

DISEÑO DE UNA METODOLOGÍA PARA EL MINADO DE LA CRIPTOMONEDA DOGECOIN EN DEBIAN/LINUX

Christian Alberto Gutiérrez Llanos¹, Enrique Eliseo Hernández Medina¹, Álvaro Peraza Garzón¹

¹ Universidad Autónoma de Sinaloa, Facultad de Informática Mazatlán (México)

Resumen

Esta investigación aborda distintos temas alrededor del minado de criptomonedas. Debido a la falta de información ordenada para conseguir minar de manera personal o casera, este estudio presenta de manera precisa y secuencial, los pasos a seguir para el minado con CPU de la criptomoneda DOGECOIN en Debian/Linux.

Palabras clave: Criptomoneda, debian, dogecoin, linux, minería.

Abstract

This research addresses different issues around cryptocurrency mining. Due to the lack of ordered information to mine personally or at home, this study presents the steps to follow for CPU mining DOGECOIN cryptocurrency in Debian/Linux in a precise and sequential manner.

Keywords: Cryptocurrency, debian, dogecoin, linux, mining.

1 INTRODUCCIÓN

Hace unos años no se tenía en cuenta el crecimiento exponencial al que llegarían las criptomonedas, pero poco a poco han ganado mucho interés generando cada vez más demanda. Una criptomoneda, es cualquier tipo de moneda que existe de forma digital o virtual y que utiliza una Blockchain como medio de control. Una Blockchain o cadena de bloques es un conjunto de tecnologías que permiten llevar un registro seguro, descentralizado, sincronizado y distribuido de las operaciones digitales, sin necesidad de la intermediación de terceros [1], esto quiere decir que no es una moneda perteneciente a una institución bancaria y no existe una autoridad o ente de control. El surgimiento de las criptomonedas va de la mano con el nacimiento del Bitcoin creado en 2009 por el desarrollador de pseudónimo Satoshi Nakamoto, sustentada en las prestaciones de una Blockchain [2].

La primera transacción con Bitcoin fue en enero de 2009 con apenas un valor de 0.00076 dólares, no fue hasta febrero de 2011 que alcanzó la paridad con el dólar. Gracias a esto la moneda se popularizó al punto de que en el año de 2013 el Bitcoin supera los mil dólares e iguala su precio al de 1 onza de oro. Debido al éxito de Bitcoin, se ha buscado crear una gran cantidad de criptomonedas, dentro de las que se encuentra DOGECOIN, objeto de estudio de la presente investigación.

DOGECOIN es una criptomoneda catalogada como meme coin (moneda de broma), basada en fragmentos de código de Bitcoin, el propósito de Dogecoin fue el de parodiar a las criptomonedas como algo sin valor, sin embargo, se hizo extremadamente popular, tiene como logo la foto de un perro de raza Shiba Inu [3].

Creada en diciembre del 2013 por Billy Markus, ex trabajador de IBM. Dogecoin emplea el método de consenso "Prueba de Trabajo" (PoW por sus siglas en inglés) para el minado de su cadena: un método de consenso es aquel en donde los participantes de la red llevan a cabo un trabajo que después es verificado por ésta. El minar Dogecoin es un proceso de verificación en la cadena de bloques de DOGE, el minero que descifre más rápido el problema se lleva la recompensa [4].

Estas recompensas son almacenadas en una Wallet o monedero de criptomonedas. En la que podemos gestionar nuestros activos. Es un software o hardware diseñado exclusivamente para almacenar y gestionar las claves públicas y claves privadas de nuestras criptomonedas.

En el caso de las claves públicas es similar a un número de cuenta bancario, cualquier persona puede tenerlo para que nos manden dinero (criptomonedas), pero no pueden extraer los fondos. A través de esta clave se pueden recibir, consultar y ver el estado de cuenta de nuestros activos.

En el caso de las claves privadas son una especie de pin o contraseña que no debemos dar a nadie, nos otorga todo el acceso a nuestros recursos, así como también la posibilidad de gastar o transferir las ganancias.

Pero para poder minar se necesita un software de confianza y que funcione a plenitud como lo es XMRIG que es un programa minero de criptomonedas legal, de código abierto, que utiliza los procesadores de la computadora para minar la criptomoneda Monero.

