

RENDIMIENTO DEL HARDWARE DE UN EQUIPO PERSONAL EN LA MINERÍA DE CRIPTOMONEDA

Jose Cruz Lerma Lomeli¹, Jorge Mario cortes Rodríguez¹, Edgar Iván Arenas Osuna¹

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

Resumen

En la presente investigación se muestran los diferentes tipos de hardware utilizados para la minería, y el rendimiento del hardware en un equipo personal a la hora de minar. Los resultados detallan que la diferencia entre el uso de CPU y el GPU es amplia en cuanto a rendimiento se refiere, ya que cada una genera una cantidad distinta de hashes a la hora de minar, por otro lado, se observó que ambos equipos son estables al momento de estar en uso.

Palabras clave: Minería, criptomoneda, rendimiento, hardware.

Abstract

In the present investigation the different types of hardware used for mining are shown, and the performance of the hardware in a personal computer when mining. The results detail that the difference between the use of the CPU and the GPU is wide in terms of performance, since each one generates a different amount of hashes when mining, on the other hand, it was observed that both computers are stable when in use.

Keywords: Mining, cryptocurrency, performance, hardware.

1 INTRODUCCIÓN

Lo que se realizó en este proyecto fue una investigación a fondo acerca del rendimiento generado por el hardware de un sistema computacional personal al momento de minar criptomoneda, pero en sí, ¿qué es una criptomoneda?, pues se pueden dar muchas definiciones de criptomoneda. Según el banco europeo central “es la representación digital de valor, no emitida por ninguna autoridad central, institución de crédito o emisor de dinero electrónico reconocido que, en ciertas ocasiones, puede ser utilizada de pago alternativo al dinero [1].

En lo cual también definimos quiénes son los principales emisores de la criptomoneda, en este caso de Bitcoin, tenemos entendido que esta criptomoneda se genera a base de trabajo o minado, todo eso basado en la red de Bitcoin como se muestra en la investigación [2].

Como se sabe las formas de pagos online que conocemos al día de hoy pertenecen a organizaciones. Ellos retienen tu dinero y debes solicitar alguna transacción o transferencia a tu nombre si deseas gastar en algo, con las criptomonedas, no existe alguna organización. Entonces, tanto tu como tus amigos, familiares o cualquier persona en general, pueden ser su propio banco, esto gracias a que, tu computadora se conecta con las computadoras de otras personas, lo cual permite una comunicación directa, es decir, sin intermediarios y esto es gracias a al sistema Blockchain (cadena de bloques) con una base de datos descentralizada. Una Blockchain es una tecnología en crecimiento, basada en un conjunto de protocolos en Internet, que está cambiando la forma en que las entidades y particulares interactuamos a través de la red. Permite realizar transacciones seguras en línea tales como darnos de alta en organizaciones, liquidación de fondos, pagos en moneda o cualquier otra clase de activos sin necesidad de que intervengan intermediarios de confianza que den validez a dichas operaciones [3].

Blockchain se puede considerar como una base de datos descentralizada y distribuida que se utiliza para registrar transacciones entre muchas computadoras, de modo que los registros no pueden modificarse retroactivamente sin el consenso de toda la red implicada. Esto permite a los participantes verificar y auditar las transacciones y reconciliar obligaciones de manera eficiente y económica. Este último punto es el que, a mi entender, está potenciando el crecimiento de esta tecnología llamando la atención de muchas entidades [3].

Esto nos lleva a los rigs de minería o los diferentes tipos de hardware utilizados en la misma, que son CPU (Unidad Central de Proceso o de sus siglas en inglés Central Processing Unit [4]), GPU (de sus siglas en inglés Graphics Processing Unit - Unidad de Procesamiento Gráfico [5]), FPGA (de sus siglas en inglés Field Programmable Gate Array, cuya finalidad es proveer al desarrollador un entorno con el cual lograr diseños electrónicos digitales de pequeña y alta complejidad [6]) o ASIC (Application Specific Integrated Circuits [7]) y cada uno funciona más óptimamente para cada tipo de moneda, por ejemplo, para la minería de Bitcoin se utilizan los ASIC, para la minería de Monero se utilizan procesadores o FPGA, etc., y todos y cada uno de estos se diferencian entre sí, ya que unos generan más hashes (proceso que transforma cualquier conjunto arbitrario de datos en una nueva serie de caracteres con una longitud fija [8]) y consumen más o menos energía, lo cual hace que las ganancias sean diferentes en la mayoría de los casos.

