

Ventajas:

- Bajo consumo energético, los validadores no necesitan equipos de altas prestaciones para realizar la validación.
- La verificación de los usuarios entrega un nivel confianza muy alto entre los usuarios de la red.

Desventajas:

- Es un sistema con una tendencia a la centralización, ya que solo una parte de los usuarios validan las transacciones.
- Posibles ataques de usuarios maliciosos mediante claves o maquinas corruptas.

2.2.6. Criptografía

Una de las características de los sistemas computacionales actuales es la seguridad y la criptografía es la parte fundamental detrás de todos estos avances en seguridad informática.

“La criptografía es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: criptografía y criptoanálisis. La criptografía se ocupa del diseño de procedimientos para cifrar; es decir, para enmascarar una determinada información de carácter confidencial. El criptoanálisis se ocupa de romper esos procedimientos para así recuperar la información. Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado el criptoanálisis correspondiente” (Sanjuan, 2012). En resumen, la criptografía es la disciplina que se encarga de cifrar cierta información para que solo pueda ser accedida por las personas autorizadas.

“La criptografía es definida como la ciencia (anteriormente considerada como arte) encargada del estudio de la codificación (encripta-miento u ocultamiento) de la información con el fin de que ningún usuario, salvo el propietario o aquel que haya sido autorizado, pueda decodificarla (desencriptarla) mediante el uso de una clave que únicamente él conoce”. (Vélez Martínez, 2017)

Según Sanjuan (2012), la criptografía presenta 3 propósitos fundamentales que son:

- Mantener la confiabilidad de la información enviada, por ende, que la información solo sea visible a los usuarios con el acceso.
- Respalidar las identidades de los destinatarios, tener plena seguridad en la identidad tanto del emisor como del receptor.
- Respalidar la integridad del mensaje, que la información que entrego el emisor sea la misma que recibe el receptor.

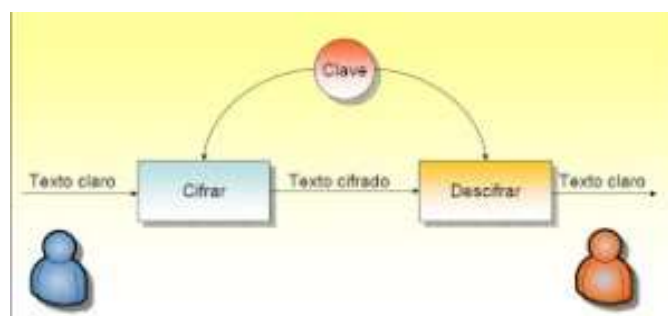


Figura 5. Proceso criptográfico. Información tomada de infosegur.com. Elaborado por infosegur

Dependiendo del tipo de clave que un sistema criptográfico use se puede dividir en:

2.2.6.1. Clave única o métodos simétricos

Es el sistema criptográfico de mayor antigüedad, pero hoy en día aun ofrece niveles de seguridad elevados. La base del funcionamiento está basada en una única clave secreta que se usa para cifrar y descifrar la información, de esta forma es necesario que todos los usuarios que vayan a utilizar este sistema tengan en el poder la clave única, es el método que se usa en la mayoría en almacenamiento de información en equipos de usuarios estándar. (Sanjuan, 2012)

Este método nace de la suposición de que la información navegara en un canal inseguro, es decir la información desde el receptor se cifra con la clave única, a continuación, avanza mediante el canal y llega al receptor el cual descifra mediante la clave única la información y obtendrá el mensaje original. Este tipo de métodos criptográficos presentan la ventaja que son mucho más rápidos en comparación con métodos asimétricos, además, están presentes en la mayoría de los equipos actuales.



Figura 6. Proceso criptográfico Simétrico. Información tomada de blog.bi-geek.com. Elaborado por Francisco Guerrero

2.2.6.2. Clave pública o métodos asimétricos

Los sistemas de claves asimétricas necesitan dos claves, en ambos extremos de la comunicación, es decir emisor y receptor cada uno contara con una clave privada y una pública. De esta forma cada usuario obtendrá una clave privada la cual deberá guardar de forma segura y una clave publica para todos los demás usuarios, este tipo de claves se encuentran relacionadas una con otra, pero configuradas de tal forma que es imposible de llegar a una con la otra sin las claves correspondientes. (Sanjuan, 2012)

El principio básico de este tipo de sistema criptográfico se presenta cuando el emisor quiere enviar un mensaje al receptor, el emisor conoce la clave pública del receptor con la cual encriptara el mensaje, la clave publica está a disposición de todo el sistema, pero la privada solo

la tiene el receptor elegido, una vez que el mensaje llegue solo podrá ser descifrado con la clave privada del receptor, de esta forma se cumple el ciclo de envío.



Figura 7. Proceso criptográfico Asimétrico. Información tomada de blog.bi-geek.com. Elaborado por Francisco Guerrero

2.2.7. Sistemas criptográficos hash

Los sistemas criptográficos hash también denominados huellas digitales son algoritmos matemáticos que modifican un mensaje y proporcionan una nueva serie de caracteres, pueden ser de longitud variable o fija. Si el sistema hash es de longitud fija a pesar del tamaño del mensaje que se ingrese el sistema proporcionara siempre un hash de la misma longitud, este tipo de sistemas se crearon con el fin de proteger información valiosa como contraseñas, patrones, frases de seguridad, etc. El funcionamiento permite que este tipo de información sensible nunca se guarde en texto plano, es decir el servidor, base de datos nunca cuenta con la clave, en cambio guarda el hash. Una vez que el usuario ingresa la clave esta se ingresa esta se prueba con el mismo sistema criptográfico, y si el hash coincide se da el acceso al usuario, cabe recalcar que es técnicamente imposible volver desde el hash hasta la cadena de caracteres asociada a este, por eso este sistema se encuentra tan difundido dentro de los sistemas de seguridad. Además, los sistemas hash se usan para proteger la integridad de mensajes, de la misma forma verificando que los hashes del mensaje enviado coincidan con los del recibido asegurando la veracidad. (López, 2021)

Según Sanjuan (2012), los sistemas criptográficos hash presentan estas características:

- Unidireccionalidad, esto significa que el poder de procesamiento para obtener la información desde el hash debe ser descomunal, en otras palabras, imposible de procesar.
- Compresión, sin importar la longitud del mensaje, el hash obtenido debe ser de una longitud fija, dependiendo del mensaje suele ser mucho menor.

- Coherente, es decir la entrada el mensaje original, producirá el mismo resultado mensaje original.
- Facilidad de cálculo, el algoritmo hash debe ser de cálculo sencillo.
- Único, no puede existir dos mensajes que produzcan el mismo hash.
- Difusión, debe ser una función compleja que contenga los bits del mensaje.

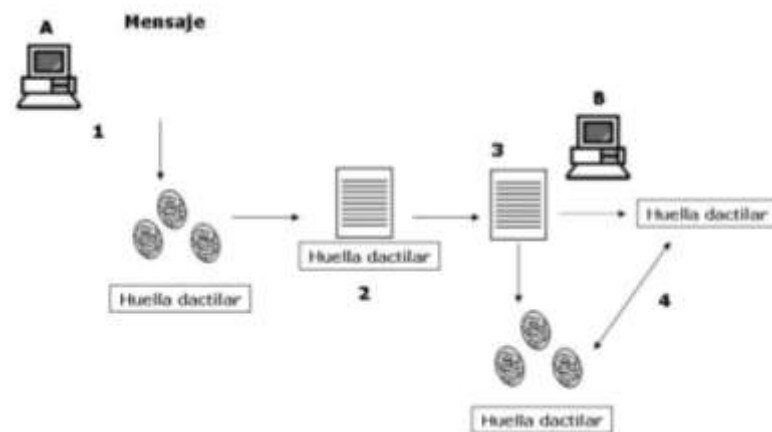


Figura 8. Proceso Sistema criptográfico hash. Información tomada de uninorte.edu.com. Elaborado por Leudis Sanjuan

Los diferentes proyectos que usan la cadena de bloques utilizan este tipo de sistemas criptográficos para mantener niveles de seguridad altos, proteger los datos de los usuarios y evitar distintos ataques a la red. Dentro del universo de las criptomonedas la minería, tiene como fin encontrar un hash con el cual firmar el bloque que se está validando, al cual se le piden ciertos requisitos dependiendo del método de consenso que se esté usando, esto es lo que demanda altos niveles de procesamiento en métodos de consenso como prueba de trabajo y otros, sin embargo en métodos que no demandan alto poder computacional solo se necesita un hash cualquiera, debido a que la dificultad de procesar estos algoritmos varían dependiendo del hardware que se use y del tipo, se nombra a continuación los principales usados en la minería y las características:

2.2.7.1. Secure Hash Algorithm SHA-256

El algoritmo Secure Hash Algorithm abreviado como SHA-256 debido a que la longitud es de 256 bits es decir 32 bytes, este algoritmo fue desarrollado por la NSA (National Security Agency) y otras agencias gubernamentales de Estados Unidos, el funcionamiento unidireccional permite producir hashes o huellas dactilares digitales únicos de cualquier tipo de información,

pero es técnicamente imposible obtener la información original del hash. Una de las características de este algoritmo es que la longitud de la cadena de caracteres del hash está definida, sin importar el tamaño de la información o archivo que se firmó con el hash siempre producirá una cadena de letras y números de 64 caracteres, codificada en 256 bits. (López, 2021)

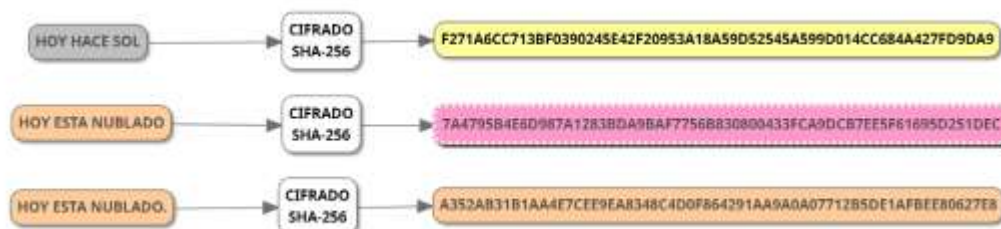


Figura 9. Algoritmo SHA-256. Información tomada de *academy.bit2me.com*. Elaborado por *bit2me*

Este algoritmo está difundido de forma amplia dentro del mundo de las criptodivisas y las cadenas de bloques, debido a que es con la que funciona la de mayor impacto global como es el bitcoin, el cual la usa desde que fue creado en el año 2008. Bitcoin utiliza este algoritmo tanto en el proceso de minería al solicitar un hash con características específicas para ser elegido para verificar un bloque, y firmar este bloque con el mismo hash producido, debido a esto es que la minería de bitcoin se ha convertido en una competencia de poder de procesamiento, por que entre más hardware el usuario tenga el poder más rápido se llegará al hash solicitado y podrá cobrar la recompensa. (López, 2021)

Además, dentro de la cadena de bloques de bitcoin se utiliza este algoritmo para generar las direcciones de billetera de los usuarios es decir el espacio donde se guarda la información del usuario y los activos. El algoritmo SHA-256 presenta grandes ventajas como altos niveles de seguridad y gran adaptabilidad a ser producido por cualquier tipo de hardware, esto a la vez a dado lugar a hardware especializado para minar las criptomonedas que lo usan, creando una desventaja al relegar a equipos de hardware modesto que no cuentan con potencia computacional elevada. A continuación, se muestra las principales criptomonedas que usan este algoritmo en la red:

Tabla 4.

Principales criptodivisas que usan el algoritmo SHA-256.

Criptomoneda	Precio	Acciones en circulación	Capitalización de mercado
Bitcoin (BTC)			

	\$43,914.72	18,780,337 BTC	\$823,298,273,758
Bitcoin Cash (BCH)	\$559.95	18,811,894 BCH	\$10,516,204,956
Bitcoin SV (BSV)	\$146.35	18,809,327 BSV	\$2,747,799,422
Peercoin (PPC)	\$0.9382	27,065,226 PPC	\$25,337,965

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

2.2.7.2. Ethash

El algoritmo Ethash se conoce en la mayoría por ser el que se usa en la minería y cadena de bloques de Ethereum la cual es la segunda criptomoneda de mayor impacto y valor en el presente, este algoritmo está fundamentado en un conocido algoritmo de hash llamado SHA-3, a diferencia de otros algoritmos los procesos de ethash son complejos y toman características informáticas avanzadas para elevar la seguridad. (bit2me, 2019)

Este algoritmo se basa en otros dos algoritmos los cuales le proporcionan características que necesitaban para el funcionamiento de la red, el primero es el algoritmo Dagger el cual construye una estructura masiva de datos, que ocupaba un espacio aproximado de 1 gigabyte de información en la etapa inicial pero luego de varias actualizaciones el tamaño de la información actual esta alrededor de los 4 o 5 gygabytes , sobre este conjunto de datos se ejecutan una compleja cantidad de operaciones de memoria que aportan complejidad. Sobre esta información se ejecuta el algoritmo Hashimoto que presenta una característica esencial para el funcionamiento de la red de Ethereum la resistencia a la minería ASIC, este tipo de minería se ejecuta con hardware especializado para cierto tipo de minería especifico, es decir equipos para minar una criptomoneda en concreto y son muy superiores en rendimiento en comparaciones con equipos de uso comercial, el algoritmo logra ser resistente a este tipo de minería provocando un consumo elevado de recursos a la memoria RAM, para lo cual no están preparados los equipos ASIC. (Mukhopadhyay, et al., 2016)

El funcionamiento de este algoritmo toma la información generada por el algoritmo Dagger agrega información de la red, las transacciones y produce un hash único para el bloque que se esté minando. Debido a lo antes mencionado, los sistemas que usan este algoritmo dependen de

grandes cantidades de memoria RAM para ejecutarse con soltura, esto hace que los sistemas que mejor se adaptan a la minería son las GPU debido que tienen una gran capacidad de memoria y elevada capacidad de cálculo, dificultando la minería en equipos con prestaciones modestas, además las redes que usan este algoritmo presentan un rendimiento de validación de bloques bastante fluido. (Mukhopadhyay, et al., 2016)

Cabe agregar que a pesar de que el algoritmo es resistente a la mayoría de los sistemas ASIC a partir del año 2018 existen mineros de este tipo que han disminuido la capacidad de minería de usuarios con equipos modestos. A continuación, se especifica las principales criptomonedas que usan este algoritmo en la red:

Tabla 5.

Principales criptodivisas que usan el algoritmo Ethash.

Criptomoneda	Precio	Acciones en circulación	Capitalización de mercado
Ethereum (ETH)	\$ 3,044.97	117,026,282.06 ETH	\$ 355,516,096,963
Ethereum Classic (ETC)	\$58.31	127,486,399.073 ETC	\$7,433,731,930
Metaverse Entropy (ETP)	\$0.135829	80,311,354.71 ETP	\$10,908,611
Etho Protocol (ETHO)	\$0.090997	17,378,616.8 ETHO	\$1,581,402

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

2.2.7.3. Script

El algoritmo Script nació como una búsqueda de un algoritmo de alta seguridad para Tarsnap un servicio de respaldo en la nube, y fue creado para soportar grandes ataques de fuerza bruta al requerir grandes cantidades de memoria para la ejecución. El proceso de funcionamiento de Script al igual que en la mayoría de sistemas hash, es el de producir una cadena alfanumérica irrepetible para proteger la información, pero lo que hace diferente a este algoritmo es que hace uso de un método llamado “Derivación mayor de claves mediante funciones secuenciales duras de memoria” el cual agrega ciertos parámetros de seguridad elevados, pero además agrega ruido

al algoritmo lo cual entrega un hash técnicamente imposible de descifrar mediante ataques de fuerza bruta. Este ruido en el algoritmo Script es un conjunto de números elegidos de forma pseudoaleatoria creado por el mismo algoritmo, que se guardan en la memoria RAM, y la función es la de ocultar la información clave, y de esta forma elevando la complejidad de corromper el hash. (Mukhopadhyay, et al., 2016)

El método script entrega un algoritmo con un rendimiento elevado, en relación con la cantidad de procesamiento que se invierte y la complejidad de los hashes que entrega, además el algoritmo es altamente manejable ya que muchas de las variables se pueden modificar para que requiera de uno u otro recurso que el programador requiera, además de que el proyecto es de código abierto. Las criptomonedas que usan este algoritmo en la minería y cadena de bloques presentaban alta resistencia a la minería ASIC, pero a partir de 2013 los sistemas de este tipo lograron ejecutarse en estos equipos, pero a pesar de esto el algoritmo presenta muchos inconvenientes de costo/beneficio por lo cual la minería existe, pero no es de las más demandadas mediante estos equipos. (bit2me, ¿Qué es la función hash Script?, 2020)

A continuación, se detalla las principales criptomonedas que usan este algoritmo en la red:

Tabla 6.

Principales criptodivisas que usan el algoritmo Script.

Criptomoneda	Precio	Acciones en circulación	Capitalización de mercado
Dogecoin (DOGE)	\$ 0.2339	130,771,840,468 DOGE	\$ 30,780,079,006
Litecoin (LTC)	\$147.42	66,752,615 LTC	\$ 9,852,801,242
Reddcoin (RDD)	\$0.003131	28,808,713,174 RDD	\$ 98,032,252
Infinitecoin (IFC)	\$0.0002329	90,595,753,019 IFC	\$21,140,733

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

2.2.7.4. X11

El algoritmo X11 está activo desde 2014 y fue creado por el desarrollador de la criptomoneda Dash llamado Evan Duffield el cual en busca de mejorar el nivel de seguridad del algoritmo

anterior de dash SHA-256 creo X11, la diferencia fundamental de este algoritmo es que este presenta un sistema en el cual se usan hasta 11 diferentes tipos de sistemas criptográficos hash que se utilizan en un orden predefinido, esto eleva de forma considerable la dificultad de ataques y por ende eleva la seguridad de la red. (bit2me, ¿Qué es el algoritmo de minería X11?, 2020)

El funcionamiento de este algoritmo comienza con el usuario elegido para minar el bloque, el cual generara el primer hash mediante el algoritmo BLAKE, el cual es el de mayor complejidad y a continuación pasara este hash por 10 sistemas hash más hasta obtener un hash que proporciona elevadísimo nivel de seguridad y anonimato a los usuarios, los otros algoritmos que se usan son: BMW, Groestl, JH, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, Echo. Cada uno de estos algoritmos hash presentan características de seguridad robustas y con esto aportan a que X11 sea un sistema muy confiable. La cual funciona este algoritmo proporciona que sea sencillo de procesar, ya que usa métodos seguros combinados y no un método complejo que demande alto procesamiento, además es uno de los algoritmos que menos consume energético cuesta a los usuarios. (Mukhopadhyay, et al., 2016)

Este algoritmo presenta grandes ventajas para desarrolladores ya que es posible modificar el orden de los algoritmos o cambiar por otro dependiendo de la necesidad, otra de las ventajas es que presenta un buen rendimiento en la minería con CPU y GPU, aunque la minería de equipos especializados ASIC se encuentra presente en los mismos, no representa un costo/beneficio que entregue grandes recompensas por lo cual no se encuentra muy difundido.