Unmineable es un sistema automatizado, permite a usuarios de todo el mundo minar monedas de una manera más eficiente. Hace la conversión de una criptomoneda con más valor en el mercado, a la que se desee dependiendo del algoritmo que se utilice. Es importante mencionar que el programa cobra una tarifa del 1%. En el caso del algoritmo se usará RandomX, algoritmo de minería de Monero [5].

Cada criptomoneda puede tener diferente proceso de minado. Por este motivo se han realizado diversas investigaciones respecto a la minería de criptomonedas, tal es el caso de estudiantes de la Universitat Politècnica de Catalunya, que en el 2020 elaboraron un trabajo donde se ha conseguido minar la criptomoneda Monero y se incluye una crítica social referente al gasto computacional que conforma dicho minado y la repercusión que tiene con el medio ambiente [6].

Sabemos de la responsabilidad que debemos de tener con el medio ambiente por eso realizamos búsquedas en diferentes artículos que mencionen como podemos ayudar a nuestro entorno si nuestro objetivo es minar criptomonedas, en la siguiente investigación “impacto ambiental de las criptomonedas” menciona los cuidados que debemos de tener al momento de estar minando y enterarnos de toda la energía que se consume al minar tan solo 4 criptomonedas en específico, al igual que da un ejemplo que señala que minar 4 Bitcoins consume 3441 MW (equivalente a mantener en funcionamiento el metro de la Ciudad de México durante 17 segundos) [7].

Es importante también saber la seguridad con la que estos programas cuentan, como tal es el caso de Blockchain donde estudiantes de las escuelas AMA International University BAHRAIN (AMAIUB) y University of Suffolk, realizaron un artículo en el cual hicieron encuestas y compararon artículos de investigación, al igual que experimentaron con aplicaciones para evaluar la implementación de Blockchain para mejorar la seguridad, para identificar los desafíos asociados y proponer soluciones para sistemas de seguridad mejorados habilitados para BlockChain y así poder tener una mayor seguridad al momento de minar criptomonedas [8].

Después de revisar varios estudios, encontramos un artículo que habla acerca de la variación de la tendencia del precio de Dogecoin [9].

Así como lo menciona en otro estudio, se ha evaluado de forma independiente el impacto económico de la criptocomunidad, acerca de que existen diversas posibilidades metodológicas para pronosticar el precio de una criptomoneda, principalmente proveniente de comunidades en línea [10].

Estos estudios revelaron algunos detalles útiles para el desarrollo de nuestra metodología.

Sabemos que el minado de criptomonedas siempre fue y es un tema que para la mayoría es complicado de entender, el propósito de la investigación fue el de diseñar una metodología que muestre la serie de pasos y los requerimientos mínimos, pero funcionales, para que cualquier persona logre minar la criptomoneda Dogecoin. Además, se hizo una comparativa entre dos sistemas operativos para saber cuál es más rentable.

En lo que resta del documento, y en la sección de metodología, se abordan los pasos y materiales necesarios para el minado de la criptomoneda. Además, se menciona la configuración del software necesario. En la sección de resultados, se muestran las distintas terminales de configuración, resultados de minado, y comparativas entre los distintos sistemas operativos mencionados anteriormente. Por último, en la sección de conclusiones damos nuestros puntos de vista asociados con la creación y ejecución de la metodología propuesta en este documento.

2 METODOLOGÍA

Se utilizaron distintos procesos de minado para converger en uno definitivo, lo primero que se hizo fue instalar el sistema operativo Debian, e instalar un programa que sirve como cartera para el almacenamiento de la moneda minada, cabe señalar que, para este proceso, nuestro usuario en Debian debe tener permisos de superusuario.

Prácticamente, lo que se hará es emplear el software Xmrigr con el algoritmo RandomX para minar Monero y utilizar el sistema web “Unmineable”, para convertir en tiempo real esa moneda por Dogecoin.

2.1 Materiales

A continuación, se muestra una lista de las herramientas y el equipo utilizado para llevar a cabo el experimento.

- Equipo de computo
 - Procesador: Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz
 - RAM: 8.0 GB DDR3 1600 MHz
 - Almacenamiento: SSD Kingston 480 GB
 - Fuente de poder(potencia): 240W
 - Gráficos: AMD Radeon HD 6450 1GB
 - Sistema operativo: Debian de 64 bits con escritorio Xfce
- Software minero: Xmrigr
- Cartera: DogeWallet
- Conexión a internet

2.2 Instalar la cartera

Lo primero que se hará es instalar una Wallet de Dogecoin, para esto se accede a la página oficial de Dogecoin: <https://dogecoin.com/wallets/>

En nuestro caso se usará la cartera “DogeWallet” (Figura 1).