Esto al ser aceptado por la gente, terminó siendo algo popular, y por consiguiente mucha gente empezó a realizar investigaciones para saber cuál era la mejor manera de “minar”, y que diera buenas ganancias sin gastar tanto, es decir, comparar diferentes tipos de hardware y algoritmos para realizar esta acción de la manera más óptima, como lo es la investigación realizada en la universidad de los andes, Colombia [9] en la cual veía si era rentable utilizar el equipo computacional de la misma universidad, desde un punto de vista económico y técnico, para la minería de criptomoneda, y así ver cuál de entre todos los tipos de maneras de minar criptomoneda era la mejor, es decir, comparando entre CPU, GPU, ASIC o FPGA, y así saber cuál de todos da un mejor rendimiento y menos consumo de recursos.

Por otra parte, tenemos el incremento de capacidad de minado, en el cual se muestra el uso máximo de las capacidades de los equipos revisados tomando en cuenta los cambios en los últimos años sobre la actualización de los mismos equipos utilizados en dicha investigación [10].

Mencionando con estas mismas las alternativas de energías que pueden ser utilizadas para el uso de optimización de operaciones adecuadas de un RIG, esto con base en las investigaciones previas realizadas en las cuales se habla sobre distintos métodos de ahorro de energía y muestra los resultados de los indicadores del rendimiento de los flujos por expansiones en los equipos [10].

Esta investigación se llevó a cabo, ya que como se mencionó antes, en estos días la minería de criptomoneda es un tema muy relevante, y aunque tenga mucho tiempo realizándose, sigue habiendo bastante interés entre los mineros y las personas que no están dentro de este mundo de la minería, dicho esto, se pretende dar a conocer la manera concreta en que los equipos personales rinden a la hora de minar y comparar los resultados obtenidos entre sí.

Mencionando la problemática que existe, que es la desinformación en muchas personas respecto a este tema ya que es algo complejo que no cualquiera puede llevar a cabo sin la debida orientación, y así que las personas tengan un conocimiento adecuado para la utilización del equipo personal de minado y empezar a minar por su cuenta si así es deseado.

Por consiguiente, los objetivos de esta investigación son:

- Explicar que son las criptomonedas.
- Mostrar los diferentes tipos de hardware de minería que se utilizan.
- Minar con un equipo personal para recolectar datos.
- Comparar la diferencia de rendimiento que hay entre CPU y GPU en un equipo personal.

2 METODOLOGÍA

En esta investigación se utilizaron los medios informáticos para realizar la recolección de datos e información acerca del tema expuesto anteriormente, esto con una metodología de la investigación tipo experimental y explicativa, con el fin de ir más allá y dar a conocer una problemática que en este caso sería la desinformación que se tiene acerca de la minería de criptomonedas, y así darle una solución dando datos que pueden ayudar a orientar a las personas en este mundo de la minería.

Además, se tuvo un enfoque cuantitativo en la recolección de datos, y a partir de estos datos se realizaron gráficos, para mostrar toda la información recolectada y hacer una comparativa de los diferentes equipos utilizados y ver cuál fue su rendimiento a la hora de estar minando.

Para minar se utilizó el software XMRig 6.7.2 en ambos casos, es decir, en el CPU y el GPU,

y un equipo con las siguientes especificaciones:

- CPU: AMD Ryzen 7 2700X, 8 núcleos, 16 hilos, de 3.70GHz
- RAM: 16 GB de 2666 MHz
- Almacenamiento: SSD M.2 de 120 GB
- Gráfica: Nvidia GYGABYTE GTX 1050 TI