A continuación, se muestra las principales criptomonedas que usan este algoritmo en la red:

Tabla 7.

Principales criptodivisas que usan el algoritmo X11.

Criptomoneda	Precio	Acciones en circulación	Capitalización de mercado
Dash (DASH)	\$ 158.56	10,316,302.5 DASH	\$ 1,635,752,926
EUNO (EUNO)	\$ 0.120537	6,272,531,264.2 EUNO	\$ 756,072,101
Polis (POLIS)	\$ 0.096344	76,814,705.6 POLIS	\$ 7,400,636
Pepecoin (MEME)	\$ 466.57	850.6 MEME	\$ 396,905

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

2.2.7.5. CryptoNight

El algoritmo CryptoNight fue creado con el fin de evitar la centralización de la red, por el uso de hardware especializado, debido a esto es un algoritmo altamente eficiente en sistemas CPU es decir equipos convencionales, y no en sistemas ASIC, también presenta menor rendimiento en sistemas GPU. Este algoritmo al igual que muchos usa el método de consenso de prueba de trabajo, este presenta a diferencia de otros algoritmos una velocidad de cálculo del hash muy veloz, ofreciendo alta escalabilidad a los usuarios de la red que lo use, y un nivel de seguridad bastante elevada. (bit2me, ¿Qué es el algoritmo de minería CryptoNight?, 2019)

El sistema fue lanzado en el año 2012 con el cifrado AES, el cual tiene un elevado nivel de seguridad de uso en aplicaciones militares, y además 2 funciones hash de alto nivel llamadas Keccak y Blake-256, estas funciones juntas codifican la información en 1600 bits una cantidad considerable, en especial en comparación con el algoritmo SHA-256 que solo usa codificación de 256 bits. Una vez que se produce este hash se toma una parte de él, en específico, los primeros 31 bits y se los reserva para usarse de clave de cifrado del algoritmo AES, el cual se cifra mediante una ronda de 10 ciclos, es decir 10 procesos de cifrado independientes, al obtener esta información el algoritmo crea un hash único de 256 bits que será el que se use para firmas el bloque que se esté minando. (TUZI, 2017)

Las principales ventajas que ofrece este algoritmo es la ejecución eficiente en CPU, lo cual le entrega un consumo energético muy eficiente en comparación a otros algoritmos antes vistos, además, cuenta con un sistema de encriptación AES. Dentro de las desventajas existe una contradicción si bien la ejecución eficiente en CPU es altamente beneficiosa ha dado lugar a que se creen equipos especializados ASIC para este algoritmo, lo cual no ha repercutido de forma considerable en la minería, pero a largo plazo propone un panorama en el cual los equipos de prestaciones modestas no logren minarlo de forma eficiente. (TUZI, 2017)

A continuación, se muestra las principales criptomonedas que usan este algoritmo en la red:

Tabla 8.

Principales criptodivisas que usan el algoritmo CryptoNight.

Criptomoneda	Precio	Acciones en circulación	Capitalización de mercado
---------------------	---------------	--------------------------------	----------------------------------

Monero (XMC)	Classic	\$	16,264,665.5 XMC	\$ 5,602,852
		0.341448		
Dero (DERO)		\$ 12.96	287,546.3 DERO	\$ 3,726,601
Bytecoin (BCN)		\$	183,671,335,386.9 BCN	\$ 476,994,458
		0.002597		
PKarbo (KRB)		\$	9,137,445.4 KRB	\$ 1,134,889
		0.124202		

Información adaptada de los repositorios y artículos investigados. Elaborado por Crithian Loayza

2.2.7.6. RandomX

El algoritmo RandomX es bastante reciente en comparación con los antes mencionados, entro en funcionamiento en 2019, y debido al reciente funcionamiento presenta una característica que muchos algoritmos intentaron, pero no lograron sostener por un tiempo prolongado, RandomX está actualmente protegido contra la minería especializada ASIC, y altamente adaptado para minería en CPU. Al igual que varios algoritmos este se usa en el método de consenso de prueba de trabajo, este algoritmo desarrollado por el equipo detrás de la criptomoneda Monero, es un algoritmo probado y revisado con estándares de seguridad muy altos, y con un nivel de escalabilidad enorme. (Suárez, 2020)

El funcionamiento de este algoritmo se basa en la aleatoriedad es decir ser casi impredecible, y debido a este factor junto con la alta complejidad es difícil de minar incluso en GPU, dejando al algoritmo en exclusividad a sistemas CPU. El algoritmo presenta 2 modos de funcionamiento, uno de mayor consumo de recursos que necesita como mínimo 2 gigabytes de memoria RAM y con posibilidad de usar “Acceso no uniforme a memoria” si el procesador tiene la opción, dentro de este espacio de memoria se procesaran los datos aleatorios. El segundo modo de funcionamiento pide prestaciones más modestas como un mínimo de 256 megabytes de memoria RAM y así mismo presenta unas ganancias considerablemente inferiores en

comparación con el método anterior. El sistema utiliza criptografía de alto nivel como son las funciones hash Blake2b y además de encriptación AES. (Suárez, 2020)

La forma en la cual RandomX ha evitado la minería ASIC, es presentar requerimientos específicos para los equipos que quieran minar una de las criptomonedas que usen este sistema, los requisitos son:

- Que el equipo tenga una arquitectura de 64 bits.
- Hardware con compatibilidad con el estándar IEEE 754 en la unidad de coma flotante, indispensable para que los datos sean aceptados.
- Equipo con soporte de encriptación AES, y las actualizaciones.
- Cantidades de memoria cache mínimas establecidas.
- Que el sistema operativo del equipo pueda manejar páginas de memoria de gran tamaño.

Gracias a todos estos requerimientos han podido evitar la minería ASIC y la posible descentralización de la red, además, presentan una característica única que lo fortifica frente a estos equipos el uso de una máquina virtual en donde se ejecutan todos los procesos fortaleciendo los estándares de la criptografía. A continuación, se especifica las principales criptomonedas que usan este algoritmo en la red:

Tabla 9.

Principales criptodivisas que usan el algoritmo RandomX.

Criptomoneda	Precio	Acciones en circulación	Capitalización de mercado
Monero (XMR)	\$ 257.17	17,969,273.98 XMR	\$ 4,621,074,769

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

2.2.8. 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, así como para jóvenes y estudiantes escolares, el equipo obtuvo un éxito considerable que lo ha colocado

como uno de los referentes en esta sección del mercado mundial. (raspberrypi.org, Setting up your Raspberry Pi, 2019)

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 propio llamado Raspberry Pi OS basado en Debian. El equipo presenta una versatilidad enorme y un consumo energético muy bajo por lo cual es usado en frentes muy amplios como: Sistema de control multimedia, Emulación de sistemas y de videoconsolas, Ordenador común a través de las diferentes distribuciones, Procesamiento de equipos de domótica y IoT, y muchas opciones más dependiendo de las necesidades e imaginación del usuario. En las últimas versiones, la eficiencia energética se ha visto mejorada lo cual la hace perfecta para proyectos que demanden uso constante, así como velocidad de conexión a la red debido al puerto ethernet Gigabit, le permite desenvolverse de forma eficiente en operaciones en línea. A continuación, se detalla los modelos con los que cuenta el hardware y las características. (raspberrypi.org, 2019)

Tabla 10.

Modelos de Raspberry Pi y características

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

Información adaptada de los repositorios y artículos investigados. Elaborado por Crishian Loayza

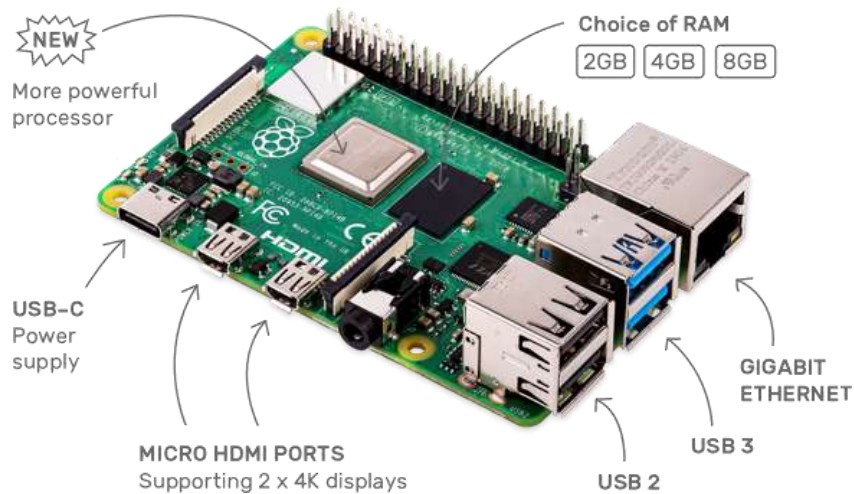


Figura 10. Raspberry Pi 4 modelo B. Información tomada de [raspberrypi.org](https://www.raspberrypi.org). Elaborado por [raspberrypi.org](https://www.raspberrypi.org)

2.2.9. CPU

El significado de las siglas CPU son Central Processing Unit es decir Unidad Central de Procesamiento, parte fundamental de un computador es la encargada de procesar todas las instrucciones u ordenes que le envíen las diferentes fuentes de entrada o salida del computador, es capaz de realizar enormes cálculos a velocidades muy altas dependiendo de la capacidad. (Miranda, 2015)



Figura 11. CPU. Información tomada de [mousegamers.com](https://www.mousegamers.com). Elaborado por Isarmina

2.2.10. GPU

El significado de las siglas GPU son Graphics Processing Unit es decir Unidad de Procesamiento Grafico, es la parte esencial de una tarjeta gráfica es la encargada de ejecutar complejos cálculos y procesos enfocados en tareas gráficas y video, existen tanto integradas dentro de las CPU o independientes en tarjetas gráficas externas. (Miranda, 2015)



Figura 12. GPU. Información tomada de programmerclick.com. Elaborado por programmerclick.com

2.2.11. ASIC

Las siglas significan Application-specific integrated circuit es decir Circuito Integrado para Aplicaciones Específicas como el nombre indica son una serie de equipos electrónicos que se fabrican para un uso específico, es decir cada una de las partes se encuentra en la placa para aportar a la función que el usuario solicito. Este tipo de hardware hoy en día se produce en masa para minar criptomonedas.



Figura 13. ASIC. Información tomada de academy.bit2me.com. Elaborado por academy.bit2me.com

2.2.12. AES

AES es un método criptográfico cuyas siglas significan Advanced Encryption Standard este sistema fue creado en Bélgica y actualmente es uno de los sistemas más usados por los altos niveles de seguridad, fue pesando con la finalidad de que fuese un método de dominio público. Ofrece cifrado por bloques y de tamaño de bloque de 128 bits con tamaños de llaves variables de 128, 192, 256. (Dag, OsvikJoppe, BosDeian, & David, 2010)

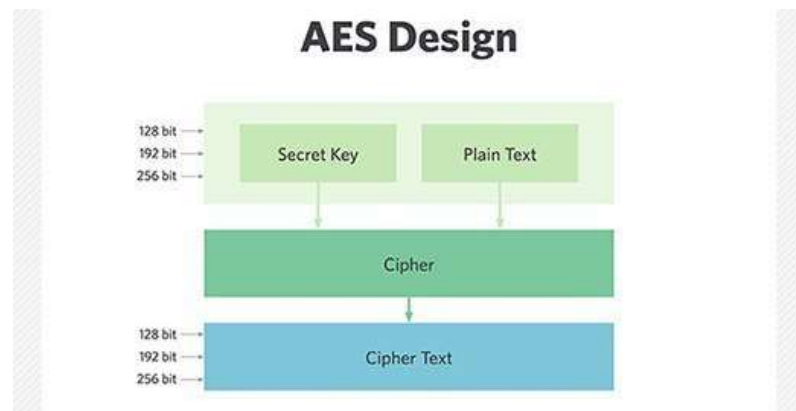


Figura 14. AES. Información tomada de searchsecurity.techtarget.com. Elaborado por Michael Cobb

2.2.13. Arquitectura ARM

Las siglas de la arquitectura ARM significan Advanced RISC Machine es decir Máquina RISC avanzada, RISC es un computador con conjunto de instrucciones reducido, este tipo de arquitectura se usa de mayor forma en microprocesadores y microcontroladores debido a que utilizan menos instrucciones que la arquitectura convencional x86, ofreciendo ventajas en equipos de dimensiones reducida o de bajo costo además esta tecnología abarca la mayoría del mercado mundial de la telefonía móvil. La tecnología esta licenciada por la empresa del mismo nombre ARM. (Alonso, 2021)



Figura 15. Procesador con arquitectura ARM. Información tomada de 49oogle.com. Elaborado por 49oogle.com

2.2.14. Hashrate

Termino usado dentro del mundo de las criptodivisas para definir la cantidad de hash que un determinado hardware puede producir para ejercer la minería, es decir la capacidad computacional del equipo. El hashrate de un equipo varía dependiendo de la criptomoneda, método de consenso o algoritmo criptográfico que se use, diferentes hardware se adaptan mejor a cada una de las variables. (Nakamoto, Algunas palabras en Bitcoin que usted puede escuchar, 2008)

2.2.15. Pool de minería

Un pool de minería es un lugar en la web en la cual los mineros pueden trabajar de forma conjunta para ejercer la minería de los bloques de la criptomoneda elegida, con el fin de recibir una recompensa conjunta pero dividida en base al poder computacional que aportaron durante todo el proceso de minado. El pool de minería permite que usuarios con capacidades pequeñas de minar puedan obtener una recompensa justa, además ofrecen ventajas como monitorización y automatización a los usuarios, por lo general estos pools cobran una comisión de lo que se ha minado usando el sistema. (Nakamoto, Algunas palabras en Bitcoin que usted puede escuchar, 2008)

2.2.16. Crypto Wallet o Monedero de criptomonedas

Un monedero de criptomonedas es un software o hardware que permite gestionar nuestros activos digitales, es decir guardar las claves públicas y privadas de nuestras diferentes criptomonedas con el fin de mantenerlas protegidas, pero también permitimos realizar intercambios, compras o ventas de forma fluida de criptomonedas. Debido a que las criptomonedas a diferencia de los activos físicos no cuentan la constancia tangible de tener el activo, lo que se guarda 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. (Conway, 2021)

2.3. Fundamentación legal

Dentro del marco de la Constitución de la Republica del Ecuador como norma suprema originaria no existe un tratamiento de las criptomonedas, pero a la vez entrega importantes artículos de consideración sobre la protección de información tecnológica, los usos y tratamiento, además algunos otros organismos estatales como el Banco Central del Ecuador que se han manifestado, con respecto a las criptomonedas.

2.3.1. Constitución de la Republica del Ecuador

- **Art. 66. Derechos de libertad. Numeral 21.-** Establece “El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación”. (Constitución de la República del Ecuador, 2011)
- **Art.385. Ciencia, tecnología, innovación y saberes ancestrales. Numeral 1.-** Establece “Generar, adaptar y difundir conocimientos científicos y tecnológicos.”. (Constitución de la República del Ecuador, 2011)
- **Art.385. Ciencia, tecnología, innovación y saberes ancestrales. Numeral 3.-** Establece “Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir”. (Constitución de la República del Ecuador, 2011)
- **Art.387. Ciencia, tecnología, innovación y saberes ancestrales. Numeral 1.-** Establece “Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo”. (Constitución de la República del Ecuador, 2011)
- **Art 387. Ciencia, tecnología, innovación y saberes ancestrales. Numeral 3.-** Establece “Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así

contribuir a la realización del buen vivir, al sumak kawsay”. (Constitución de la República del Ecuador, 2011)

2.3.2. Código Orgánico Integral Penal (COIP)

- **Art 178. Delitos contra el derecho a la intimidad personal y familiar** - Establece “La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años”. (Asamblea Nacional Republica del Ecuador, 2014)
- **Art 190. Apropiación fraudulenta por medios electrónicos** - Establece “La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años”. (Asamblea Nacional Republica del Ecuador, 2014)
- **Art. 229. Revelación ilegal de base de datos** - Establece “La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años”. (Asamblea Nacional Republica del Ecuador, 2014)
- **Art 232. Ataque a la integridad de sistemas informáticos.** - Establece “La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de

telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años”. (Asamblea Nacional Republica del Ecuador, 2014)

- **Art 234. Acceso no consentido a un sistema informático, telemático o de telecomunicaciones** - Establece “La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años”. (Asamblea Nacional Republica del Ecuador, 2014)

2.3.3. Banco Central del Ecuador

El Banco Central del Ecuador emitió un comunicado en el año 2018 sobre la criptomoneda bitcoin, conocida por ser la de mayor impacto a nivel mundial y dijo lo siguiente: “El Banco Central del Ecuador informa a la ciudadanía que el bitcoin no es un medio de pago autorizado para su uso en el país. El bitcoin es una criptomoneda que no tiene respaldo, pues sustenta su valor en la especulación. Las transacciones financieras realizadas a través del bitcoin no están controladas, supervisadas ni reguladas por ninguna entidad del Ecuador, razón por la que su uso representa un riesgo financiero para quienes lo utilizan. Es importante señalar que no está prohibida la compra y venta de criptomonedas -como el bitcoin- a través de Internet; sin embargo, se recalca que bitcoin no es una moneda de curso legal y no está autorizada como un medio de pago de bienes y servicios en el Ecuador, conforme lo establece el artículo 94 del Código Orgánico Monetario y Financiero.” El artículo 94 del Código Orgánico Monetario y Financiero indica que “todas las transacciones, operaciones monetarias, financieras y sus registros contables, realizados en la República del Ecuador, se expresarán en dólares de los Estados Unidos de América, de conformidad con este Código”. (BCE, 2018)

Por consiguiente, las criptomonedas, específicamente el bitcoin no está en regulación del estado, pero a la vez indican que el uso, o intercambio no se encuentran prohibidos afirmándose en la Ley de Defensa del Consumidor que garantiza al ciudadano el derecho a escoger bienes

con libertad “Derecho a que proveedores públicos y privados oferten bienes y servicios competitivos, de óptima calidad, y a elegirlos con libertad”. (ECUADOR, 2000)

Capítulo III

Propuesta

3.1. Métodos de investigación

3.1.1. Metodología cuasi experimental

Este método se basa en imponer a un objeto o grupo a que se manipulen variables de estudio por el investigador para mantener bajo control la variación de estas variables y cuáles serán las consecuencias debido a esas manipulaciones, a diferencia del método experimental en el método cuasi experimental los procesos ocurren o se aplican no de forma aleatoria, en cambio se aplican esperando que una de las variables tenga un resultado previsible. Según Navarro (2016) “El método cuasi experimental se utiliza cuando no es posible la asignación aleatoria o cuando por razones prácticas o éticas es necesario utilizar grupos naturales o ya formados como por ejemplo sujetos con una determinada enfermedad. Por lo tanto, se aplica en aquellos casos donde el investigador no puede presentar los niveles de la variable independiente a voluntad ni puede crear los grupos experimentales por aleatorización, aunque sí puede introducir algo similar al diseño experimental en programación de procedimientos para la recopilación de datos como el cuándo y el a quién de la medición.” Además, agrega que este tipo de metodología en muchos casos viene definido desde una organización como una condición para ingresar en diferentes frentes de investigación con lineamientos establecidos.