Figura 1. Cartera DogeWallet.

Se selecciona la cartera y se descarga.

Como el sistema que usamos es de 64 bits seleccionamos la versión “DogeWallet.linux64.tgz”, comenzará la descarga automáticamente.

Cuando la descarga haya terminado el archivo se guardará en nuestra carpeta de “Descargas”.

Desde la terminal nos posicionaremos en la carpeta Descargas con el comando: `cd Descargas/`

Escribimos en la terminal el comando “ls” para ver el contenido de la carpeta (Figura 2).

```
nrk@optiplex:~$ cd Descargas/  
nrk@optiplex:~/Descargas$ ls  
DogeWallet.linux64.tgz  
nrk@optiplex:~/Descargas$
```

Figura 2. Terminal en Descargas con comando ls.

Debemos descomprimir el archivo que acabamos de descargar (en la terminal saldrá con color rojo), así que ponemos el siguiente comando: `tar xzvf DogeWallet.linux64.tgz`

Dejamos que termine de descomprimir (Figura 3).

```
DogeWallet/pnacl/pnacl_public_x86_64_crtend.o
DogeWallet/pnacl/pnacl_public_x86_64_pnacl_lic_nexe
DogeWallet/pnacl/pnacl_public_x86_64_libgcc.a
DogeWallet/pnacl/pnacl_public_x86_64_crtbegin.o
DogeWallet/pnacl/pnacl_public_x86_64_libpnacl_irt_shim_dummy.a
DogeWallet/pnacl/pnacl_public_pnacl_json
DogeWallet/pnacl/pnacl_public_x86_64_ld_nexe
DogeWallet/pnacl/pnacl_public_x86_64_libcrt_platform.a
DogeWallet/pnacl/pnacl_public_x86_64_crtbegin_for_eh.o
DogeWallet/pnacl/pnacl_public_x86_64_libpnacl_irt_shim.a
DogeWallet/pnacl/pnacl_public_x86_64_pnacl_sz_nexe
nrk@optiplex:~/Descargas$
```

Figura 3. Archivo DogeWallet descomprimido.

Volvemos a poner el comando “ls” y veremos que ahora hay una carpeta llamada “DogeWallet” (en color azul), ponemos el comando: “cd DogeWallet” para entrar a la carpeta, y después “ls” (Figura 4).

```
DogeWallet/pnacl/pnacl_public_x86_64_pnacl_sz_nexe
nrk@optiplex:~/Descargas$ ls
DogeWallet DogeWallet.linux64.tgz
nrk@optiplex:~/Descargas$ cd DogeWallet/
nrk@optiplex:~/Descargas/DogeWallet$ ls
chrome_crashpad_handler lib nwjc
chromedriver locales payload
credits.html minidump_stackwalk pnacl
DogeWallet nacl_helper resources.pak
DogeWallet.desktop nacl_helper_bootstrap swiftshader
DogeWallet.png nacl_irt_x86_64.nexe v8_context_snapshot.bin
icudtl.dat nw_100_percent.pak
install.sh nw_200_percent.pak
nrk@optiplex:~/Descargas/DogeWallet$
```

Figura 4. Terminal en carpeta DogeWallet con “ls”.

Entre esos archivos hay uno llamado “install.sh”, debemos ejecutarlo y lo hacemos con el comando: “sudo sh install.sh”(Figura 5).

```
nrk@optiplex:~/Descargas/DogeWallet$ sudo sh install.sh
### Creating installation directories...
### Installing DogeWallet...
### Integrating DogeWallet with linux desktop...
### Setting file permissions...
### Updating desktop database...
### Installation Complete!
nrk@optiplex:~/Descargas/DogeWallet$
```

Figura 5. Programa DogeWallet instalado.

Buscamos el programa en nuestras aplicaciones y lo abrimos.

Crearemos una nueva cartera presionando el botón “Create New Wallet”, y saldrá lo siguiente (Figura 6):



Figura 6. Pantalla con la contraseña.

En el recuadro negro estará escrita nuestra contraseña de la cartera (consta de 12 palabras).

Es MUY IMPORTANTE resguardar esa contraseña, ya que es la única manera de acceder a la cartera.

Una vez que hayamos copiado la contraseña; seleccionamos la opción que dice “I have written down or otherwise securely store my passphrase” y pulsamos “OK”.