3 RESULTADOS

En la figura 1 y 2 se muestra una captura del equipo a la hora de minar desde el CPU y GPU.

```

XMRig 6.7.2
2022-11-08 22:44:22.991] cpu    accepted (12/0) diff 100396 (59 ms)
2022-11-08 22:44:27.529] cpu    accepted (13/0) diff 100396 (60 ms)
2022-11-08 22:44:35.036] net    new job from pool.supportxmr.com:7777 diff 104310 algo rx/0 height 2751747
2022-11-08 22:44:50.100] cpu    accepted (14/0) diff 104310 (82 ms)
2022-11-08 22:45:06.102] miner  speed 10s/60s/15m 1920.9 1854.1 n/a H/s max 1950.2 H/s
2022-11-08 22:45:10.951] cpu    accepted (15/0) diff 104310 (83 ms)
2022-11-08 22:45:35.053] net    new job from pool.supportxmr.com:7777 diff 108090 algo rx/0 height 2751747
2022-11-08 22:45:39.714] cpu    accepted (16/0) diff 108090 (84 ms)
2022-11-08 22:46:07.316] miner  speed 10s/60s/15m 1923.2 1909.8 n/a H/s max 1950.2 H/s
2022-11-08 22:46:35.072] net    new job from pool.supportxmr.com:7777 diff 106290 algo rx/0 height 2751747
2022-11-08 22:47:08.561] miner  speed 10s/60s/15m 1956.2 1934.4 1837.8 H/s max 1956.2 H/s
2022-11-08 22:47:11.075] net    new job from pool.supportxmr.com:7777 diff 106290 algo rx/0 height 2751748
2022-11-08 22:47:35.086] net    new job from pool.supportxmr.com:7777 diff 99540 algo rx/0 height 2751748
2022-11-08 22:48:09.842] miner  speed 10s/60s/15m 1949.5 1947.2 1862.8 H/s max 1959.9 H/s
2022-11-08 22:48:11.285] net    new job from pool.supportxmr.com:7777 diff 99540 algo rx/0 height 2751749
2022-11-08 22:48:35.099] net    new job from pool.supportxmr.com:7777 diff 93600 algo rx/0 height 2751749
2022-11-08 22:49:10.987] miner  speed 10s/60s/15m 1944.9 1954.4 1873.8 H/s max 1968.1 H/s
2022-11-08 22:49:35.113] net    new job from pool.supportxmr.com:7777 diff 88335 algo rx/0 height 2751749
2022-11-08 22:50:12.113] miner  speed 10s/60s/15m 1958.7 1919.5 1883.6 H/s max 1968.1 H/s
2022-11-08 22:50:35.123] net    new job from pool.supportxmr.com:7777 diff 83655 algo rx/0 height 2751749
2022-11-08 22:50:56.021] cpu    accepted (17/0) diff 83655 (82 ms)
2022-11-08 22:51:13.315] miner  speed 10s/60s/15m 1935.8 1917.4 1890.5 H/s max 1968.1 H/s
2022-11-08 22:51:17.883] net    new job from pool.supportxmr.com:7777 diff 83655 algo rx/0 height 2751750
2022-11-08 22:51:35.138] net    new job from pool.supportxmr.com:7777 diff 82576 algo rx/0 height 2751750
2022-11-08 22:52:09.361] net    new job from pool.supportxmr.com:7777 diff 82576 algo rx/0 height 2751751
2022-11-08 22:52:13.699] cpu    accepted (18/0) diff 82576 (60 ms)
2022-11-08 22:52:14.472] miner  speed 10s/60s/15m 1923.8 1936.0 1893.6 H/s max 1968.1 H/s
2022-11-08 22:52:17.687] cpu    accepted (19/0) diff 82576 (60 ms)
2022-11-08 22:52:17.877] cpu    accepted (20/0) diff 82576 (60 ms)
    
```