Esta metodología es un parte fundamental del proceso educativo, y se requirió de ella dentro de este trabajo de titulación debido a que al momento al momento de evaluar la factibilidad de la minería de criptodivisas con Raspberry Pi se manejarán diferentes variables de las cuales se tiene conocimiento sobre los fenómenos regulares durante el trabajo, y de esta forma encontrar la configuración con mejor rendimiento.

3.1.2. Método Descriptivo

El método descriptivo también llamado de diagnóstico método es el encargado de describir un fenómeno, situación o población el cual es el motivo de estudio y características. Las funciones del método son definir, clasificar, descomponer y redactar las partes fundamentales del objeto de estudio.

El propósito de los métodos de este tipo es el de recabar la mayor cantidad de datos específicos que puedan usarse en promedios y cálculos estadísticos que muestran tendencias. Usado de forma regular en estudios, es el punto de inicio a diferentes estudios más minuciosos y complejos sobre un fenómeno definido, al ofrecer datos sobre forma y función. (Yanez, 2019)

Las principales preguntas que busca responder este método son acerca del qué, cómo, cuándo y dónde centrado en el estudio en cuestión, este método no usa el recurso del por qué el fenómeno se comporta de cierta forma. Además, no tiene en cuenta las relaciones entre estas características y se basta con describirlas, y a diferencia de otras metodologías no modifican o alteran las variables del fenómeno y basa conclusiones en datos conocidos. Esta metodología forma parte importante dentro de este estudio, debido a que proporciona las herramientas ideales para comprender las diferentes partes que conforman los procesos de la minería de criptodivisas, describiendo funcionalidades e importancia dentro del proceso.

3.1.3. Metodología Evaluativa

La metodología evaluativa presenta una forma efectiva y sistemática de obtener la mayor cantidad de información sobre un determinado fenómeno o proyecto, las diferentes características, funcionamiento y resultados, con el fin de recabar nueva información relevante para la investigación que aporte para la toma de decisiones respecto al funcionamiento del proyecto. Presenta una gran flexibilidad al momento de valorar diferentes proyectos ya sean de carácter, social, educativo o investigativo ya que sus procesos científicos permiten acumular cantidades considerables de evidencia fiable sobre los resultados que producen un cumulo de procesos. (Mejía-Castillo, 2018)

Dentro de esta metodología es común plantearse la revisión de evaluaciones anteriores del fenómeno elegido, lo cual permite identificar características destacables para tener en cuenta o que deban mantenerse controladas. Además, el encargado de realizar la evaluación debe tener en claro las condiciones en las que se encuentra el fenómeno y documentarlo, junto con los diferentes impedimentos y características no conocidas. (Mejía-Castillo, 2018)

Esta metodología nos permitirá obtener una respuesta sobre la factibilidad del proyecto y de la información que se obtenga, luego de ejecutar los diferentes procesos que conforman la minería de criptodivisas, alcance y capacidad.

3.2. Población y muestra

La población elegida para esta encuesta está conformada por los estudiantes de noveno semestre de la materia arquitectura cliente servidor de la carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil y estudiantes que se encuentran desarrollando proyectos de tesis de grado con temas relacionados a la línea de investigación de la propuesta de tesis. La muestra es de 52 estudiantes de una población de 52, para lograr recabar la mayor cantidad de información importante.

3.3. Técnica de recolección de datos

Se propone el uso de una encuesta como instrumento para identificar el nivel de conocimiento sobre criptodivisas, minería y el hardware Raspberry Pi de los estudiantes de los últimos niveles de la carrera de ingeniería en teleinformática de la Universidad de Guayaquil. Para revisar detalladamente las preguntas de la encuesta ver anexo 1.

3.3.1. Encuesta

Pregunta 1: ¿Conoce lo que es una criptodivisa?

Tabla 11.

Cantidad de alumnos que conocen que es una criptodivisa

Opción	Estudiantes	Porcentaje
Si	42	84%
No	8	16%

Información adaptada de Google Forms. Elaborado por Crithian Loayza

¿ Conoce lo que es una criptodivisa?

50 respuestas

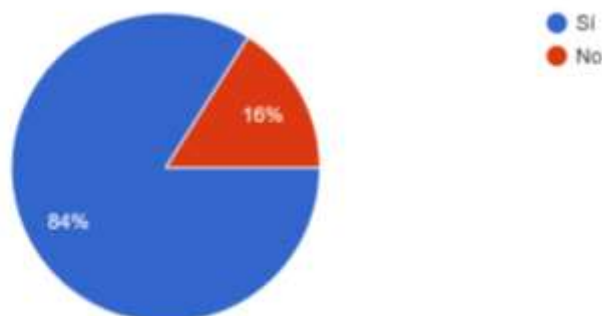


Figura 16. Cantidad de alumnos que conocen que es una criptodivisa. Información tomada de Google Forms. Elaborado por el autor

Análisis: El 84% de las respuestas indican que, si conocen que es una criptodivisa, y el 16% entrega una respuesta negativa, lo cual entrega un margen positivo sobre la difusión del tema, dentro del contexto de la encuesta.

Pregunta 2: ¿Cuál de las siguientes criptodivisas conoce?

Tabla 12.

Que criptodivisa se encuentra más difundida entre los alumnos

Opción	Estudiantes	Porcentaje
Bitcoin	50	96.2%
Ethereum	0	0%
Dogecoin	1	1.9%
Monero	0	0%
Ninguno	1	1.9%

Información adaptada de Google Forms. Elaborado por Cristhian Loayza

¿Cuál de las siguientes criptodivisas conoce?

52 respuestas

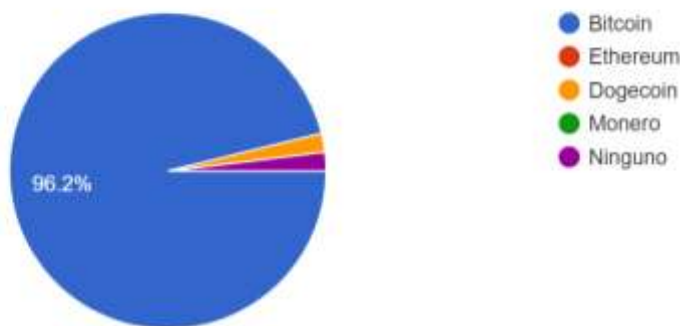


Figura 17. Que criptodivisas se encuentra más difundida entre los alumnos. Información tomada de Google Forms. Elaborado por el autor

Análisis: Dentro del abanico de opciones que se planteo sobre las criptodivisas que conocen los encuestados, el 96,2% indico que conoce bitcoin lo cual es entendible debido a su popularidad, el 1.9% indico que conoce dogecoin, y de la misma forma 1.9% que no conoce ninguna criptodivisa, dándonos una clara idea que varios encuestados conocen bitcoin sin incluso saber que es una criptodivisa.

Pregunta 3: ¿Conoce usted algo del proceso de minería de criptodivisas?**Tabla 13.**

Cantidad de alumnos que conocen sobre el proceso de minería de criptodivisas

Opción	Estudiantes	Porcentaje
Si	20	38.5%
No	32	61.5%

Información adaptada de Google Forms. Elaborado por Crithian Loayza

¿Conoce usted algo del proceso de minería de criptodivisas?

52 respuestas

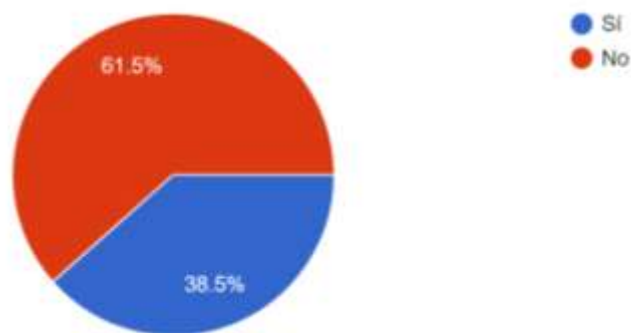


Figura 18. Cantidad de alumnos que conocen sobre el proceso de minería de criptodivisas. Información tomada de Google Forms. Elaborado por el autor

Análisis: El 61.5% de las respuestas indican que, no conocen que es el proceso de minería de criptodivisas, y el 38.5% que, si conoce el proceso, lo cual da un margen negativo sobre la difusión del tema, dentro del contexto de la encuesta.

Pregunta 4: ¿Cuál de estos algoritmos criptográficos de minería conoce?**Tabla 14.**

Algoritmo criptográfico más difundido

Opción	Estudiantes	Porcentaje
SHA-256	8	15.7%
Ethash	2	3.9%
Scrypt	14	27.5%

RandomX	5	9.8%
Ninguno	22	43.1%

Información adaptada de Google Forms. Elaborado por Crithian Loayza

¿Cuál de estos algoritmos criptográficos de minería conoce?

51 respuestas

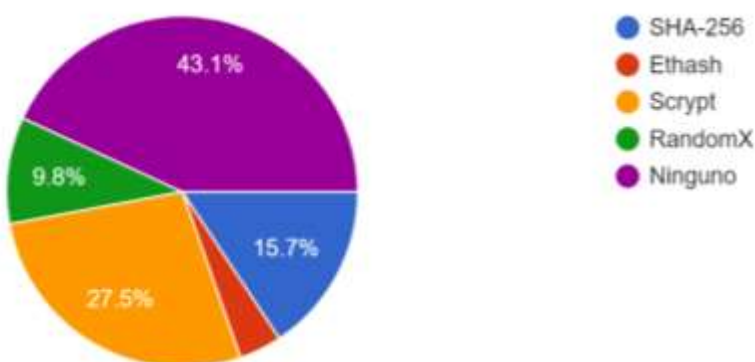


Figura 19. Algoritmo criptográfico más difundido. Información tomada de Google Forms. Elaborado por el autor

Análisis: El 43.1% de los encuestados indican que no conocen ninguno de los algoritmos criptográficos mencionados, y el 27,5% que conoce Scrypt este algoritmo se usa en varis sistemas de telecomunicaciones por lo cual su difusión es mayor en el contexto, el 15.7% indica que conoce SHA-256, el 9.8% Randomx y solo 3.9% Ethash.

Pregunta 5: ¿Cuál de los siguientes ordenadores de bajo costo y tamaño reducido conoce?

Tabla 15.

Ordenador de bajo costo y tamaño reducido más difundido

Opción	Estudiantes	Porcentaje
Raspberry Pi	46	92%
Orange Pi	0	0%
ODDYSEY	0	0%
Nova Pi	1	2%
Otra (Arduino, No sé, Sony)	3	6%

Información adaptada de Google Forms. Elaborado por Cristhian Loayza

¿Cuál de los siguientes ordenadores de bajo costo y tamaño reducido conoce?

50 respuestas

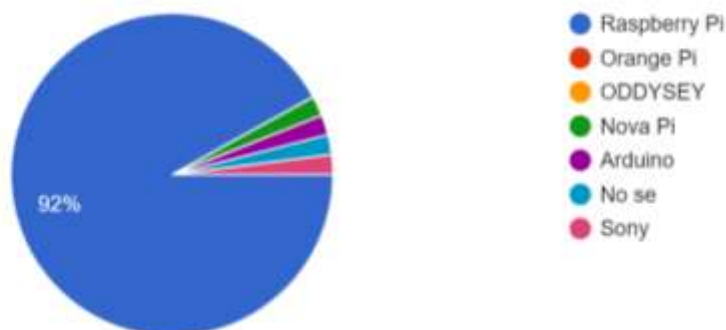


Figura 20. Ordenador de bajo costo y tamaño reducido más difundido. Información tomada de Google Forms. Elaborado por el autor

Análisis: El 92% de encuestados indican que conocen Raspberry Pi, altamente esperado debido a su popularidad, los demás solamente obtuvieron Nova Pi el 2%, Sony 2%, No sé 2%, Arduino 2%, Arduino y No se fueron opciones ingresadas por los encuestados en otros.

Pregunta 6: ¿Sabía que se puede minar criptodivisas con Raspberry Pi?

Tabla 16.

Cantidad de alumnos que conocen que se puede minar criptodivisas con Raspberry Pi

Opción	Estudiantes	Porcentaje
Si	30	57.7%
No	22	42.3%

Información adaptada de Google Forms. Elaborado por Cristhian Loayza

¿Sabía que se puede minar criptodivisas con Raspberry Pi ?

52 respuestas

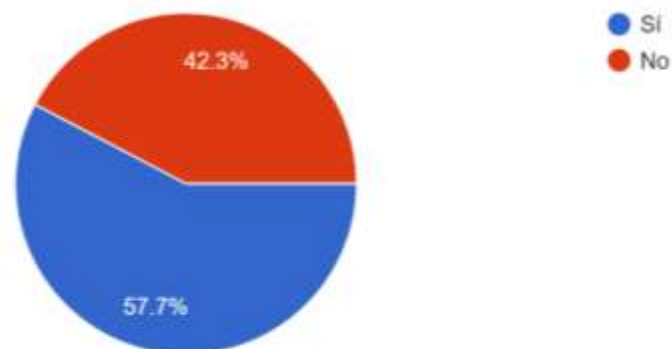


Figura 21. Cantidad de alumnos que conocen que se puede minar criptodivisas con Raspberry Pi. Información tomada de Google Forms. Elaborado por el autor

Análisis: Una cantidad considerable de los encuestado conoce que se puede minar criptodivisas mediante Raspberry Pi exactamente el 57.7%, y el 42.3% que no.

Pregunta 7: ¿Cuál de estas cualidades considera favorables de Raspberry Pi?

Tabla 17.

Cualidad de Raspberry Pi más favorable

Opción	Estudiantes	Porcentaje
Tamaño compacto	24	46.2%
Bajo consumo	10	19.2%
Precio accesible	11	21.2%
Comunidad mundial	7	13.5%

Información adaptada de Google Forms. Elaborado por Cristhian Loayza

¿Cuál de estas cualidades considera favorables de Raspberry Pi ?

52 respuestas

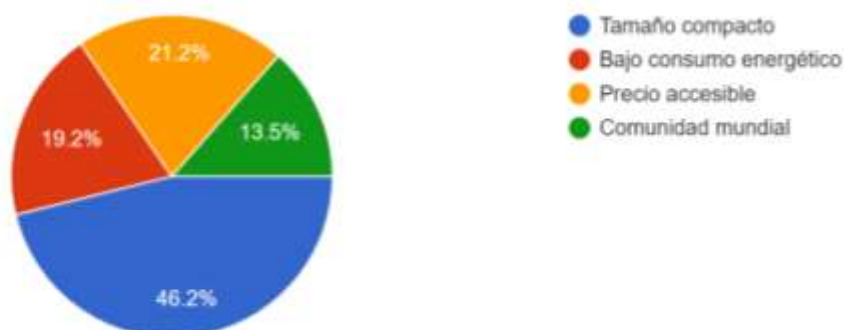


Figura 22. Calidad de Raspberry Pi más favorable. Información tomada de Google Forms. Elaborado por el autor

Análisis: Dentro de las cualidades de Raspberry pi, las que se consideran favorables por los encuestados son, tamaño compacto 46.2%, precio accesible 21.2%, bajo consumo energético 19.2%, y comunidad mundial 13.5%.

Pregunta 8: ¿Sabía que el uso de hardware para minería de criptomonedas requiere un elevado consumo energético?

Tabla 18.

Cantidad de alumnos que conocen que para minar criptomonedas se requiere un elevado consumo energético

Opción	Estudiantes	Porcentaje
Si	31	59.6%
No	21	40.4%

Información adaptada de Google Forms. Elaborado por Cristhian Loayza

¿Sabía que el uso de hardware para minería de criptomonedas requiere un elevado consumo energético?

52 respuestas

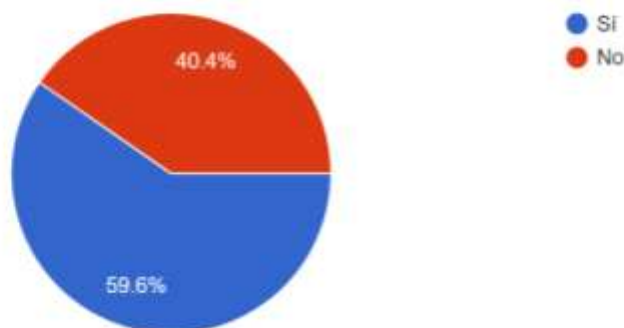


Figura 23. Cantidad de alumnos que conocen que para minar criptomonedas se requiere un elevado consumo energético. Información tomada de Google Forms. Elaborado por el autor

Análisis: Según las respuestas de los encuestados su conocimiento sobre el elevado consumo energético para el proceso de minería de criptodivisas está dividido y el 59.6% indica que, si lo sabía, y el 40,4% que no.