Ya tenemos nuestra cartera lista.

2.3 Descargar el software Xmrig

Entramos a la siguiente página: <https://github.com/xmrig/xmrig/releases>

Y descargamos el archivo “xmrig-6.18.1-linux-static-x64.tar.gz”.

Desde la terminal, nos ubicamos en la carpeta Descargas con el comando “cd Descargas/” y después “ls” para ver el contenido de la carpeta.

Debe salir el archivo que descargamos en color rojo, para descomprimir ponemos el comando:

“tar xzvf xmrig-6.18.1-linux-static-x64.tar.gz” (Figura 7).

```
nrk@optiplex:~$ cd Descargas
nrk@optiplex:~/Descargas$ ls
xmrig-6.18.1-linux-static-x64.tar.gz
nrk@optiplex:~/Descargas$ tar xzvf xmrig-6.18.1-linux-static-x64.tar.gz
xmrig-6.18.1/
xmrig-6.18.1/config.json
xmrig-6.18.1/xmrig
xmrig-6.18.1/SHA256SUMS
nrk@optiplex:~/Descargas$
```

Figura 7. Archivo Xmrig descomprimido.

2.4 Iniciar el minado

Desde la terminal entramos a la carpeta que acabamos de descomprimir que estará en Descargas, con este comando: “cd xmrig-6.18.1” (Figura 8).

```
nrk@optiplex:~/Descargas$ ls
xmrig-6.18.1 xmrig-6.18.1-linux-static-x64.tar.gz
nrk@optiplex:~/Descargas$ cd xmrig-6.18.1
nrk@optiplex:~/Descargas/xmrig-6.18.1$
```

Figura 8. Terminal en la carpeta xmrig-6.18.1.

Una vez en esta carpeta, creamos un documento de texto que hará iniciar el programa, este documento puede llevar cualquier nombre, pero tiene que terminar en “.sh” (en nuestro caso lo llamaremos “minar.sh”), lo creamos con el comando: “touch minar.sh” (Figura 9).

```
nrk@optiplex:~/Descargas$ cd xmrig-6.18.1
nrk@optiplex:~/Descargas/xmrig-6.18.1$ touch minar.sh
nrk@optiplex:~/Descargas/xmrig-6.18.1$
```

Figura 9. Creación del documento de texto con el comando touch.

Y abrimos ese documento con cualquier editor de texto (usaremos el programa sublime.) o directamente en la terminal con el comando:

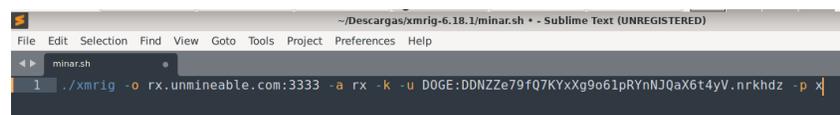
“nano minar.sh”.

En este documento escribiremos lo siguiente:

```
./xmrig -o rx.unmineable.com:3333 -a rx -k -u COIN:YOUR_ADDRESS.WORKER_NAME -p x
```

Necesitamos la dirección de nuestra cartera, se obtiene abriendo el monedero DogeWallet y en la parte superior derecha está la opción de “View Address” y ahí podremos copiar la dirección que está debajo del código QR.

En el documento de texto solo cambiaremos donde dice “COIN” por “DOGE”. Después de los dos puntos pondremos la dirección de la cartera. Luego del punto, un nombre de trabajador cualquiera (Figura 10).



```
~/Descargas/xmrig-6.18.1/minar.sh - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
1 ./xmrig -o rx.unmineable.com:3333 -a rx -k -u DOGE:DDNZze79f07KYxXg9e61pRYnNJQaX6t4yV.nrkhdz -p x
```

Figura 10. Documento de texto con la moneda, la address y el nombre del trabajador.

Guardamos el documento que tiene que ir en la misma carpeta que el programa, ahora solo queda ejecutarlo para que empiece a minar.

