Universidad Zaragoza
1542

Trabajo Fin de Máster

Eficiencia energética de dispositivos de cálculo en el minado de criptomoneda basada en Blockchain

Autor

Pedro Horno Maggioni

Directores

Rubén Gran Tejero
Darío Suárez Gracia

Ingeniería Industrial / Escuela de Ingeniería y Arquitectura

2018

TRABAJOS DE FIN DE GRADO / FIN DE MÁSTER

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

(Este documento debe acompañar al Trabajo Fin de Grado (TFG)/Trabajo Fin de Máster (TFM) cuando sea depositado para su evaluación).

D./Dª. Pedro Horno Maggioni,

con nº de DNI 71269212D en aplicación de lo dispuesto en el art. 14 (Derechos de autor) del Acuerdo de 11 de septiembre de 2014, del Consejo de Gobierno, por el que se aprueba el Reglamento de los TFG y TFM de la Universidad de Zaragoza,

Declaro que el presente Trabajo de Fin de (Grado/Máster) Máster, (Título del Trabajo) Eficiencia energética de dispositivos de cálculo en el minado de criptomoneda basada en Blockchain,

es de mi autoría y es original, no habiéndose utilizado fuente sin ser citada debidamente.

Zaragoza, 05/09/2018

Fdo: Pedro Horno Maggioni

Gracias a Rubén y Darío por darme la oportunidad de realizar este proyecto. Me ayudaron desde el primer día que me presenté en su despacho. Les doy las gracias también por todas las horas que invirtieron resolviendo mis dudas y por supuesto, por su enorme paciencia conmigo.

Gracias también a mis padres, Ana y Javier, a mi hermano Javier, a mi novia Irene y amigos por el apoyo que siempre me habéis dado.

EFICIENCIA ENERGÉTICA DE DISPOSITIVOS DE CÁLCULO EN EL MINADO DE CRIPTOMONEDA BASADA EN BLOCKCHAIN — RESUMEN

La tecnología de bloques, o *Blockchain* en inglés, está dando sus primeros pasos. Se está empezando a utilizar numerosas industrias pero, sin duda alguna, el sector financiero es el que más la está desarrollando. Esta tecnología permite, por ejemplo, crear divisas virtuales (criptomonedas) que no necesitan una tercera parte, como un banco, para gestionarlas. En cambio, en *Blockchain* existe una red de nodos de confianza que asegura que las transacciones de estas monedas virtuales son válidas y no existe fraude. Esto se consigue a partir de una serie de algoritmos que, mediante la resolución de un problema matemático, aseguran el consenso entre los nodos sobre dichas transacciones.

La resolución del problema matemático supone un elevado gasto energético, pero tiene una recompensa económica. Por eso, han aparecido empresas dedicadas exclusivamente a resolver estos problemas matemáticos. Además se puede participar a pequeña escala, usando dispositivos de cómputo generales como: CPUs y GPUs.

Con este proyecto se quiere determinar si esta actividad es rentable a nivel usuario. Para ello, se determinan los consumos reales de dos dispositivos de cómputo (CPU y GPU) durante la resolución del problema matemático. Con estos resultados, se desarrolla un estudio de eficiencia energética de cada uno de ellos y una posterior comparativa entre ambos. A continuación, se realiza un estudio económico sobre la rentabilidad actual de ser parte de la red y finalmente, se comparan los datos económicos obtenidos en el proyecto con los porporcionados por distribuidores de *hardware* específico.

Del estudio económico se concluye que hoy en día no es rentable minar ni a nivel usuario, ni a gran escala. En primer lugar, se requiere de una gran inverisón incial para la compra de *hardware*. En segundo lugar, el precio de la criptomoneda estudiada (Ether) es la principal barrera que determina la rentabilidad del proyecto y finalmente, en el estudio se demuestra que el consumo energético es otro factor clave. No es lo mismo realizar un estudio considerando sólo el consumo energético del dispositivo de cómputo (CPU o GPU), como hacen los distribuidores de estos dispositivos, que considerando el consumo total del sistema.

ÍNDICE

1 INTRODUCCIÓN

1.1 MOTIVACIÓN

Actualmente estamos inmersos en una revolución tecnológica de grandes dimensiones. Algunos la comparan con la vivida tras la aparición de Internet, pero ¿qué más se puede inventar?