3.3.2. Análisis global de resultados

Los encuestados, que se dividen entre estudiantes de la materia arquitectura cliente servidor y estudiantes que se encuentran desarrollando proyectos de tesis de grado con temas relacionados a la línea de investigación de la propuesta de tesis, demostraron mediante sus respuestas que tienen un conocimiento general del tema, debido a que su conocimiento sobre que es una criptodivisa es alto, pero en aspectos importantes sobre su funcionamiento como la minería presentan respuestas positivas menores, y en el aspecto de que tipos de algoritmo criptográfico conoce una gran parte no conoce ninguno, dejando al grupo como un conjunto que conoce en general del tema pero no su funcionamiento o características.

Sobre las preguntas sobre el hardware Raspberry Pi la mayoría tiene conocimiento de su existencia y destacaron como cualidades favorables su tamaño reducido, precio accesible y consumo energético reducido.

3.4. Elementos utilizados para el diseño de la propuesta

Dentro del presente trabajo de investigación donde evaluaremos 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 analizaremos cada una de estas antes de elegir la criptomoneda que minaremos en nuestro hardware.

3.4.1. Algoritmos de consenso

Dentro del presente trabajo 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 los 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.

Tabla 19.

Comparativa de algoritmos de consenso y características

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

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Tabla 20.

Comparativa de algoritmos de consenso y características

Algoritmo	Consumo energético	Requisito de usabilidad	Descentralización
Prueba de trabajo	Elevado consumo, dependiendo del equipo	Hardware regular, sin requisitos	Regular, bajo peligro de perdida, por equipos especializados
Prueba de participación	Mínimo, no exige al equipo	Tener el activo, entre más activo más posibilidad de minarlo	Alta, usuarios pueden participar de forma más activa

Prueba de participación delegada	Mínimo, no exige al equipo	Tener el activo, entre más activo más posibilidad de minarlo	Regular, delegados con más activos tienen más posibilidades
Prueba de actividad	Elevado consumo, dependiendo del equipo	Tener el activo, hardware regular	Regular, bajo peligro de pérdida, por equipos especializados
Prueba de quemado	Bajo, con incertidumbre de alto consumo por intercambio	Tener el activo, entre más activo más minería, pérdida de activo para minar	Baja, peligro de pérdida por usuarios con grandes cantidades de activo
Prueba de capacidad	Bajo, equipos en consumo mínimo	Dispositivo de almacenamiento masivo	Regular, peligro de ataques por ser relativamente nueva
Prueba de tiempo transcurrido	Bajo, equipos en consumo mínimo	Procesador Intel	Regular, sensible a ataques al procesador
Prueba de asignación	Bajo, equipos IoT son de bajo consumo	Equipos IoT, minería mínima debido a potencia de equipos	Alta, sin posibilidad de acumulación de poder
Protocolo Ripple	Bajo, servidores consumen energía mínima	Proyecto creado para privados	Nula, centralización total, cada nodo controla un servidor
Prueba de autoridad	Bajo, validadores funcionan con equipos modestos	Verificar identidad en la red, y aportar con proyectos para mejora	Baja, ciertos usuarios validan todas las transacciones

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

En las tablas anteriores, se analizó varios de los aspectos más importantes de los algoritmos de consenso, para poder determinar cuál o cuáles son los más idóneos para en conjunto con el algoritmo criptográfico elegir la mejor opción que se adapte al hardware Raspberry Pi.

Debido a que el equipo minador ejecutara la minería desde cero debemos 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 debemos descartar 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 nuestro 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 debemos descartar es la Prueba de asignación el cual utiliza pequeños dispositivos como cámaras, parlantes y demás para minar de forma pasiva, y no entra en los lineamientos del proyecto debido a que queremos 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.

3.4.2. 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 nuestro hardware que usa CPU para minar por lo cual no es un detalle menor. 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, realizaremos una tabla comparativa con las opciones más representativas de la actualidad.

Tabla 21.

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)
<u>Ethash</u>	ASIC, CPU, GPU	Alta, basado en SHA-3, varios algoritmos a la vez	Ethereum (ETH), Ethereum Clasic(ETC)
<u>Scrypt</u>	ASIC, CPU, GPU	Alta, requiere mucha memoria, resistente ataques fuerza bruta	Dogecoin (DOGE), Litecoin (LTC)
<u>X11</u>	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)

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Como se puede observar en la **Tabla 21**, las características que hemos destacado de cada uno de los algoritmos fueron, el hardware de uso es decir en qué tipos de dispositivos se puede minar, debido a que entre más extendida este la minería con el algoritmo menos rentable resultara, además es de importancia elegir un algoritmo que limite o evite la minería en dispositivos ASIC los cuales presentan niveles de minado por encima del resto provocando que los usuarios con poco poder computacional se vean afectados y además son equipos que consumen grandes cantidades de energía lo cual no se apega a la sostenibilidad energética que buscamos. En el ámbito de la seguridad todos los algoritmos presentan niveles altos debido al tiempo que llevan siendo probados, en algunos casos como X11 o RandomX mantienen una ventaja al usar sistemas que crean aleatoriedad al momento de producir el hash elevando la complejidad. Y por último las criptodivisas que funcionan con este algoritmo, es importante que la criptodivisa que se elija funcione mediante el método de consenso que se determinó más idóneo como fue Prueba de trabajo, y que la cadena de bloques entregue seguridad y confianza a los usuarios.

En base a las características que interesan los algoritmos más idóneos serían 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 una 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 (Coinmarketcap, 2021) 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.

3.4.3. 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. (Li, et al., 2019)

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 (Coinmarketcap, 2021)



Figura 24. Logotipo de Monero (XMR). Información tomada de nuevofinanciero.com. Elaborado por nuevofinanciero.com

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.

3.4.4. Pool de minería

Como se detalló en el capítulo anterior un pool de minería permite que un grupo de mineros ejecuten la minería de forma simultánea, entregando la recompensa en base al 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 detallaremos algunos de los pool más difundidos de la criptomoneda elegida y sus características para elegir la opción idónea.

Tabla 22.

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

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

En este caso elegiremos xmrpool.eu debido tener una comisión baja, pero sobre todo su pago mínimo que es el más bajo de todos el cual nos permitirá enviar nuestras criptomonedas de forma temprana a nuestro monedero.

3.4.5. Modelo Raspberry Pi

El equipo minador Raspberry Pi mantiene varias versiones de su placa de desarrollo, desde el Model A+ a la más actual 4 Model B, y como se detalló anteriormente en la Tabla 10 existen varias diferencias, sobre todo en la memoria RAM y el procesador. Debido a esto en el proyecto se trabajará con el modelo más actual 4 Model B en su versión de 4 GB de RAM, lo cual es una cantidad con la cual se puede manejar la mayoría de las aplicaciones y sistemas, además de que su procesador cuenta con 4 núcleos de procesamiento ideales para tareas exigentes, y que este modelo presenta un puerto ethernet gigabit que permitirá una conexión de red de alta velocidad. El consumo energético de este equipo es de alrededor de 6 watts +-0.5 watts en el modo de operación exigente. (raspberrypi.org, Configurando tu Raspberry Pi, 2020)

3.4.6. Sistema operativo

El hardware Raspberry Pi al ser una placa de desarrollo y proyectos, no viene con un sistema operativo por defecto e invita a sus usuarios a elegir el que mejor se adapte a sus necesidades, entre los sistemas compatibles están Ubuntu, Debian, Manjaro ARM Linux, RISC OS Pi y

muchos más pasando por sistemas de línea de comando, a adaptados para IoT o para consolas de videojuegos. (raspberrypi.org, Configurando tu Raspberry Pi, 2020)

Pero dentro del contexto del trabajo la alternativa más viable es Raspberry Pi OS el sistema operativo propio de la Raspberry Pi Foundation de 32 bits, el cual está diseñado para exprimir las características del hardware, evitando fallos o bugs de forma general, este sistema operativo GNU/Linux está basado en Debian y se lleva desarrollando desde 2012. El sistema está optimizado para cálculos de coma flotante por hardware lo que brindará un mejor rendimiento frente a la minería que se ejecutará.

3.5. Diseño de la propuesta

Una vez determinados los diferentes elementos relevantes para la propuesta es de importancia determinar un esquema que defina en qué 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

3.5.1. Conexión del hardware e instalación del sistema operativo

3.5.1.1. Conexión del hardware

Como se mencionó en el punto Modelo de Raspberry Pi el modelo que usará el proyecto es el 4 Model B, este como sus versiones anteriores trata de simplificar los procesos, por lo cual lo único que se incluye dentro de su caja es la placa y una guía, pero es recomendable desde su propia página oficial el uso de disipadores en los componentes del equipo, y ventilación en caso de uso de manera constante para mantener una temperatura adecuada, a continuación, se mostrarán las conexiones del hardware.



Figura 25. Caja Raspberry Pi 4 Model B versión 4GB RAM



Figura 26. Raspberry Pi Raspberry Pi 4 Model B y disipadores.

Una vez colocados los disipadores, se necesita adicional para poder comenzar a utilizar el hardware una fuente de 5 voltios y 3 amperios, con conector tipo USB C que es el estándar actual que usa la Raspberry Pi 4 Model B, una unidad de almacenamiento en nuestro caso MicroSD, y un cable miniHDMI a HDMI para poder visualizar el contenido, además de entradas de información como teclado y ratón.

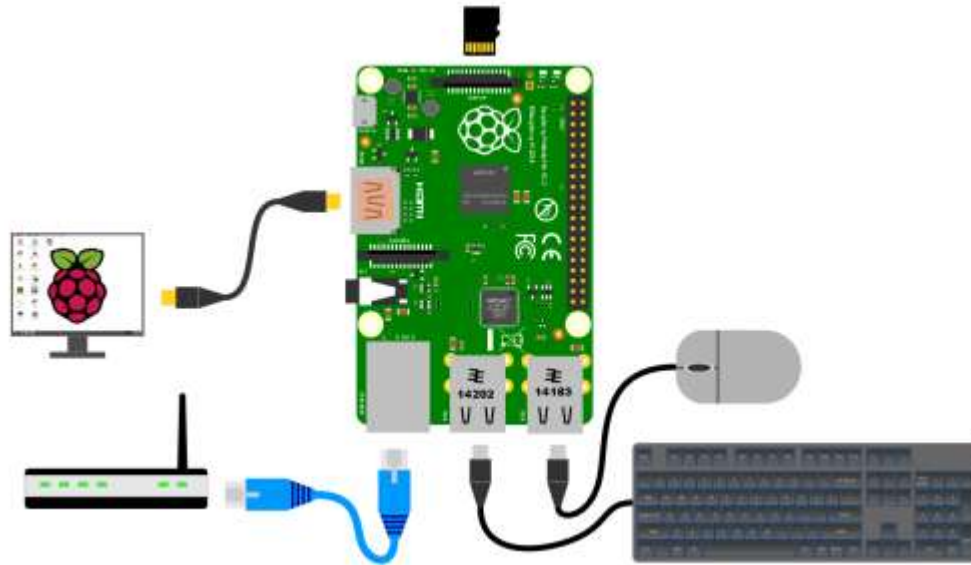


Figura 27. Raspberry Pi y conexiones. Información tomada de leanpub.com. Elaborado por Malcolm Maclean

3.5.1.2. Instalación de sistema operativo

Como se definió anteriormente para el presente trabajo se usará el sistema operativo Raspberry Pi OS, desde la página oficial de la organización y con la ayuda de un computador con entrada MicroSD podremos cargar el sistema operativo a nuestra unidad de almacenamiento, a continuación, el proceso:

- Dentro de la página oficial de la organización <https://www.raspberrypi.org/> en el apartado de software encontraremos el programa Raspberry Pi imager que permitirá instalar tanto el software oficial como cualquier distribución o sistema que queramos siempre y cuando tengamos la imagen del software.



Figura 28. *Raspberrypi.org/software*

- Una vez el software descargado e instalado, al ejecutar el programa nos aparecerá de la siguiente forma.



Figura 29. *Raspberry Pi imager instalado*

- Una vez en esta pantalla, debemos elegir el software en la opción Operating System, como anteriormente se comento se usara Raspberry Pi OS, el instalador ofrece la version estandar que requiere 1.2 GB de espacio de disco mas 2 opciones, la opciones full incluye software adicional de programacion y reproduccion multimedia que requiere 2.4 GB y una version lite sin software adicional que ocupa 0.4 GB, en nuestro caso usaremos la version full.



Figura 30. *Raspberry Pi imager- Operating System*

- Una vez elegida la distribución optima, se elige la unidad en donde se instalara el sistema operativo, en la opción Storage.



Figura 31. Raspberry Pi imager- Storage

- En este punto solo falta elegir la opción de write, para que el programa instale todo lo necesario, una ventana advertirá de que se borrarán todos los archivos que estén actualmente en la unidad de almacenamiento debemos aceptar y el proceso comenzara.



Figura 32. Raspberry Pi imager- Listo para el proceso



Figura 33. Raspberry Pi imager- Proceso iniciado

- Una vez el proceso de Raspberry Pi imager concluyo tendremos la MicroSD lista con el sistema operativo, procederemos a conectarla a la Raspberry Pi y encenderla para desde este punto inicializar el equipo.

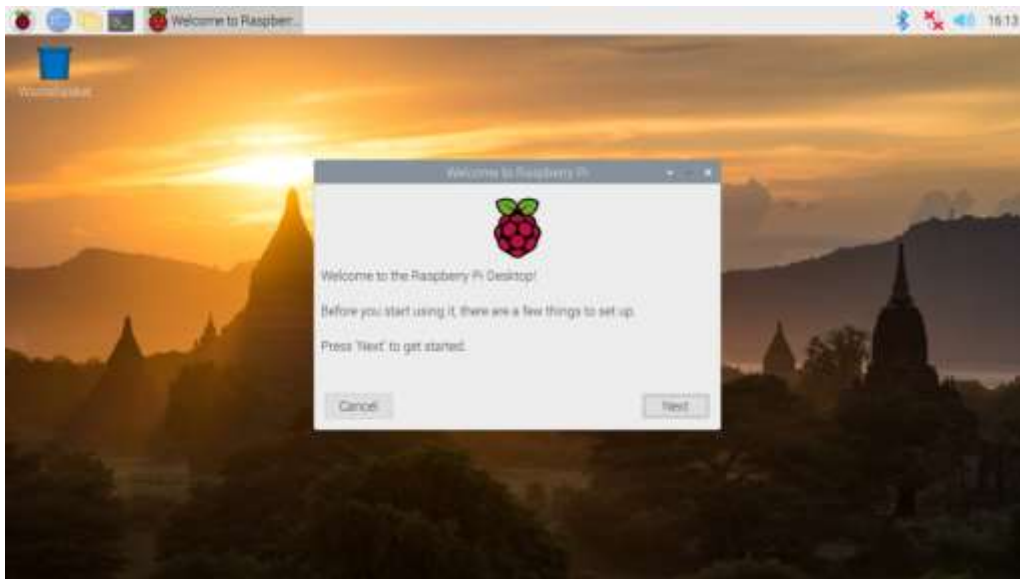


Figura 34. Raspberry Pi OS- Guia de inicio

- Se puede observar el sistema presenta una interfaz amigable y fácil de usar, basta con seguir la guía de inicio, agregar una contraseña, conectarse a una red de su preferencia, elegir su idioma y esperar a que se actualice para tener el equipo listo.

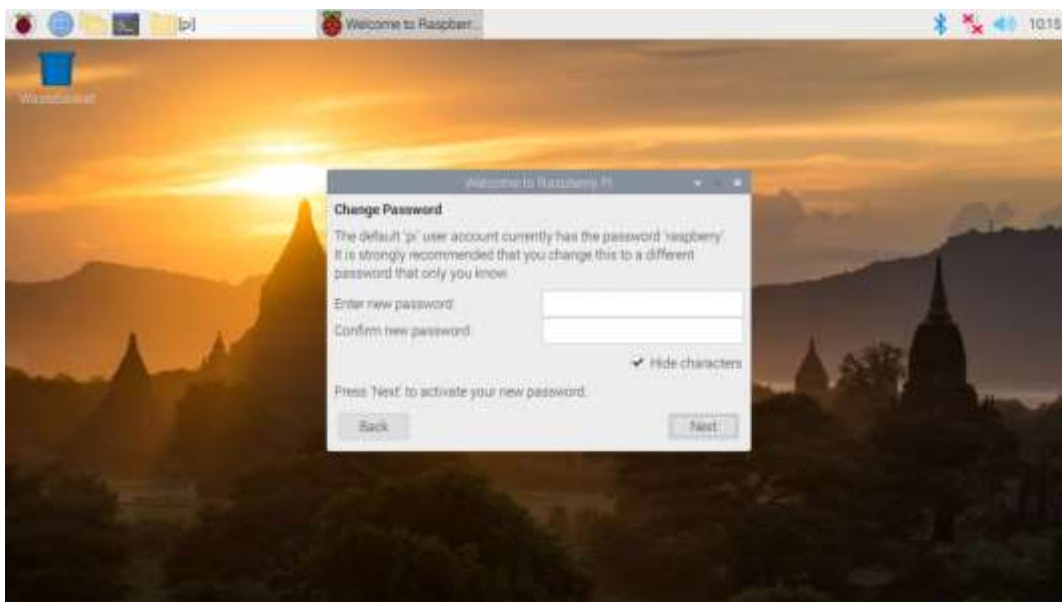


Figura 35. Raspberry Pi OS- Clave del equipo

3.5.2. Configuración del wallet para criptomonedas

Uno de los requisitos previos a ejecutar la minería de criptodivisas es tener una dirección dentro de la blockchain de la criptomoneda que elegimos, en este caso Monero. Se puede crear de varias formas en wallets conocidas, pero ~~creándola~~ en la wallet oficial tenemos un nivel de confianza mayor, debido a que a esta dirección llegan nuestras criptodivisas.