En la terminal, nos posicionamos en la carpeta del programa con “cd Descargas/xmrig-6.18.1”, y ejecutamos el documento de texto que acabamos de crear con el siguiente comando:

“sudo sh minar.sh” (Figura 11).

```
nrk@optiplex:~/Descargas/xmrig-6.18.1$ ls
config.json  minar.sh  SHA256SUMS  xmrig
nrk@optiplex:~/Descargas/xmrig-6.18.1$ sudo sh minar.sh
[sudo] password for nrk:
* ABOUT      XMRig/6.18.1 gcc/9.3.0
* LIBS       libuv/1.44.1 OpenSSL/1.1.1o hwloc/2.7.1
* HUGE PAGES supported
* 1GB PAGES  unavailable
* CPU        Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz (1) 64-bit AES
             L2:1.0 MB L3:6.0 MB 4C/4T NUMA:1
* MEMORY    0.9/7.7 GB (12%)
             DIMM3: <empty>
             DIMM1: 8 GB DDR3 @ 1600 MHz
             DIMM4: <empty>
             DIMM2: <empty>
```

Figura 11. Iniciar el programa de minado.

Automáticamente el programa comenzará a minar.

Como ejecutamos el documento con el comando “sudo”, nos pedirá la contraseña del usuario.

En caso de que abriéramos el documento sin “sudo” únicamente “sh minar.sh” el mismo programa nos dirá que tendremos un rendimiento bajo “HASHRATE WILL BE LOW” (Figura 12).

```
nrk@optiplex:~/Descargas/xmrig-6.18.1$ sh minar.sh
* ABOUT      XMRig/6.18.1 gcc/9.3.0
* LIBS       libuv/1.44.1 OpenSSL/1.1.1o hwloc/2.7.1
* HUGE PAGES supported
* 1GB PAGES  unavailable
* CPU        Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz (1) 64-bit AES
             L2:1.0 MB L3:6.0 MB 4C/4T NUMA:1
* MEMORY    0.9/7.7 GB (10%)
* DONATE     1%
* ASSEMBLY   auto:intel
* POOL #1    rx.unmineable.com:3333 algo rx/0
* COMMANDS  Hashrate, Pause, Resume, Results, Connection
[2022-11-07 23:23:35.960] net use pool rx.unmineable.com:3333 137.184.01.203
[2022-11-07 23:23:35.960] cpu use argon2 implementation SSE3
[2022-11-07 23:23:35.960] msr msr kernel module is not available
[2022-11-07 23:23:35.960] msr FAILED TO APPLY MSR MOD, HASHRATE WILL BE LOW
[2022-11-07 23:23:35.960] randomx init dataset algo rx/0 (4 threads) seed d408f013613f7e83...
```

Figura 12. HASHRATE WILL BE LOW.

Para detener el minado solo presionamos Ctrl + C (Figura 13).

```
[2022-11-07 23:23:54.489] net new job from rx.unmineable.com:3333 diff 100001 algo rx/0 height 2751064 (3 tx)
[2022-11-07 23:24:42.556] miner speed 10s/60s/15m 804.4 n/a n/a H/s max 1310.8 H/s
[2022-11-07 23:24:53.579] signal Ctrl+C received, exiting
[2022-11-07 23:24:53.581] cpu stopped (2 ms)
nrk@optiplex:~/Descargas/xmrig-6.18.1$
```

Figura 13. Detener el minado con Ctrl + C.

3 RESULTADOS

Como resultado del experimento, a continuación, se muestra la ruta a seguir para el minado de la criptomoneda Dogecoin.

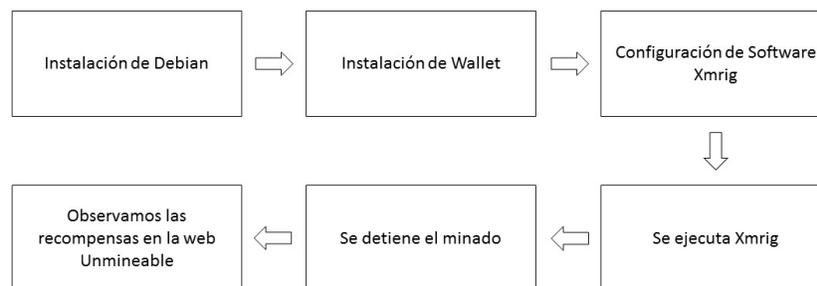


Figura 14. Diagrama de la metodología.

Empleando esta metodología, se procedió a minar durante 8 horas con el equipo mencionado anteriormente, obteniendo así las siguientes ganancias (Figura 15).



Figura 15. Monedas obtenidas en 8 horas.

De la misma manera se implementó en el sistema operativo Windows, efectuando una comparativa con el sistema Debian durante 120 minutos, dando como resultado los datos de la Tabla 1.

Tabla 1. Comparativa entre los sistemas.