Figura 1. Evidencia del equipo al estar minado con CPU.

```

C:\WINDOWS\system32\cmd.exe
ID GPU Temp Fan Core Mem Kern |
-----+-----+-----+-----+-----+-----+
0 1050Ti 63 42 % 1733 3504 3 |
-----+-----+-----+-----+-----+
3:30:55 Pool: etc.2miners.com:1010 [141.95.124.89]
3:30:55 Pool Hashrate: 7.06 MH/s Efficiency: 56.55 %
3:30:55 Balance: 0.672123 ETC
3:30:55 Shares/Minute: 0.05
3:30:55 Uptime: 0d 04:07:06 Electricity: 0.295 kWh
3:31:02 New Job: 00b82b07 Epoch: #542 Block: #16260538 Diff: 8.7266
3:31:08 New Job: 0b329171 Epoch: #542 Block: #16260539 Diff: 8.7266
3:31:18 New Job: 9fee2d76 Epoch: #542 Block: #16260539 Diff: 8.7266
3:31:23 New Job: 7b196048 Epoch: #542 Block: #16260540 Diff: 8.7266
-----+-----+-----+-----+-----+
ID GPU Speed Shares Best Power Efficiency |
-----+-----+-----+-----+-----+
0 1050Ti 12.48 MH/s 12/0/0 46.46G 72 W 173.28 KH/W |
-----+-----+-----+-----+-----+
ID GPU Temp Fan Core Mem Kern |
-----+-----+-----+-----+-----+
0 1050Ti 63 42 % 1733 3504 3 |
-----+-----+-----+-----+-----+
3:31:25 Pool: etc.2miners.com:1010 [141.95.124.89]
3:31:25 Pool Hashrate: 7.05 MH/s Efficiency: 56.50 %
3:31:25 Balance: 0.672123 ETC
3:31:25 Shares/Minute: 0.05
3:31:25 Uptime: 0d 04:07:36 Electricity: 0.296 kWh
3:31:26 New Job: 686ef712 Epoch: #542 Block: #16260541 Diff: 8.7266
    
```

Figura 2. Evidencia del equipo al estar minado con GPU.

Una de las principales diferencias que se visualizan en las anteriores evidencias es la cantidad de hashes generados por segundo que en el CPU son de máximo 1968.1 H/s y en el GPU son hasta de 12 MH/s, lo cual es una gran diferencia entre estas dos formas de minado, ya que mientras mayor sea la cantidad de hashes generados en el menor tiempo posible podrá generar una mayor ganancia.

Lo que se hizo posteriormente fue la realización de una gráfica comparativa para analizar la manera en la que rinden el GPU y el CPU al estar minando, respecto a la carga de trabajo contra el tiempo transcurrido.

Lo que se vio es que tanto la GPU como el CPU utilizados son parecidos en cuanto a la estabilidad a la hora de estar en uso, ya que como se muestra en la Figura 3, al momento de poner a minar la GPU y el CPU, a pesar del distinto porcentaje de uso, los dos son bastantes estables y las variaciones de trabajo son muy pocas.

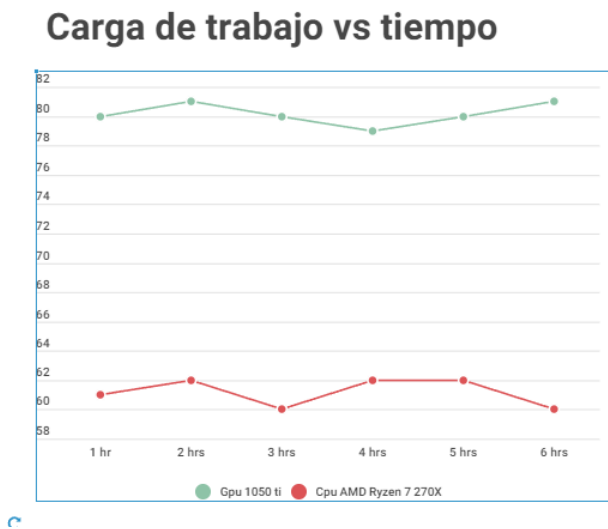


Figura 3. Gráfica comparativa.

En la figura 4 se muestra la comparación de los hashes generados por el CPU y GPU.

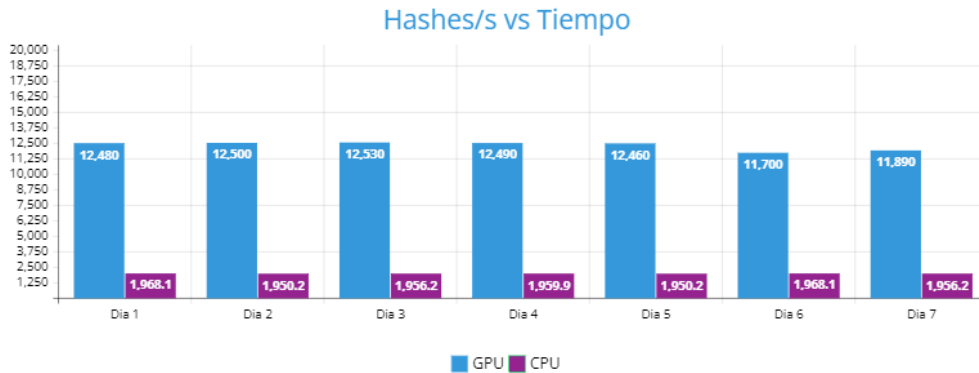


Figura 4. Muestra de los hashes generados por segundo en GPU y CPU.