Blockchain es un término que en los próximos años va a resultar familiar. ¿El motivo? Grandes empresas tecnológicas como Google [4], Facebook [6], IBM [3]; así como los grandes bancos a nivel mundial, JP Morgan, Santander, HSBC, entre otras muchos [12], están invirtiendo en esta tecnología. El interés acerca de ella, radica en que es una nueva forma de registro de datos más segura y rápida [22].

A finales de la década de los 90 se disponían de todas las herramientas necesarias para construir esta tecnología. Se realizaron algunos proyectos, pero fueron poco fructíferos. Casi todos ellos estaban relacionados con la creación de criptomonedas, que finalmente no tuvieron éxito [2]. Fue la creación del Bitcoin en 2008 [32], el punto a partir del cuál se le empieza a dar importancia a esta tecnología, debido a las características y oportunidades que mostraba de descentralización, anonimato y seguridad.

Tras la aparición de Bitcoin y su rápido crecimiento, surgen distintas plataformas de cadenas de bloques, o *Blockchain* en inglés, con características similares, pero ligeras diferencias. Una de ellas es Ethereum. Se trata de una plataforma *Blockchain* en la que además de transacciones, se permite la creación de contratos inteligentes, *Smart Contracts*, o incluso aplicaciones móviles distribuidas, *DApps*, donde los datos son distribuidos por la red. Otros sectores donde se usa el *Blockchain* son: servicios financieros, sanidad, música, propiedad intelectual, sistemas electorales, automoción e Internet de las Cosas (IoT), entre otros [21].

Los *Smart Contracts* son contratos que, una vez introducidos en la *Blockchain*, no pueden ser alterados por ninguna de las partes. El control y la ejecución de estos contratos recae sobre todos los nodos de la red. De esta forma se consigue que un contrato implementado en una *Blockchain* sea totalmente fiable y seguro. Actualmente, empresas

tanto del sector público como del privado, están investigando las posibilidades de la implantación de este tipo de contratos. Como caso más cercano, la DGA acaba de impulsar un proyecto de contratación pública utilizando la tecnología *Blockchain* [1]. Debido a las características que ofrece Ethereum, hemos basado este proyecto en su tecnología.

Una de las actividades asociadas al *Blockchain* es el minado de bloques. Esta actividad tiene dos propósitos. En primer lugar, permite añadir los bloques a la cadena de bloques. Es un proceso computacionalmente complejo, que requiere mucha energía. En segundo lugar, permite que la red sea de confianza. Es decir, *Blockchain* es una estructura de datos en la que es prácticamente imposible modificar un dato una vez introducido en la red. Imagínese un libro contable inmutable. Esto es posible gracias a un sistema de consenso entre todos los usuarios de la red *Blockchain*.

Esta actividad es imprescindible para el funcionamiento de la red. Si no existiera el minado, no habría consenso, ni libro contable, y por eso no se podrían realizar transacciones.

Para incentivar a los usuarios a participar en el minado, en el caso de Ethereum, existe una recompensa económica de 3 Ether, criptomoneda de la red Ethereum. En este momento supondrían unos 1500€ aproximadamente. Debido a este atractivo se ha creado una nueva forma de negocio.

Hoy en día existen empresas exclusivamente dedicadas a minar bloques, y cada día hay más competencia. Debido a la estructura y funcionamiento de la red, conforme más nodos haya minando, menor es la probabilidad de cada uno de ellos de minar un bloque. Además, un mayor número de nodos supone un mayor consumo energético de la red [29].

Para hacerse una idea de la magnitud del consumo energético, se muestra en la figura Figura 1 un mapa mundial coloreado de acuerdo al porcentaje que representa la energía total del minado de Bitcoin con respecto al consumo eléctrico en cada país.