- Se ingresa a la página oficial de Monero y en la sección de software, elegiremos la que sea adecuada para nuestro equipo.

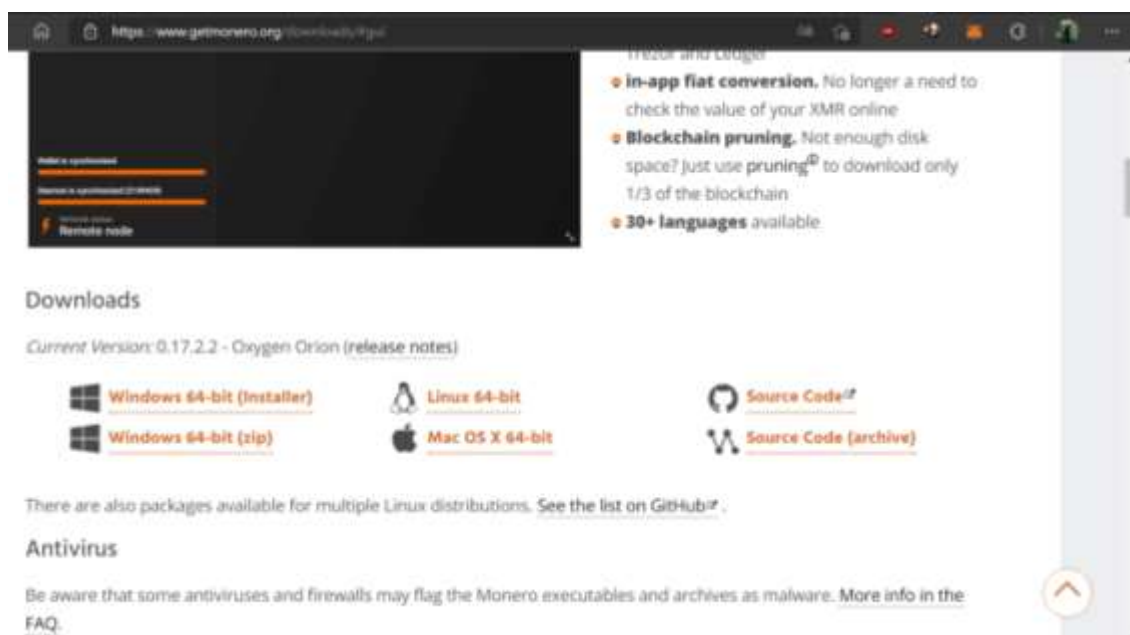


Figura 36. Página oficial del wallet de Monero- Sistemas disponibles

- Una vez disponible el instalador de la wallet, solo debemos seguir los pasos del instalador hasta tenerlo listo.



Figura 37. Oxygen Orion GUI Wallet - Instalador del wallet de Monero

- El wallet, cuenta con varias opciones para ejecutarlo, se opta por la opción de “Crear un nuevo monedero”

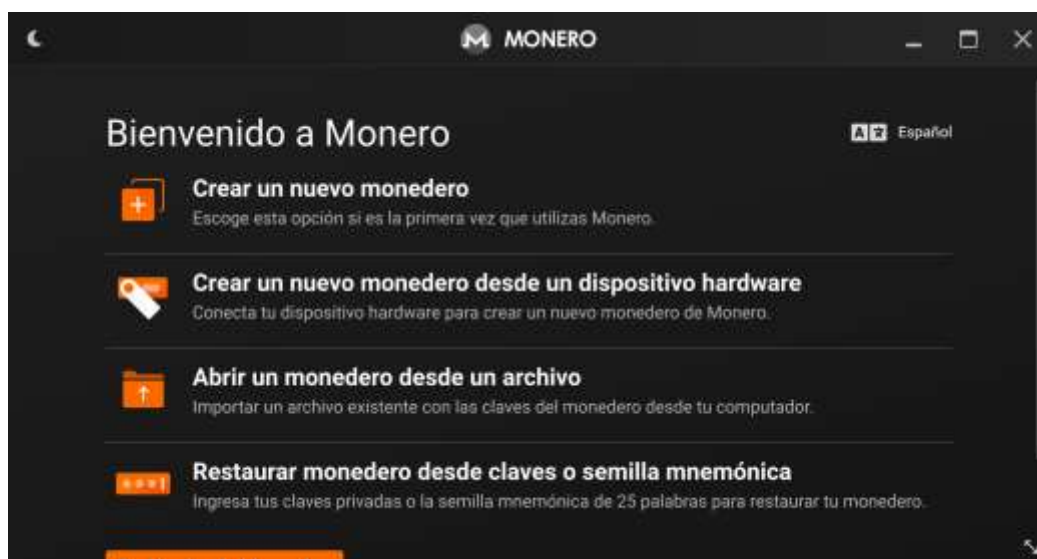


Figura 38. Monero Wallet – Opciones de monedero

- Se escoge un nombre para el wallet, un lugar en donde se guardarán los datos y muy importantes guardar la frase semilla, esta permitirá recuperar los activos que contenía el wallet en caso de olvidar la contraseña.

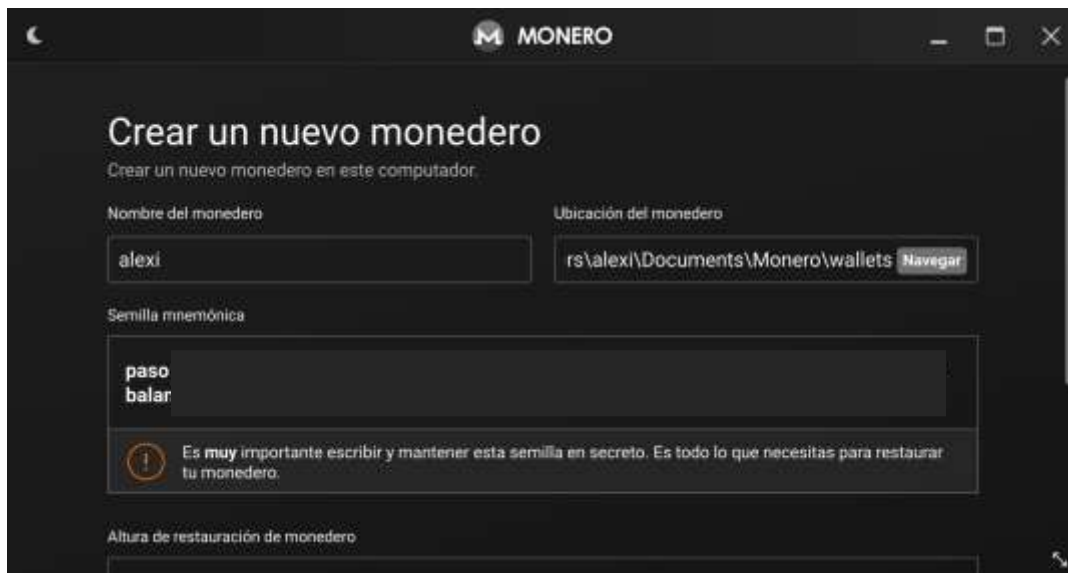


Figura 39. Monero Wallet – Datos del monedero

- Luego de agregar una contraseña el wallet estará listo para usar, en la opción de recibir encontraremos la dirección de Monero e información de los bloques por minar de la red. En este punto estará todo listo para comenzar el proceso de minería.

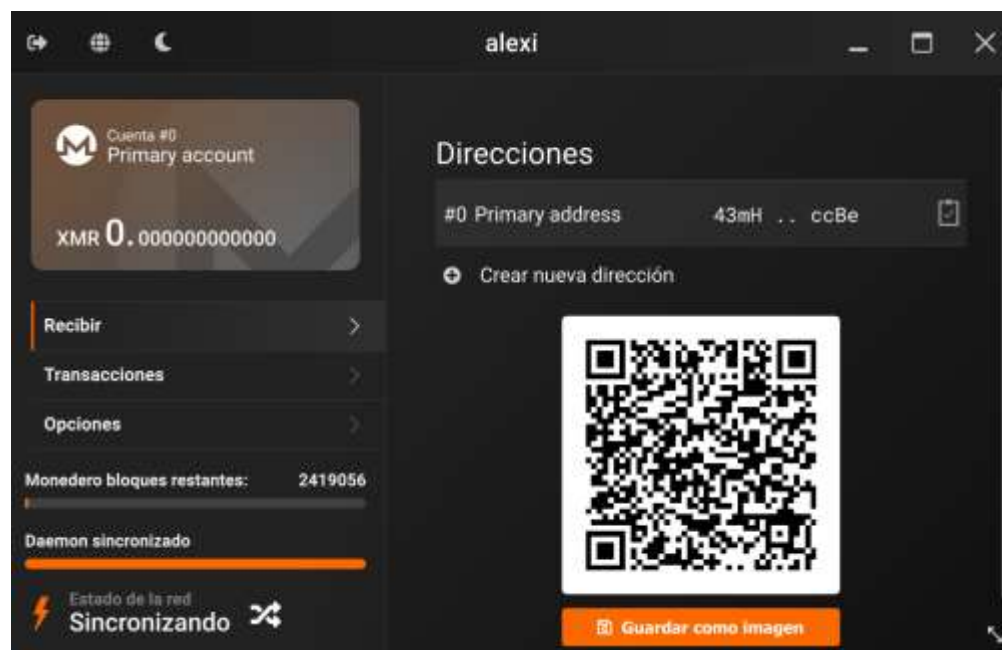
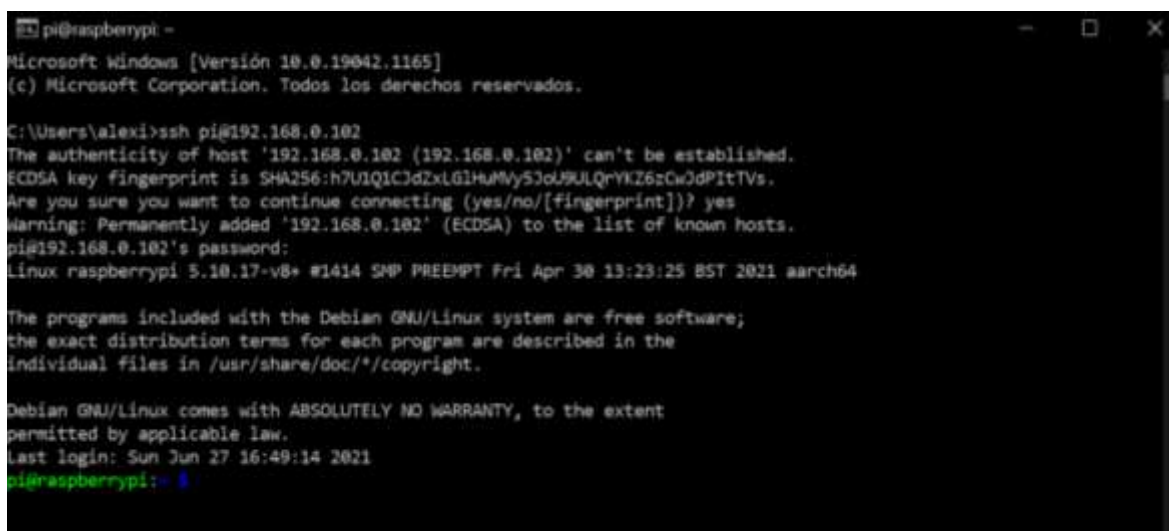


Figura 40. Monero Wallet – Wallet listo

3.5.3. Configuración del software minador

Llegados a este punto 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 tenemos varias opciones para manejar el hardware y ejecutar la minería, pero en este caso se usará de forma remota mediante SSH. Es realmente sencillo 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 debemos confirmar y por ultimo ingresar la clave que le asigno al equipo.



```

pi@raspberrypi ~
Microsoft Windows [Versión 10.0.19042.1165]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\alexi>ssh pi@192.168.0.102
The authenticity of host '192.168.0.102 (192.168.0.102)' can't be established.
ECDSA key fingerprint is SHA256:h7U1Q1CJdZxLGilHuMMyS3oU9ULQrYKZ6zCwOdPitTVs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.102' (ECDSA) to the list of known hosts.
pi@192.168.0.102's password:
Linux raspberrypi 5.10.17-v8+ #1414 SMP PREEMPT Fri Apr 30 13:23:25 BST 2021 aarch64

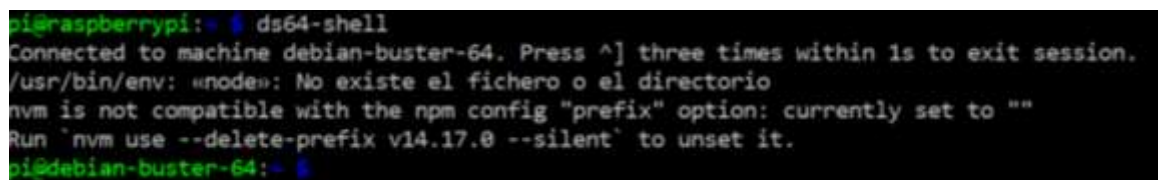
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun 27 16:49:14 2021
pi@raspberrypi:~$

```

Figura 41. Terminal Raspberry Pi OS mediante Windows – Conexión mediante SSH a Raspberry Pi

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`, y listo el equipo estará adaptado para los requerimientos del algoritmo



```

pi@raspberrypi:~$ ds64-shell
Connected to machine debian-buster-64. Press ^] three times within 1s to exit session.
/usr/bin/env: «node»: No existe el fichero o el directorio
nvm is not compatible with the npm config "prefix" option: currently set to ""
Run `nvm use --delete-prefix v14.17.0 --silent` to unset it.
pi@debian-buster-64:~$

```


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>.

```
pi@debian-buster-64:~$ git clone https://github.com/xmrig/xmrig.git
Clonando en 'xmrig'...
remote: Enumerating objects: 23682, done.
remote: Counting objects: 100% (451/451), done.
remote: Compressing objects: 100% (237/237), done.
remote: Total 23682 (delta 250), reused 343 (delta 214), pack-reused 23231
Recibiendo objetos: 100% (23682/23682), 9.69 MiB | 720.00 KiB/s, listo.
Resolviendo deltas: 100% (17467/17467), listo.
```

Figura 45. Terminal Raspberry Pi OS mediante Windows – clonando repositorio de software minador

En este punto se tiene el minador en nuestro equipo con todas las dependencias que necesita el minador, debemos entrar 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.

```
pi@debian-buster-64:~$ cd xmrig
pi@debian-buster-64:~/xmrig$ mkdir build
pi@debian-buster-64:~/xmrig$ cd build
pi@debian-buster-64:~/xmrig/build$ cmake ..
-- The C compiler identification is GNU 8.3.0
-- The CXX compiler identification is GNU 8.3.0
-- Check for working C compiler: /usr/bin/cc
-- Check for working C compiler: /usr/bin/cc -- works
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Detecting C compile features
-- Detecting C compile features - done
-- Check for working CXX compiler: /usr/bin/c++
-- Check for working CXX compiler: /usr/bin/c++ -- works
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Detecting CXX compile features
-- Detecting CXX compile features - done
```

Figura 46. Terminal Raspberry Pi OS mediante Windows – Creando ejecutable del software minador

Listo el ejecutable, se procede a compilar para poder concluir con la configuración del software minador, el comando para compilar en los sistemas basados en Linux es `make`.

```

pi@debian-buster-64:~/xmrig$ make
Scanning dependencies of target ethash
[ 0%] Building C object src/3rdparty/libethash/CMakeFiles/ethash.dir/ethash_internal.c.o
[ 1%] Building C object src/3rdparty/libethash/CMakeFiles/ethash.dir/keccakF800.c.o
[ 1%] Linking C static library libethash.a
[ 1%] Built target ethash
Scanning dependencies of target argon2
[ 1%] Building C object src/3rdparty/argon2/CMakeFiles/argon2.dir/lib/argon2.c.o
[ 1%] Building C object src/3rdparty/argon2/CMakeFiles/argon2.dir/lib/core.c.o
[ 2%] Building C object src/3rdparty/argon2/CMakeFiles/argon2.dir/lib/encoding.c.o
[ 2%] Building C object src/3rdparty/argon2/CMakeFiles/argon2.dir/lib/gkcat.c.o
[ 3%] Building C object src/3rdparty/argon2/CMakeFiles/argon2.dir/lib/impl-select.c.o
[ 3%] Building C object src/3rdparty/argon2/CMakeFiles/argon2.dir/lib/blake2/blake2.c.o
[ 3%] Building C object src/3rdparty/argon2/CMakeFiles/argon2.dir/arch/generic/lib/argon2-arch.c.o
[ 4%] Linking C static library libargon2.a
[ 4%] Built target argon2
Scanning dependencies of target xmrig
[ 4%] Building CXX object CMakeFiles/xmrig.dir/src/3rdparty/fmt/format.cc.o
[ 5%] Building CXX object CMakeFiles/xmrig.dir/src/backend/cpu/CpuLaunchData.cpp.o
[ 5%] Building CXX object CMakeFiles/xmrig.dir/src/backend/opencl/kernels/nv/HashesKernel.cpp.o
[ 6%] Building CXX object CMakeFiles/xmrig.dir/src/base/crypto/Algorithm.cpp.o
[ 6%] Building CXX object CMakeFiles/xmrig.dir/src/base/crypto/Coin.cpp.o
[ 6%] Building CXX object CMakeFiles/xmrig.dir/src/base/crypto/keccak.cpp.o
[ 7%] Building CXX object CMakeFiles/xmrig.dir/src/base/crypto/sha3.cpp.o
[ 7%] Building CXX object CMakeFiles/xmrig.dir/src/base/io/Async.cpp.o
[ 8%] Building CXX object CMakeFiles/xmrig.dir/src/base/io/Console.cpp.o
[ 8%] Building CXX object CMakeFiles/xmrig.dir/src/base/io/Env.cpp.o
[ 9%] Building CXX object CMakeFiles/xmrig.dir/src/base/io/json/Json.cpp.o
[ 9%] Building CXX object CMakeFiles/xmrig.dir/src/base/io/json/JsonChain.cpp.o
[ 9%] Building CXX object CMakeFiles/xmrig.dir/src/base/io/json/JsonRequest.cpp.o
[10%] Building CXX object CMakeFiles/xmrig.dir/src/base/io/log/backends/ConsoleLog.cpp.o

```

Figura 47. Terminal Raspberry Pi OS mediante Windows – Compilando ejecutable del software minador

3.5.4. Ejecución de la minería de criptodivisas y pruebas de uso

3.5.4.1. Ejecución de la minería de criptodivisas

Una vez el software minador previamente instalado, es cuestión de 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`.

```

pi@raspberrypi:~$ ds64-shell
Connected to machine debian-buster-64. Press ^] three times within 1s to exit session.
/usr/bin/env: «node»: No existe el fichero o el directorio
nvm is not compatible with the npm config "prefix" option: currently set to ""
Run `nvm use --delete-prefix v14.17.0 --silent` to unset it.
pi@debian-buster-64:~$ cd xmrig
pi@debian-buster-64:~/xmrig$ cd build
pi@debian-buster-64:~/xmrig/build$

```

Figura 48. Terminal Raspberry Pi OS mediante Windows – Ingreso al software

En este punto solo falta ingresar los datos al software minador para que se ejecute, estos deben ser ingresados en un orden específico detallado y se pueden obtener desde la página oficial del software minador solo debemos ingresar la dirección de nuestro 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 xmrrpool.eu:9999 -u *dirección del wallet* -k -tls`. El

único cambio que se efectuara es el puerto 5555 en el cual la dificultad del minado se ajustara a la capacidad del hardware.