Al ver la comparación de los hashes generados en ambos casos, se ve una gran diferencia de potencia entre el GPU y el CPU al minar.

4 CONCLUSIÓN

A lo largo de la investigación se ha analizado el estado actual de la aplicación del hardware orientado a la minería de criptomonedas y su rendimiento sobre la misma, podemos observar que el uso del hardware para la minería de criptomonedas tiene que ser un equipo altamente diseñado para la labor a realizar, como fue mostrado con anterioridad, el tener solo hardware con alta capacidad no es una forma segura de poder tener un rendimiento adecuado para este tipo de trabajo. Ya que incluso en el periodo actual de esta investigación se está generando una nueva forma de trabajo que es el proof of stake que da prioridad al bajo consumo energético y no es necesario un equipo especializado para la realización de la validación de las cadenas de bloques.

Como últimas palabras tenemos en puerta la nueva forma de trabajar con el hardware que se tenga a disposición con el nuevo protocolo PoS, que, gracias a él, el malgasto de energía y la inmensa inversión que era necesaria para trabajar con el hardware especializado para el protocolo PoW, empezará a pasar al pasado de la minería como lo conocíamos.

REFERENCIAS

- [1] J. S. Roa, «CRIPTOMONEDAS,» [En línea]. Available: <https://www.pj.gov.py/ebook/monografias/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf>.
- [2] R. R. G. Disla, «BITCOIN: Todo es apócrifo hasta que se canoniza,» agosto 2017. [En línea]. Available: https://www.researchgate.net/profile/Renato-Gonzalez-Disla/publication/318981147_BITCOIN_Todo_es_apocrifo_hasta_que_se_canoniza/links/59890f44a6fdcc75625a63af/BITCOIN-Todo-es-apocrifo-hasta-que-se-canoniza.pdf.
- [3] J. Berenguer, «Blockchain la tecnología que está en boca de todos,» 11 2017. [En línea]. Available: <https://www.andbank.com/wp-content/uploads/2017/11/2017-10-27-que-es-el-Blockchain-Joan-Berenguer-ESP.pdf>.

- [4] M. R. Pedruelo, «El procesador,» 2011. [En línea]. Available: https://riunet.upv.es/bitstream/handle/10251/10673/El_procesador.pdf.
- [5] V. F. P. LATOJA, «USO DE PROCESADORES DE TARJETAS,» 03 2013. [En línea]. Available: http://opac.pucv.cl/pucv_txt/txt-6500/UCF6855_01.pdf.
- [6] J. C. Sánchez, «Estudio comparativo de simulaciones físicas en GPU,» 03 2018. [En línea]. Available: <https://rdu.unc.edu.ar/bitstream/handle/11086/6325/tesis.pdf?sequence=1>.
- [7] A. Z. Aviv Yaish, «Correct Cryptocurrency ASIC Pricing:,» 18 07 2020. [En línea]. Available: <https://arxiv.org/pdf/2002.11064.pdf>.
- [8] A. e. d. p. d. datos, «INTRODUCCIÓN AL HASH COMO TÉCNICA DE SEUDONIMIZACIÓN DE DATOS PERSONALES,» 10 2019. [En línea]. Available: https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_es.pdf.
- [9] H. E. C. B. Juan David Serrano Mugica, «Evaluación cuantitativa de minería de criptomonedas en la Universidad de los Andes,» 11 2021. [En línea]. Available: <https://repositorio.uniandes.edu.co/bitstream/handle/1992/55360/25437.pdf?sequence=1>.
- [10] C. U. Bernal, «ANÁLISIS Y ESTUDIO FINANCIERO DE LAS ALTERNATIVAS DE OPTIMIZACIÓN DE OPERACIÓN DEL RIG,» 07 07 2018. [En línea]. Available: <https://repository.udistrital.edu.co/bitstream/handle/11349/13873/UrdanetaBernalC%20atalina.pdf?sequence=1&isAllowed=y>.