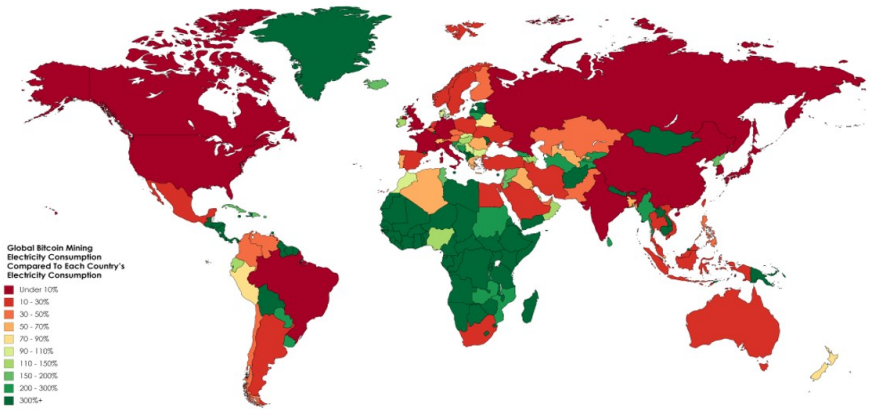


Figura 1: Comparativa global del consumo energético total en el minado de Bitcoin frente al consumo energético por país [8]

Como se puede observar en la Figura 1, el consumo mundial de energía sólo en el minado del Bitcoin, ya supone entre el 10 % y 30 % del consumo energético actual de España. Más visual aún, el minado de Bitcoin supone más del 100 % del consumo energético de los países de color verde. En la figura sólo se está representado el Bitcoin, pero existen alrededor de 1500 criptomonedas diferentes [7]. De modo que el papel que está adquiriendo el consumo energético en el minado de *Blockchain* es de gran importancia. Por eso, se va a estudiar el consumo energético asociado al proceso de minado en distintos dispositivos, así como su eficiencia energética.

El consumo energético proviene mayoritariamente del minado de los bloques, pero no es único gasto energético. La ejecución de estos algoritmos en los dispositivos de cálculo hace que aumente la temperatura de los dispositivos e instalaciones drásticamente, teniendo que enfriarlas. Para ello, se utilizan distintos métodos de refrigeración: convección forzada individual, en la que cada dispositivo tiene un ventilador acoplado (Figura 7); o refrigeración del recinto con frío industrial, como en los centros de datos. Para reducir el gasto en refrigeración, las empresas con grandes servidores están optando por localizarse en zonas muy frías. Por ejemplo, Facebook ha localizado uno de sus centros de datos en Suecia [30] y Microsoft, en cambio, está explorando la posibilidad de sumergir los suyos bajo el agua [24].

No solo existe la minería a gran escala, sino que hay muchos usuarios que participan en el proceso de minado desde sus hogares. Cuando se realiza minería a pequeña escala, interesa saber cuál es el consumo eléctrico del minado y cuáles son los dispositivos más adecuados, ya que el margen de beneficio es menor. Debido a las características del minado, puede llegar un momento en el que ya no sea rentable minar a nivel usuario.

1.2 OBJETIVOS

El objetivo principal de este trabajo es realizar un estudio energético de distintos dispositivos de minado de una criptomoneda basada en *Blockchain*. Esto permitirá saber en qué circunstancias y con qué dispositivo es más rentable minar, en función de la cotización real de la criptomoneda y de la potencia computacional de la red.

Para ello, se estudiará la programación del software de una aplicación de criptominado, que permitirá entender el proceso real de minado en *Blockchain*. Gracias a la programación heterogénea se ejecutará la aplicación de Ethereum en cada uno de los dispositivos de estudio. Posteriormente, se medirá el consumo energético tanto de forma directa, como indirecta, en los dispositivos de cómputo. Esto permitirá calcular la eficiencia energética de cada dispositivo en el proceso de minado. Finalmente, se realizará un estudio para determinar la viabilidad económica de minar a nivel usuario.

1.3 ALCANCE

La dificultad de este trabajo radica en el estudio en detalle del proceso de minado, en la aplicación de conocimientos de la rama de ingeniería eléctrica para la medición del consumo energético y finalmente, en el aprendizaje de ingeniería informática para: entender el funcionamiento de una red distribuida, el uso de las aplicaciones de minado y comprender el funcionamiento de los dispositivos de cómputo utilizados.

Primero, se debe entender cómo es el mecanismo de minado de bloques de la red Ethereum. Se trata de un conjunto de algoritmos complejos que aseguran que la red sea segura y de confianza. A grandes rasgos, estos algoritmos sirven para validar todas las transacciones que se realizan en la red.

Para el estudio energético, se han ejecutado dos aplicaciones de minado en distintos dispositivos de cómputo en una máquina Linux.