Figura 49. Página oficial xmrig – Guía de ingreso de datos al software minador

```
pi@debian-buster-64:~/xmrig$ ./xmrig --donate-level 1 -o xmrpool.eu:5555 -u 43mHnDKUramUnaB2CLsDvD1cgV6z6k5TR6NsR1jyyxucqE6GCTnpax1UNgmPHJ3YY2viTukW4UqXUjQoZknzYcDyocBe
```

Figura 50. Terminal Raspberry Pi OS mediante Windows – instrucciones de minado

Con la ejecución de estas instrucciones comenzará el proceso de minería de criptodivisas para posteriormente evaluar su factibilidad.

```
pi@debian-buster-64:~/xmrig$ ./xmrig --donate-level 1 -o xmrpool.eu:5555 -u 43mHnDKUramUnaB2CLsDvD1cgV6z6k5TR6NsR1jyyxucqE6GCTnpax1UNgmPHJ3YY2viTukW4UqXUjQoZknzYcDyocBe
* ABOUT      XMRig/6.12.1 gcc/8.3.0
* LIBS       libuv/1.24.1 OpenSSL/1.1.1d hwloc/1.11.12
* HUGE PAGES supported
* 1GB PAGES  unavailable
* CPU        ARM Cortex-A72 (1) 64-bit -483
             L2:0.0 MB L3:0.0 MB 4C/4T NUMA:1
* MEMORY     0.5/3.7 GB (14%)
* DONATE     1%
* POOL #1    xmrpool.eu:5555 algo auto
* COMMANDS   hashrate, pause, resume, results, connection
* OPENCL     disabled
* CLUDA      disabled
2021-08-28 19:06:54.199] net      use pool xmrpool.eu:5555 51.89.217.80
2021-08-28 19:06:54.200] net      new job from xmrpool.eu:5555 diff 50000 algo rx/0 height 2437324
2021-08-28 19:06:54.200] cpu      use argon2 implementation default
2021-08-28 19:06:55.400] randomx  init dataset algo rx/0 (4 threads) seed 872505f0da609445...
2021-08-28 19:06:55.481] randomx  allocated 2336 MB (2088+256) huge pages 0% 0/1168 +31T (1 ms)
2021-08-28 19:06:55.825] net      new job from xmrpool.eu:5555 diff 50000 algo rx/0 height 2437324
2021-08-28 19:07:26.770] net      new job from xmrpool.eu:5555 diff 50000 algo rx/0 height 2437325
```

Figura 51. Terminal Raspberry Pi OS mediante Windows – minería de criptodivisas en ejecución

Como se muestra en la imagen anterior, el software reconoce automáticamente el procesador del equipo, arquitectura que este caso será 64 bits ya que el sistema está dentro de la máquina virtual de Raspberry Pi OS, la memoria RAM disponible y RAM total. En este punto se tiene ciertos comandos que ayudaran a tener una idea más clara de cómo funciona el sistema, el primero es el hashrate que en el capítulo 2 se detalló como el número de hashes que resuelve el equipo por segundo, y dentro del software este nos proveerá un desglose del hashrate de cada uno de los núcleos del procesador, y sus promedios en diferentes tiempos, dándonos un promedio final de la suma del hashrate de todos los núcleos.

CPU #	AFFINITY	10s H/s	60s H/s	15m H/s
0	0	15.35	16.35	16.29
1	1	16.19	15.38	15.42
2	2	15.77	15.87	15.76
3	3	16.19	15.73	15.86
-	-	63.49	63.33	63.33

Figura 52. Terminal Raspberry Pi OS mediante Windows – comando hashrate del software minador

El comando connection nos entregara información detallada de nuestra conexión, el pool de minería que estemos usando, el algoritmo en nuestro caso RandomX y varios detalles adicionales.

```
- CONNECTION
* pool address      xmrpool.eu:5555 (51.89.217.80)
* algorithm         rx/0
* difficulty         50000
* ping time         207ms
* connection time   44s
```

Figura 53. Terminal Raspberry Pi OS mediante Windows – comando connection del software minador

El comando results entregara diferentes valores que se han presentado durante el tiempo que lleva ejecutada la minería, 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 sería 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.

```
- RESULTS
* accepted          16 (100.0%)
* pool-side hashes 153600 avg 9600
* difficulty         9600
* avg result time   241.0s
- TOP 10
# | DIFFICULTY | EFFORT % |
1 |    650937 |    23.60 |
2 |    637827 |    24.08 |
3 |    498999 |   307.82 |
4 |    401555 |   382.52 |
5 |    311099 |   493.75 |
6 |    239330 |   641.87 |
7 |    166077 |   924.91 |
8 |    148544 |  1034.06 |
9 |    143355 |  1071.50 |
10 |   123344 |  1245.34 |
```

Figura 54. Terminal Raspberry Pi OS mediante Windows – comando resultados del software minador

3.5.4.2. Pruebas de uso

3.5.4.2.1. Pruebas en Raspberry Pi

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, a continuación, se detalla las características.

Tabla 23.

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)

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza


```

@debian-buster-64:~$ ./xmrig --donate-level 1 -o xmrpool.eu:5555 -u 43nHmDKUramUnaB2CLsDvD1cgV6z6kSTR6NsR1jyyxucqE6GCTmpax1UNgmwpHJ3YY2viTukW4UqXUjqqZknzYcDyocBe
1jyyxucqE6GCTmpax1UNgmwpHJ3YY2viTukW4UqXUjqqZknzYcDyocBe
* ABOUT      XMRig/6.12.1 gcc/8.3.0
* LIBS       libuv/1.24.1 OpenSSL/1.1.1d hwloc/1.11.12
* HUGE PAGES supported
* 1GB PAGES  unavailable
* CPU        ARM Cortex-A72 (1) 64-bit -480
*            L2:0.0 MB L3:0.0 MB 4C/4T NUMA:1
* MEMORY     0.6/3.7 GB (15%)
* DONATE     1%
* POOL #1    xmrpool.eu:5555 algo auto
* COMMANDS   Hashrate, Pause, Resume, results, connection
* OPENCL     disabled
* CUDA       disabled
2021-08-29 14:34:29.394] net      use pool xmrpool.eu:5555 51.89.217.88
2021-08-29 14:34:29.394] net      new job from xmrpool.eu:5555 diff 50000 algo rx/0 height 2437915
2021-08-29 14:34:29.394] cpu      use argon2 implementation default
2021-08-29 14:34:30.594] randomx  init dataset algo rx/0 (4 threads) seed 872585fbdad609445...
2021-08-29 14:34:30.594] randomx  allocated 2336 MB (2080+256) huge pages 0K 0/1100 +327 (1 ms)
2021-08-29 14:34:43.823] net      new job from xmrpool.eu:5555 diff 50000 algo rx/0 height 2437915
2021-08-29 14:35:02.583] randomx  dataset ready (32389 ms)
2021-08-29 14:35:02.904] cpu      use profile rx (4 threads) scratchpad 2048 KB
2021-08-29 14:35:02.910] cpu      READY threads 4/4 (4) huge pages 0K 0/4 memory 8192 KB (6 ms)
2021-08-29 14:35:47.930] net      new job from xmrpool.eu:5555 diff 25000 algo rx/0 height 2437915
2021-08-29 14:35:50.387] cpu      accepted (1/0) diff 25000 (197 ms)
2021-08-29 14:35:51.669] net      new job from xmrpool.eu:5555 diff 25000 algo rx/0 height 2437916
2021-08-29 14:36:02.972] miner    speed 10s/60s/15m 98.84 n/a n/a H/s max 99.66 H/s
2021-08-29 14:36:32.441] cpu      accepted (2/0) diff 25000 (205 ms)


```

Figura 55. Terminal Raspberry Pi OS mediante Windows – Minería de criptodivisas inicio


Como se muestra en la **Figura 54**, el proceso de minería comenzó a las 14:34:29 del 29 de agosto del 2021, y el primer hashrate que entrega el software es de 98.84 H/s de media y de 99.66 H/s de máximo lo cual nos da una idea de cuál es la capacidad del hardware, y que se podrá revisar una vez el proceso se ejecute durante algunas horas. Para monitorizar las criptodivisas minadas se debe utilizar la página del pool de minería, e ingresando la dirección del wallet se visualizará esa información.

Your Mining Statistics & Monero XMR Mining Payment History


43rHmDKUramUnaB2CLsDvD1cgV6z6kSTR6NsR1jyyxucqE6GCTmpax1UNgmwpHJ3YY2viTukW4UqXUjqqZknzYcDyocBe




Pending Balance: 0.000069539894 XMR




Last Block Reward: 0.000004516407 XMR




Total Paid: 0.000000000000 XMR



Last Share Submitted: Now ...



Total Hashes Submitted: 26,179,307



Hash Rate: 83.33 H/sec

Your Workers / Rigs






 Worker / Rig ID	 Hash Rate	 Accepted Hashes	 Expired Hashes	 Info
default	83.33 H/s	26,062,747	116,560	

Figura 55. Tablero de información de xmrpool.eu – Información de criptomonedas minadas inicio

Al observar el tablero se obtiene información muy interesante, de la cual 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, 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.

```

pi@debian-buster-64: ~/xmrig/build
[2021-08-29 17:27:33.787] cpu      accepted (91/0) diff 9600 (211 ms)
[2021-08-29 17:28:12.680] miner   speed 10s/60s/15m 99.04 99.11 99.12 H/s max 99.89 H/s
[2021-08-29 17:28:45.686] cpu      accepted (92/0) diff 9600 (199 ms)
[2021-08-29 17:28:50.405] net      new job from xmrigpool.eu:5555 diff 9600 algo rx/0 height 2438013
[2021-08-29 17:29:06.595] net      new job from xmrigpool.eu:5555 diff 9600 algo rx/0 height 2438014
[2021-08-29 17:29:12.755] miner   speed 10s/60s/15m 99.01 99.12 99.12 H/s max 99.89 H/s
[2021-08-29 17:29:14.220] cpu      accepted (93/0) diff 9600 (191 ms)
[2021-08-29 17:29:47.953] cpu      accepted (94/0) diff 9600 (197 ms)
[2021-08-29 17:30:03.725] cpu      accepted (95/0) diff 9600 (203 ms)
[2021-08-29 17:30:12.830] miner   speed 10s/60s/15m 99.24 99.29 99.13 H/s max 99.89 H/s
[2021-08-29 17:31:12.883] miner   speed 10s/60s/15m 99.61 99.29 99.14 H/s max 99.89 H/s
[2021-08-29 17:31:37.219] net      new job from xmrigpool.eu:5555 diff 9600 algo rx/0 height 2438014
[2021-08-29 17:32:12.929] miner   speed 10s/60s/15m 99.31 99.10 99.14 H/s max 99.89 H/s
[2021-08-29 17:32:29.854] net      new job from xmrigpool.eu:5555 diff 9600 algo rx/0 height 2438015
[2021-08-29 17:32:30.595] cpu      accepted (96/0) diff 9600 (205 ms)
[2021-08-29 17:33:12.973] miner   speed 10s/60s/15m 99.39 99.02 99.14 H/s max 99.89 H/s
[2021-08-29 17:33:41.811] cpu      accepted (97/0) diff 9600 (202 ms)
[2021-08-29 17:34:13.024] miner   speed 10s/60s/15m 99.31 99.14 99.13 H/s max 99.89 H/s
[2021-08-29 17:34:41.646] net      new job from xmrigpool.eu:5555 diff 9600 algo rx/0 height 2438016
  
```

Figura 57. Terminal Raspberry Pi OS mediante Windows – Minería de criptodivisas fin

El proceso de minado termino a las 17:34:41 del 29 de agosto del 2021, y 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 proceso 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.

CPU #	AFFINITY	10s H/s	60s H/s	15m H/s
0	0	24.82	24.79	24.76
1	1	24.72	24.65	24.62
2	2	24.93	24.92	24.86
3	3	24.93	24.94	24.89
-	-	99.39	99.29	99.14

Figura 58. Terminal Raspberry Pi OS mediante Windows – Minería de criptodivisas comando hashrate de final de minería

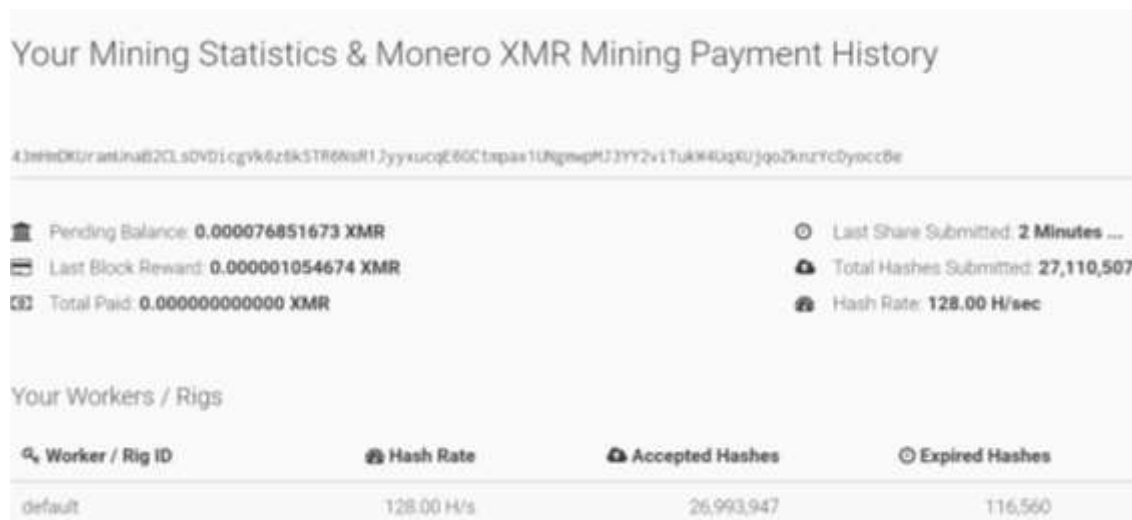


Figura 59. Tablero de información de xmrpool.eu – Información de criptomonedas minadas fin

Luego de que el proceso de minado se detuvo y ejecuta el comando hashrate se obtuvo que el hashrate promedio de los últimos 15 minutos es 99.14 H/s, que será el definitivo, además se obtuvo 0.000076851673 XMR luego de 3 horas de minado, al cual debe restarse lo que había inicialmente en el pool y se obtendrá lo que el proceso logro minar, se detallará a continuación.

Tabla 24.

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

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Con esta información del proceso de minería se puede evaluar la factibilidad de esta, y sus capacidades frente a otros equipos.

3.5.4.2.2. Pruebas en equipo secundario

Para obtener un punto de comparación verificable es importante establecer la 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, a continuación, se detalla las características.

Tabla 25.

Características de equipo secundario

Modelo	Laptop Lenovo Flex 14
Procesador	AMD Ryzen 5 3500U 4 núcleos 8 hilos
Memoria RAM	12 GB
Memoria ROM	256 GB SSD
Consumo	65 watts/0.065 kW/h
Precio	\$850.00 (precio local)

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Se ejecuto la minería de criptodivisas en el equipo Windows, la cual se detalla en el anexo 2 y para tener una comparación justa, se ejecutó en un lapso de alrededor de 3 horas al igual que en Raspberry Pi, los detalles a continuación.

Tabla 26.

Minería en equipo secundario

Tiempo de actividad	3 horas (11:03 del 29/08/2021 hasta 14:03 del 29/08/2021)
Cantidad de XMR inicio	0.000059939883 XMR
Cantidad de XMR fin	0.000069539894 XMR
XMR minado	0.000009600011 XMR
Promedio de hashrate	544 H/s
Consumo	65 watts

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Con esta información se puede contrastar los resultados obtenidos por Raspberry Pi y analizar su factibilidad.

3.5.5. Factibilidad de la minería de criptodivisas mediante Raspberry Pi

Luego de ejecutar la minería en Raspberry Pi y en un equipo de uso regular, se plantea mediante una comparativa que tan factible es la minería de criptodivisas en dicho hardware, se tratara en varios ámbitos para luego hacer un análisis general de su factibilidad.

3.5.5.1. Factibilidad del hardware

En este punto se compara el rendimiento que entregan ambos hardware, cual es la diferencia y la comparación respectiva.

Tabla 27.

Comparativa del hardware

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

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Como se puede observar en la **Tabla27** el equipo secundario con su hardware nos está entregando alrededor de 31% más de rendimiento de minado, solo teniendo en cuenta esta característica.

Analizando estos datos y teniendo en contexto la diferencia de potencia entre los hardware a considerar, podemos declarar que la factibilidad de la minería de criptodivisas en Raspberry Pi presenta un nivel regular de potencia que a pesar de ser inferior al del equipo secundario, su naturaleza compacta y de bajo consumo abre la puerta a ser considerado como un equipo interesante.