Sistema operativo	Tiempo en minutos			
	30	60	90	120
Debian	0.00381151	0.00806279	0.01143451	0.01656538
Windows	0.00117236	0.00437484	0.00698481	0.01193975

Como se observó en la tabla anterior, en el sistema operativo Debian se logró minar: “0.01656538” monedas, esto en un lapso de 120 minutos, mientras tanto, en el sistema Windows se minaron “0.01193975” monedas, en el mismo lapso.

Un inconveniente que se presentó en el sistema Windows es que durante el minado poco a poco se iba acumulando la RAM afectando así el rendimiento del equipo, y por ende del minado.

4 CONCLUSIONES

Con base en los resultados, concluimos, que se logró diseñar de manera exitosa la metodología para el minado de la criptomoneda Dogecoin.

Así como también se verificó, que el sistema más rentable para el minado de dicha criptomoneda es Debian, ya que el rendimiento promedio es mayor, esto es debido a que el sistema consume menos recursos del equipo.

Respecto al consumo eléctrico, durante el minado, teniendo un uso promedio de 168 Wh, durante las 8 horas que se minó en Debian se consumió un total de 1344 W (el equivalente a tener una plancha encendida durante 1 hora).

Dando por terminada esta investigación, encontramos muy interesante, el haber diseñado una metodología, que pueda servir de apoyo para todas aquellas personas que estén interesadas en incursionar en el mundo de la minería de criptomonedas.

REFERENCIAS

- [1] solunion, «solunion,» 26 agosto 2021. [En línea]. Available: <https://www.solunion.cl/blog/que-es-y-para-que-sirve-la-tecnologia-blockchain/>. [Último acceso: noviembre 2022].
- [2] I. Barceró Ferre, «economipedia,» 25 septiembre 2017. [En línea]. Available: <https://economipedia.com/definiciones/criptomoneda.html>. [Último acceso: noviembre 2022].
- [3] Y. Fernández, «XATAKA,» 22 abril 2022. [En línea]. Available: <https://www.xataka.com/basics/que-dogecoin-como-funciona-que-se-ha-hecho-popular#:~:text=El%20Dogecoin%20es%20un%20tipo%20de%20criptomoneda%20que%20naci%C3%B3%20como,le%20a%C3%B1aden%20frases%20gramaticalmente%20incorrectas..> [Último acceso: noviembre 2022].

- [4] C. Marulanda López, «ComprarAcciones,» 2 Noviembre 2022. [En línea]. Available: <https://compraracciones.com/mx/minar-dogecoin/>. [Último acceso: Noviembre 2022].
- [5] b. academy, «bit2me academy,» 2022. [En línea]. Available: [https://academy.bit2me.com/que-algoritmo-mineria-randomx-monero/#:~:text=RandomX%20es%20el%20nombre%20del,a%20su%20protocolo%20y%20blockchain](https://academy.bit2me.com/que-algoritmo-mineria-randomx-monero/#:~:text=RandomX%20es%20el%20nombre%20del,a%20su%20protocolo%20y%20blockchain.). [Último acceso: noviembre 2022].
- [6] O. V. Gangonells, «LA MINERÍA EN CRIPTOMONEDAS,» *BARCELONATECH*, vol. 1, nº 1, p. 67, 2022.
- [7] M. S. García, «IMPACTO AMBIENTAL DE LAS CRIPTOMONEDAS,» *BARCELONATECH*, vol. 1, nº 1, p. 59, 2022.
- [8] M. Mahdi y A. Maaruf, «Applications of Blockchain Technology beyond Cryptocurrency,» *Annals of Emerging Technologies in Computing*, vol. 2, nº 1, p. 6, 2018.
- [9] S. Sanagavarapu y S. Sridhar, «Multi-Head Self-Attention Transformer for Dogecoin Price Prediction,» *IEEE Xplore*, vol. 1, nº 1, p. 6, 2021.
- [10] E. Lansiuax, N. Tchagaspanian y J. Forget, «Community Impact on a Cryptocurrency: Twitter Comparison Example Between Dogecoin and Litecoin,» *frontiers*, vol. 1, nº 1, p. 17, 2022.
- [11] L. Gundaboina, S. Badotra, T. Kaur Bhatia, K. Sharma, G. Mehmood, M. Fayaz y I. Ullah Khan, «Ming Cryptocurrency-Based Security Using Renewable Energy as Source,» *Security and Communication Networks*, vol. 1, nº 1, p. 13, 2022.