3.5.5.2. Factibilidad económica

En este apartado se compara el aspecto económico que implica la adquisición de cada uno de los hardware, y el beneficio que puede entregar en un tiempo determinado.

Tabla 28.**Factores económicos**

Hardware	Precio	XMR (3 horas)
Raspberry Pi	\$ 80.00	0.000007311779 XMR
Equipo secundario	\$ 850.00	0.000009600011 XMR

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Gracias a la **Tabla 28** podemos ver que el equipo secundario es al menos 10,6 veces más costoso que Raspberry Pi, por lo tanto, con el costo del equipo secundario se podría conseguir 0.0000775048574 XMR en un lapso de 3 horas. El valor actual de Monero es de \$291.86, por lo tanto, el equipo secundario no estaría entregando \$0.0028, y las Raspberry pi que se pueden obtener con el valor del equipo secundario podrían entregar alrededor de \$0.0226 lo cual implica 8 veces más XMR que el equipo secundario, a continuación, se detallaran los valores que se lograrían en un mes para tener una idea más clara.

Tabla 29.**Comparativa económica**

Hardware	XMR (1 mes)	Valor
Raspberry Pi	0.05580349732 XMR	\$ 16.28
Equipo secundario	0.0069120079 XMR	\$ 2.01

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

Con esta información se puede analizar que la factibilidad de la minería de criptodivisas en el ámbito económico frente al equipo secundario es de al menos 8.1 veces mayor, esto quiere decir que con el poder adquisitivo con el que se puede comprar el equipo secundario se compraría hasta 10,6 veces Raspberry Pi de las cuales se obtendrá 8.1 veces más XMR que del equipo secundario. Esto es realmente positivo y demuestra que las características de simplicidad y eficiencia en la minería son mucho más rentables que equipos de uso común.

3.5.5.3. Factibilidad energética

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 30.

Comparativa energética

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

Información adaptada de los repositorios y artículos investigados. Elaborado por Cristhian Loayza

En vista de la información obtenida se puede observar que Raspberry Pi consume 10.8 menos energía que el equipo secundario, y nos entregaría la misma cantidad de activo que el equipo secundario con solo 7.9 watts siendo al menos 8.22 más eficiente en el minado, razones claras de ser una opción energética más sostenible, sin renunciar a una red segura y descentralizada, entregando a una cantidad más significativa de usuarios la capacidad de minar debido al valor reducido del equipo, verificando su factibilidad energética frente a la minería tradicional.

3.5.5.4. Factibilidad general

Luego de analizar la factibilidad en diferentes ámbitos se puede decir de forma general que es altamente factible la minería de criptodivisas en Raspberry Pi, las múltiples ventajas dentro del ámbito económico permiten adquirir hardware que en su conjunto es mucho más rentable que el tradicional. Su concepto de simplicidad frente a equipos comunes permite un consumo energético considerablemente menor entregando una minería sostenible sin renunciar a la seguridad que este proceso aporta a la red, entrega una respuesta a las actuales críticas del proceso de minado mundial por el elevado derroche energético y centralización de la red. Frente a estos factores juntos es claro que la factibilidad del proceso de minado en Raspberry Pi es altamente factible y sus ventajas abren la puerta a un proceso de minería mucho más amigable.

3.6. Conclusiones y recomendaciones

3.6.1. 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.

3.6.2. Recomendaciones

- 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 ha que el valor de estas puede crecer incluso varios cientos de veces en tiempos cortos, entregando un beneficio al usuario que realizo el análisis.
- Ejecutar la minería en un clúster de Raspberry Pi para evaluar el crecimiento del rendimiento de los equipos al trabajar en conjunto.

- Investigar o crear un script de automatización del proceso de minería en Raspberry Pi, que comience el proceso al encender el equipo mejorando sus procesos.
- Se recomienda agregar un kit de refrigeración al equipo para aumentar su rendimiento y cuidar su vida útil.

ANEXOS

ANEXO 1

Preguntas de la encuesta

- ¿Conoce lo que es una criptomoneda?
Sí/No
- ¿Cuál de las siguientes criptomonedas conoce?
Bitcoin/ Ethereum/ Dogecoin/ Monero/ Otro
- ¿Conoce usted algo del proceso de minería de criptomonedas?
Sí/No
- ¿Cuál de estos algoritmos criptográficos de minería conoce?
SHA256/ Ethash/ Scrypt/ RandomX/ Ninguno/ Otro
- ¿Cuál de los siguientes ordenadores de bajo costo y tamaño reducido conoce?
Raspberry Pi/ Orange Pi/ ODDYSEY/ Nova Pi/ Otro
- ¿Sabía que se puede minar criptomonedas con Raspberry Pi?
Sí/No
- ¿Cuál de estas cualidades considera favorables de Raspberry Pi?
Tamaño compacto/ Bajo consumo energético/ Precio accesible/ Comunidad Mundial/
Otra
- ¿Sabía que el uso de hardware para minería de criptomonedas requiere un elevado consumo energético?
Sí/No

ANEXO 2

Minería de criptodivisas en equipo Windows y prueba de uso:

1. En la página del software minador <https://xmrig.com/miner>, elegiremos el apartado download y luego nuestro sistema operativo en este caso Windows

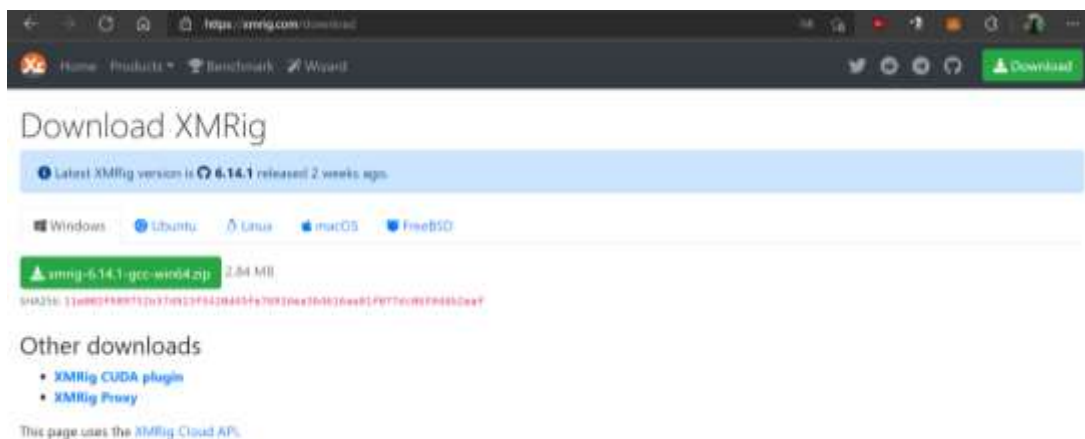


Figura 60. Página web xmrig download – selección de sistema operativo

2. Comenzará la descarga automáticamente, una vez terminada debemos descomprimir la carpeta que se encuentra dentro y tendremos listo el software minador.

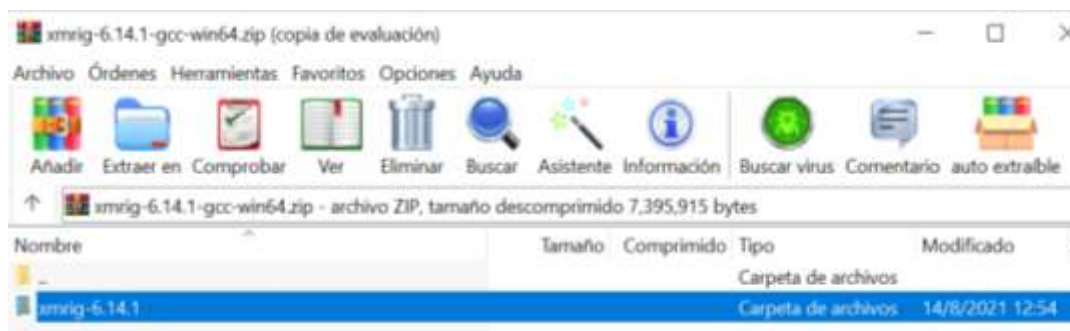


Figura 61. Xmrig software – Descomprimir carpeta

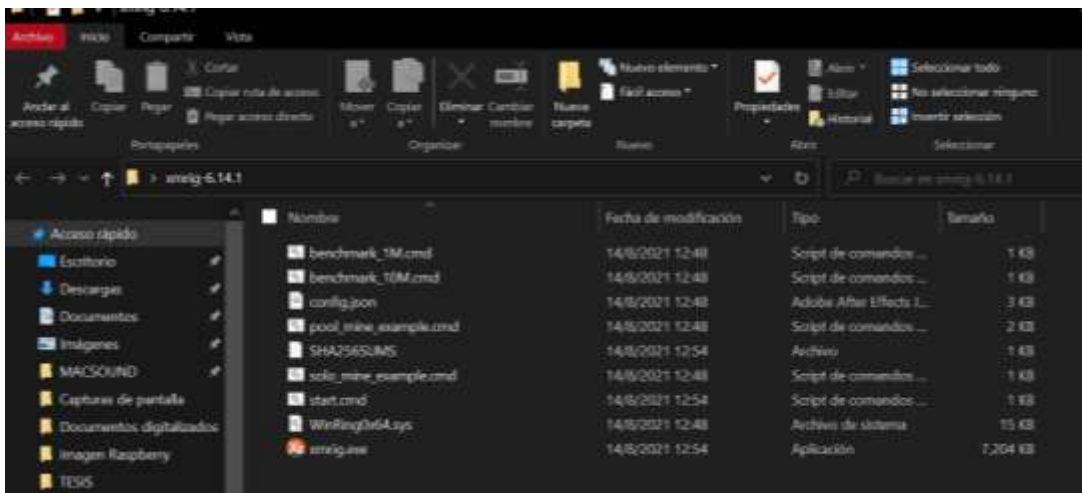


Figura 62. Xmrig carpeta – recursos y ejecutable del software minador

3. En este punto debemos ir a la página de xmrig y crear un archivo config.json que será reemplazado por el que está dentro de la carpeta descomprimida, este archivo tendrá nuestra información, al igual que la línea de datos usada en Raspberry Pi OS.

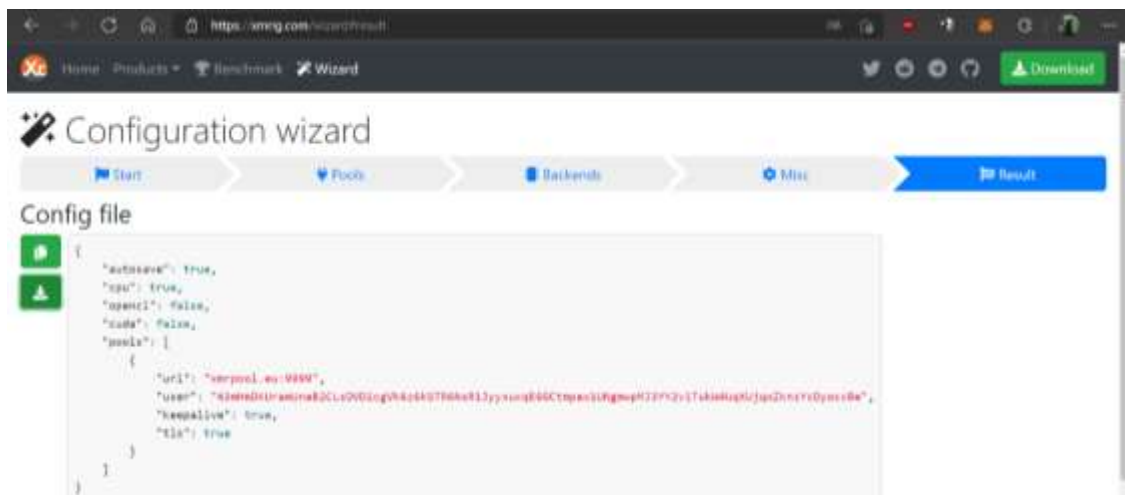


Figura 63. Página web xmrig wizard– archivo config.json

4. Con el cambio de este archivo dentro de la carpeta xmrig, solo debemos abrir el ejecutable y listo la minería se ejecutará de manera automática. Minería comienza 11:03 del 29/08/2021 hasta 14:03 del 29/08/2021.

```

XMRig 6.14.1
* ABOUT      XMRig/6.14.1 gcc/10.1.0
* LIBS       libuv/1.41.0 OpenSSL/1.1.1k hwloc/2.4.1
* HUGE PAGES permission granted
* 1GB PAGES  unavailable
* CPU        AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx (1) 64-bit AES VM
             L2:2.0 MB L3:4.0 MB 4C/8T ALMA:1
* MEMORY     7.3/9.9 GB (74%)
             DIMM_A0: 4 GB DDR4 @ 2400 MHz 4ATF51264HZ-2G6E1
             DIMM_B0: 8 GB DDR4 @ 2400 MHz 99U5700-02B_A00G
* MOTHERBOARD LENOVO - 8155
* DONATE     1%
* ASSEMBLY   auto:ryzen
* POOL #1    xmrpool.eu:9999 algo auto
* COMMANDS   hashrate, pause, resume, results, connection
* OPENCL     disabled
* CUDA       disabled

[2021-08-29 11:03:33.024] net      use pool xmrpool.eu:9999 TLsv1.3 51.89.217.88
[2021-08-29 11:03:33.025] net      fingerprint (SHA-256): "79c81f656ff4da7359b7df8648856f2d47a511863c852afdb1768682b9f7fa81"
[2021-08-29 11:03:33.026] net      new job from xmrpool.eu:9999 diff 50000 algo rx/0 height 2437785 (12 tx)
[2021-08-29 11:03:33.026] cpu       use argon2 implementation AVX2
[2021-08-29 11:03:33.027] msr       to access MSR registers Administrator privileges required.
[2021-08-29 11:03:33.027] msr       FAILED TO APPLY MSR MNO, HASHRATE WILL BE LOW
[2021-08-29 11:03:33.028] randomx   init dataset algo rx/0 (8 threads) seed 872585fbd609445...
[2021-08-29 11:03:33.226] randomx   allocated 2336 MB (2000+256) huge pages 0K/1168 +JIT (198 ms)
[2021-08-29 11:03:38.795] net      new job from xmrpool.eu:9999 diff 50000 algo rx/0 height 2437786 (10 tx)
[2021-08-29 11:03:41.535] randomx   dataset ready (8389 ms)
[2021-08-29 11:03:41.535] cpu       use profile rx (2 threads) scratchpad 2048 KB
[2021-08-29 11:03:41.581] cpu       READY threads 2/2 (1) huge pages 100% 2/2 memory 4096 KB (46 ms)
[2021-08-29 11:04:24.715] net      new job from xmrpool.eu:9999 diff 25490 algo rx/0 height 2437786 (10 tx)
[2021-08-29 11:04:26.145] cpu       accepted (1/0) diff 25490 (192 ms)
[2021-08-29 11:04:29.551] cpu       accepted (2/0) diff 25490 (216 ms)
[2021-08-29 11:04:42.839] miner     speed 10s/60s/15m 550.8 548.7 n/a M/s max 596.1 M/s

```

Figura 64. Xmrigr ejecutado en Windows– minería iniciada

```

XMRig 6.14.1
[2021-08-29 13:56:52.795] cpu       accepted (412/0) diff 17000 (248 ms)
[2021-08-29 13:57:10.946] miner     speed 10s/60s/15m 596.6 595.1 593.3 M/s max 618.0 M/s
[2021-08-29 13:57:15.334] cpu       accepted (413/0) diff 17000 (185 ms)
[2021-08-29 13:57:27.709] cpu       accepted (414/0) diff 17000 (193 ms)
[2021-08-29 13:57:43.236] net      new job from xmrpool.eu:9999 diff 11005 algo rx/0 height 2437895 (5 tx)
[2021-08-29 13:57:44.442] cpu       accepted (425/0) diff 11005 (195 ms)
[2021-08-29 13:58:02.414] cpu       accepted (426/0) diff 11005 (214 ms)
[2021-08-29 13:58:12.204] miner     speed 10s/60s/15m 609.7 607.3 607.7 M/s max 618.0 M/s
[2021-08-29 13:58:39.401] net      new job from xmrpool.eu:9999 diff 11005 algo rx/0 height 2437896 (27 tx)
[2021-08-29 13:58:43.571] miner     speed 10s/60s/15m 613.6 610.8 608.8 M/s max 618.0 M/s
[2021-08-29 13:58:53.275] net      new job from xmrpool.eu:9999 diff 9600 algo rx/0 height 2437896 (27 tx)
[2021-08-29 13:59:34.447] cpu       accepted (417/0) diff 9600 (217 ms)
[2021-08-29 13:59:51.510] cpu       accepted (418/0) diff 9600 (197 ms)
[2021-08-29 13:59:56.359] cpu       accepted (419/0) diff 9600 (230 ms)
[2021-08-29 14:00:14.837] miner     speed 10s/60s/15m 604.6 603.8 600.2 M/s max 618.0 M/s
[2021-08-29 14:00:28.280] net      new job from xmrpool.eu:9999 diff 14400 algo rx/0 height 2437896 (27 tx)
[2021-08-29 14:01:15.995] miner     speed 10s/60s/15m 577.4 582.5 580.0 M/s max 618.0 M/s
[2021-08-29 14:01:23.289] net      new job from xmrpool.eu:9999 diff 9600 algo rx/0 height 2437896 (27 tx)
[2021-08-29 14:01:32.829] cpu       accepted (430/0) diff 9600 (291 ms)
[2021-08-29 14:01:40.782] net      new job from xmrpool.eu:9999 diff 9600 algo rx/0 height 2437896 (68 tx)
[2021-08-29 14:01:41.650] cpu       accepted (431/0) diff 9600 (610 ms)
[2021-08-29 14:02:04.335] cpu       accepted (432/0) diff 9600 (199 ms)
[2021-08-29 14:02:06.077] cpu       accepted (433/0) diff 9600 (276 ms)
[2021-08-29 14:02:10.588] cpu       accepted (434/0) diff 9600 (217 ms)
[2021-08-29 14:02:17.120] miner     speed 10s/60s/15m 611.1 605.5 599.3 M/s max 618.0 M/s
[2021-08-29 14:02:17.127] cpu       accepted (435/0) diff 9600 (218 ms)
[2021-08-29 14:02:18.335] net      new job from xmrpool.eu:9999 diff 14400 algo rx/0 height 2437896 (68 tx)
[2021-08-29 14:02:25.454] net      new job from xmrpool.eu:9999 diff 14400 algo rx/0 height 2437897 (3 tx)
[2021-08-29 14:02:45.606] cpu       accepted (436/0) diff 14400 (190 ms)
[2021-08-29 14:02:46.405] cpu       accepted (437/0) diff 14400 (213 ms)
[2021-08-29 14:02:55.770] net      new job from xmrpool.eu:9999 diff 14400 algo rx/0 height 2437898 (10 tx)
[2021-08-29 14:03:13.308] net      new job from xmrpool.eu:9999 diff 21600 algo rx/0 height 2437898 (10 tx)
[2021-08-29 14:03:18.270] miner     speed 10s/60s/15m 592.3 594.3 590.7 M/s max 618.0 M/s
[2021-08-29 14:03:48.849] net      new job from xmrpool.eu:9999 diff 21600 algo rx/0 height 2437899 (10 tx)

```

Figura 65. Xmrigr ejecutado en Windows– minería finalizada

5. Para finalizar el proceso ejecutamos el comando hashrate para visualizar el promedio del proceso, y revisar en la página del pool la cantidad de criptodivisa que se ha minado.

CPU #	AFFINITY	10s H/s	60s H/s	15m H/s
0	0	269.8	263.9	n/a
1	2	287.7	280.4	n/a
-	-	557.5	544.3	n/a

Figura 66. Xmrig ejecutado en Windows– Comando hashrate

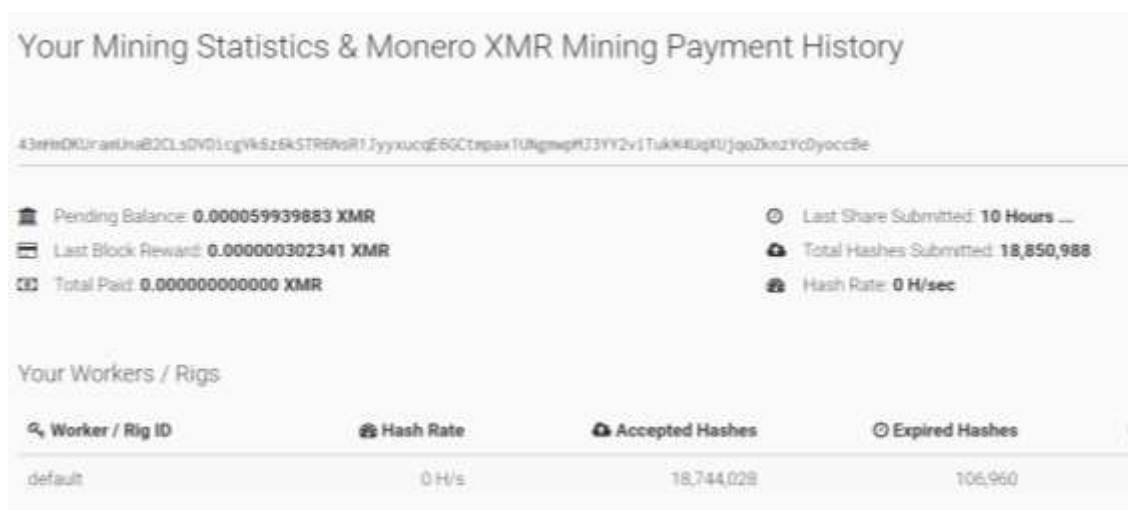


Figura 67. Tablero de información de xmrpool.eu – Información de criptomonedas minadas inicio

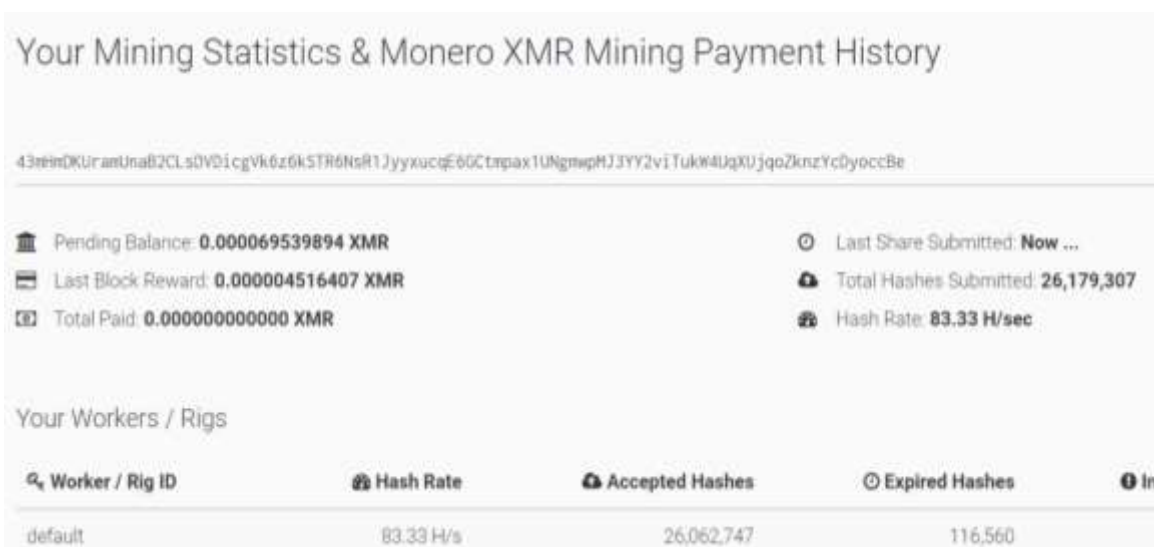


Figura 68. Tablero de información de xmrpool.eu – Información de criptomonedas minadas fin

Bibliografía

- 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. Obtenido de https://www.researchgate.net/publication/339170604_Implementation_of_Bitcoin_Mining_using_Raspberry_Pi
- Alonso Serrano, A., García Sanz, L., León Rodrigo, I., García Gordo, E., Gil Álvaro, B., & Ríos Brea, L. (2016). *Métodos de investigación de enfoque experimental*. Recuperado el 16 de Junio de 2021, de Postgradoune: <https://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/10.pdf>
- Alonso, R. (2021). Todo lo que necesitas saber sobre los procesadores ARM. Obtenido de <https://hardzone.es/tutoriales/componentes/procesador-arm/>
- Alsunaidi, S., & Alhaidari, F. (2019). Una encuesta de algoritmos de consenso para Tecnología Blockchain. Arabia Saudita. doi: 10.1109/ICCISci.2019.8716424
- Amores Martinez, A. (29 de 12 de 2020). Blockchain, Algoritmos de consenso. España. Obtenido de <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/127926/6/aamoresmTFM1220memoria.pdf>
- Bach, L. M., Mihaljevic, B., & Zagar, M. (2018). Comparative Analysis of Blockchain Consensus Algorithms. Croacia. Obtenido de <https://ieeexplore.ieee.org/abstract/document/8400278>
- Barrezueta, H. D. (01 de Diciembre de 2016). *CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN*. Recuperado el 17 de Mayo de 2021, de DerechoEcuador.com: https://www.derechoecuador.com/uploads/content/2020/12/file_1606929530_1606929536.pdf
- BCE, B. C. (2018). *COMUNICADO OFICIAL SOBRE EL USO DEL BITCOIN*. Obtenido de <https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1028-comunicado-oficial-sobre-el-uso-del-bitcoin>

- Bonneau, J., & Heninger, N. (2020). Financial Cryptography and Data Security. *24th International Conference, FC 2020*, (págs. 523-530). Kinabalu. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-51280-4_28
- 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
- Caizapanta, M., Borja, E., & González, M. (Noviembre de 2018). Desarrollo de las criptomonedas en Ecuador, responsabilidad y riesgo. Quito, Pichincha, Ecuador. Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=7143990>
- Campaña Iza, X. M., & Zumba Sampedro, W. X. (2020). Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo. Quito. Obtenido de <http://www.dspace.uce.edu.ec/bitstream/25000/21832/1/T-UCE-0011-ICF-256.pdf>
- Chase, B., & MacBrough, E. (2018). Analysis of the XRP Ledger Consensus Protocol. Obtenido de <https://academy.bit2me.com/wp-content/uploads/2021/05/XRP-WHITEPAPER.pdf>
- Chen, L., Xu, L., Shah, N., Gao, Z., & Lu, Y. S. (2017). On Security Analysis of Proof-of-Elapsed-Time., (págs. 285-290). Houston. Obtenido de https://link.springer.com/chapter/10.1007/978-3-319-69084-1_19
- Coinmarketcap. (2021). Principales 100 Criptomonedas por capitalización de mercado. Obtenido de <https://coinmarketcap.com/es/>
- COIP. (10 de Febrero de 2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL*,. Recuperado el 17 de Mayo de 2021, de Ministerio de Defensa Nacional: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- CONSTITUCION DE LA REPUBLICA DEL ECUADOR. (20 de Octubre de 2008). *CONSTITUCION DE LA REPUBLICA DEL ECUADOR*. Recuperado el 17 de Mayo de 2021, de COSEDE: <https://www.cosede.gob.ec/wp-content/uploads/2019/08/CONSTITUCION-DE-LA-REPUBLICA-DEL-ECUADOR.pdf>
- Conway, L. (2021). Best Bitcoin Wallets. Obtenido de <https://www.investopedia.com/best-bitcoin-wallets-5070283>

- Dag, A., OsvikJoppe, W., BosDeian, S., & David, C. (2010). Fast Software AES Encryption. Obtenido de https://link.springer.com/chapter/10.1007/978-3-642-13858-4_5
- Domingo, C. (2018). BITCOIN, CRIPTOMONEDAS Y BLOCKCHAIN. España. Obtenido de https://pladlibroscl0.cdnstatics.com/libros_contenido_extra/38/37925_Bitcoin_Cripto_monedas_Y_Blockchain.pdf
- ECUADOR, C. N. (2000). *LEY ORGÁNICA DE DEFENSA DEL CONSUMIDOR*. Obtenido de <https://www.dpe.gob.ec/wp-content/dpetransparencia2012/literala/BaseLegalQueRigeLaInstitucion/LeyOrganicadeConsumidor.pdf>
- Flamur, B., Olivera, G.-T., & Emilija, M.-K. (2017). CRYPTOCURRENCIES – ADVANTAGES AND DISADVANTAGES. Obtenido de <https://js.ugd.edu.mk/index.php/JE/article/view/1933/1706>
- Gallardo, S. A., Gutiérrez, I. L., & Fuentes. (2008). Arquitectura en capas para el desarrollo de una aplicación basada en redes peer-to-peer. *Revista GTI*, 59-68.
- Gangonells, O. V. (2020). LA MINERÍA EN CRIPTOMONEDAS. Barcelona.
- Garay, J. M. (27 de Octubre de 2020). La seguridad cibernética en los adolescentes y su vulnerabilidad al hackeo. *Universidad de Murcia*. Recuperado el 28 de Abril de 2021, de https://www.um.es/documents/2918258/18875715/Escrita_CyT_IES+FLORIDABLANCA.pdf/118886e0-bf96-46f6-9034-0ff9f7af32a1
- Gaspar Garcia, J. (2016). *MÉTODOS DE INVESTIGACIÓN DE ENFOQUE EXPERIMENTAL*. Obtenido de <https://d1wqtxts1xzle7.cloudfront.net/55568285/Experimental-with-cover-page-v2.pdf?Expires=1628913083&Signature=L7NP6FyGTqGnuZ0bZ2mns92Rk~5mP-iaonjG-os1eAvliWHH~Vpu~PmHm3aMdaBeoIemrLEbj0uGqg1uUzrGYF3nFEFBZVNY0bb6TVJR28IwYRJ9-i~1fan6BIvW~N-LKZV54pesPj0onNo>
- Giannone, A. (2016). Investigación en Progreso: Método de Inclusión de. *Revista Latinoamericana de Ingenieria de Software*. doi:10.18294/relais.2016.252-254

- Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: market analysis and perspectives. *Journal of Industrial and Business Economics*, 1-18. Obtenido de <https://link.springer.com/article/10.1007%2Fs40812-019-00138-6>
- Hayes, A. (2021). Proof of Capacity (Cryptocurrency). Obtenido de <https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp>
- Jakobsson, M., & Juels, A. (1999). Proof of Work and Bread Pudding Protocols.
- King, S., & Nadal, S. (2012). PPCoin: criptomoneda de igual a igual con prueba de participación.
- Lansky, J. (2018). Possible State Approaches to Cryptocurrencies. *Possible State Approaches to Cryptocurrencies*. Czech Republic. doi:10.20470/jsi.v9i1.335
- LEY ORGANICA DE EDUCACION SUPERIOR. (12 de Octubre de 2010). *LEY ORGANICA DE EDUCACION SUPERIOR, LOES*. Recuperado el 31 de Mayo de 2021, de CES: <https://www.ces.gob.ec/documentos/Normativa/LOES.pdf>
- 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>
- López, A. (Abril de 2021). Criptografía: Qué son los algoritmos hash y para qué se utilizan. Obtenido de <https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/>
- López-Herrera, F., Macías Trejo, L. G., & de la Torre Torre, O. V. (2020). *Desempeño de ocho de las criptomonedas de mayor capitalización de mercado*. Morelia. Obtenido de <http://estocastica.azc.uam.mx/index.php/re/article/view/131>
- Mejia Jervis, T. (27 de Agosto de 2020). *Investigación descriptiva: características, técnicas, ejemplos*. Recuperado el 16 de Junio de 2021, de lifeder: <https://www.lifeder.com/investigacion-descriptiva/>
- Mejía-Castillo, H. J. (Julio de 2018). LA METODOLOGÍA DE INVESTIGACIÓN EVALUATIVA UNA ALTERNATIVA PARA LA VALORACIÓN DE PROYECTOS. Honduras. Obtenido de <https://www.lamjol.info/index.php/RIBCC/article/view/5945/5657>

- Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A brief survey of Cryptocurrency systems. Auckland, New Zealand. Obtenido de <https://ieeexplore.ieee.org/abstract/document/7906988>
- Nakamoto, S. (2008). Algunas palabras en Bitcoin que usted puede escuchar. Obtenido de <https://bitcoin.org/es/vocabulario#direccion>
- Nakamoto, S. (2008). *Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer*. Obtenido de https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf
- Orrala Cajas, K. D., & Chompol Pincay, L. E. (2017). ANÁLISIS DE LAS VENTAJAS DEL USO DEL BITCOIN EN EL ECUADOR. Guayaquil, Ecuador. Obtenido de <http://repositorio.ug.edu.ec/bitstream/redug/23667/1/B-CINT-PTG-N.211.Orrala%20Cajas%20Kattya%20De%20Los%20%c3%81ngeles.Chompol%20Pincay%20Luis%20Eduardo.pdf>
- Pérez-Subías, M. (2003). Redes P2P una nueva forma de almacenar y acceder a la información. Bit (141), Madrid, COIT/AEIT, octubre-noviembre, 28-30. *Bit*, 28-30.
- 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/>
- Preukschat, A., Kuchkovsky, C., Gómez Lardies, G., Díez García, D., & Molero, Í. (2017). Blockchain: la revolución industrial del internet. España. Obtenido de https://www.planetadelibros.cl/libros_contenido_extra/36/35615_Blockchain.pdf
- raspberrypi.org. (2019). Setting up your Raspberry Pi. Obtenido de <https://projects.raspberrypi.org/en/projects/raspberry-pi-setting-up>
- raspberrypi.org. (2020). *Configurando tu Raspberry Pi*. Obtenido de <https://www.raspberrypi.org/documentation/computers/getting-started.html#using-raspberry-pi-imager>
- REAL ACADEMIA ESPAÑOLA. (2001). Diccionario de la lengua española. *versión 23.4 en línea*(23). Recuperado el 15 de Agosto de 2021, de <https://dle.rae.es>
- Romero, M. Á. (Mayo de 2020). Las Criptomonedas. Sevilla, España. Obtenido de <https://idus.us.es/bitstream/handle/11441/108439/ROMERO%20CUBERO%20MIGUEL%20%c3%81NGEL%20TFG%5b274999%5d.pdf?sequence=1&isAllowed=y>

- Rose, Eldridge, & Chapin. (2015). La internet de las cosas - una breve reseña. *Internet Society*, 5.
- Sánchez Cano, J. E. (2019). El bitcoin y su demanda exponencial de energía: economía versus sostenibilidad. *PANORAMA ECONÓMICO*, 83-108. Obtenido de <http://www.panoramaeconomico.mx/ojs/index.php/PE/article/view/43/32>
- Seth, S. (Abril de 2021). CRYPTOCURRENCY STRATEGY & EDUCATION.
- Seth, S. (2021). Proof of Assignment (PoA). Obtenido de <https://www.investopedia.com/terms/p/proof-assignment-poa.asp>
- Suárez, J. (2020). Implementación eficiente en GPGPUs de la criptomoneda Monero. España. Obtenido de https://addi.ehu.es/bitstream/handle/10810/48832/TFG___Julen.pdf?sequence=2&isAllowed=y
- TUZI, D. (2017). CRYPTONIGHT GPU MINING EFFICIENCY. Obtenido de <https://trepo.tuni.fi/bitstream/handle/123456789/26464/Tuzi.pdf?sequence=4&isAllowed=y>
- Valente, M. (Julio de 2019). What is Proof of Authority? Obtenido de <https://www.coinhouse.com/learn/what-is-proof-of-authority/>
- Vélez Martínez, C. (2017). Criptografía. *Gaceta Instituto de Ingeniería*, 21-21. Obtenido de <http://gacetaii.iingen.unam.mx/GacetaII/index.php/gii/article/view/1889>
- Vranken, H. (2017). Sustainability of bitcoin and blockchains. Netherlands.
- World Economic Forum. (15 de Enero de 2020). *The Global Risks Report 2020*. Recuperado el 28 de Abril de 2021, de <https://www.weforum.org/reports/the-global-risks-report-2020>
- Yanez, D. (2019). *lifeder*. Obtenido de <https://www.lifeder.com/metodo-descriptivo/>