Se han obtenido los datos de potencia consumida durante el proceso de minado, con un periodo de muestreo de un segundo, en cada uno de los dispositivos utilizados. Estos datos se han analizado en Python. Esta aplicación ha permitido automatizar el proceso de gestión y representación de los datos obtenidos de cada uno de los ensayos realizados.

Además, se ha realizado un curso *online* de Aprendizaje Automático de 11 semanas. Esto brindó la oportunidad de implementar un algoritmo de Regresión Lineal [19], para realizar un análisis energético y económico sobre el proceso de minado con más detalle.

1.4 ORGANIZACIÓN DE ESTE DOCUMENTO

El documento se encuentra dividido en base a los pasos que se deben realizar para alcanzar el objetivo final.

El Capítulo 2 muestra los distintos dispositivos de cómputo que se usan hoy en día para el minado de *Blockchain*, el uso actual de criptomonedas y su relación con el *Blockchain*, y se explica la importancia que tiene el consumo energético en este sector.

En el Capítulo 3 se muestra la base teórica de Ethereum, cómo es la estructura de un bloque y cómo es el proceso de minado de bloques.

En el Capítulo 4 se describe con qué dispositivo y herramientass se ha trabajado, y cómo se ha implementado el algoritmo de minado.

En el Capítulo 5 se describen los distintos ensayos realizados y los resultados obtenidos.

En el Capítulo 6 se desarrolla el estudio económico que se ha llevado a cabo en torno al proceso de minado a nivel usuario.

Por último, en el Capítulo 7 se muestra la conclusión del proyecto y se hace un resumen de todos los objetivos que se han cumplido.

A continuación, se adjuntan los anexos en los que se incluyen el algoritmo de minado en detalle y los algoritmos de Aprendizaje Automático usados para el procesado de datos, una comparativa entre dispositivos más detallada y el diagrama de Gantt del proyecto.

2

ESTADO DEL ARTE

Este capítulo describe qué es la tecnología *Blockchain* y se presentan varios dispositivos de cómputo que existen para ejecutar la aplicación de Ethereum. Así mismo, se especifican los consumos estándar de cada uno de los dispositivos.

2.1 BLOCKCHAIN

Un modelo tradicional de almacenamiento de información está basado en un modelo centralizado, donde la arquitectura cliente-servidor da acceso a los datos.

Una de las alternativas a la centralización del registro de datos, es la tecnología *Blockchain*, que permite almacenar y transmitir datos en la red de una forma distribuida y segura [13].

La Figura 2 muestra una representación de las distintas formas de conexión de los nodos de una red [20]. Como se puede observar, en el esquema de la red centralizada todos los usuarios dependen de un único nodo. Si falla este nodo, todos sus clientes dejan de funcionar. En cambio, en una red distribuida, todos los nodos crean una malla interconectada, dando redundancia en el servicio.

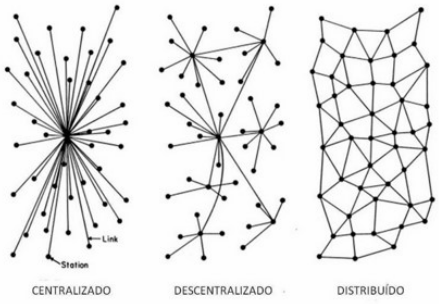


Figura 2: Esquemas de conexión de nodos en una red [33]

Blockchain, como su nombre indica, es una cadena de bloques. Estos bloques contienen cualquier tipo de información (transacciones, música, imágenes, contratos, código...). Cada bloque tiene una referencia de un único bloque que ya pertence a la cadena de bloques. Así se le

otorga a la red la condición de cadena. Pero, ¿cómo se consigue que los datos y transacciones se transmitan de forma segura si no hay un regulador del sistema?

Se consigue a través de la resolución de un problema matemático por parte de los nodos que soportan la red (mineros). Este proceso consta de dos fases. En primer lugar, se busca la solución (*Nonce*) del problema matemático. A este proceso se le denomina minado. En segundo lugar, los nodos de la red validan la solución propuesta por el minero.

Para explicar el funcionamiento de la red Ethereum, se ha creado un diagrama de flujo (Figura 3) en el que se representan las distintas etapas desde que se hace una transacción hasta que se une el bloque a la cadena.

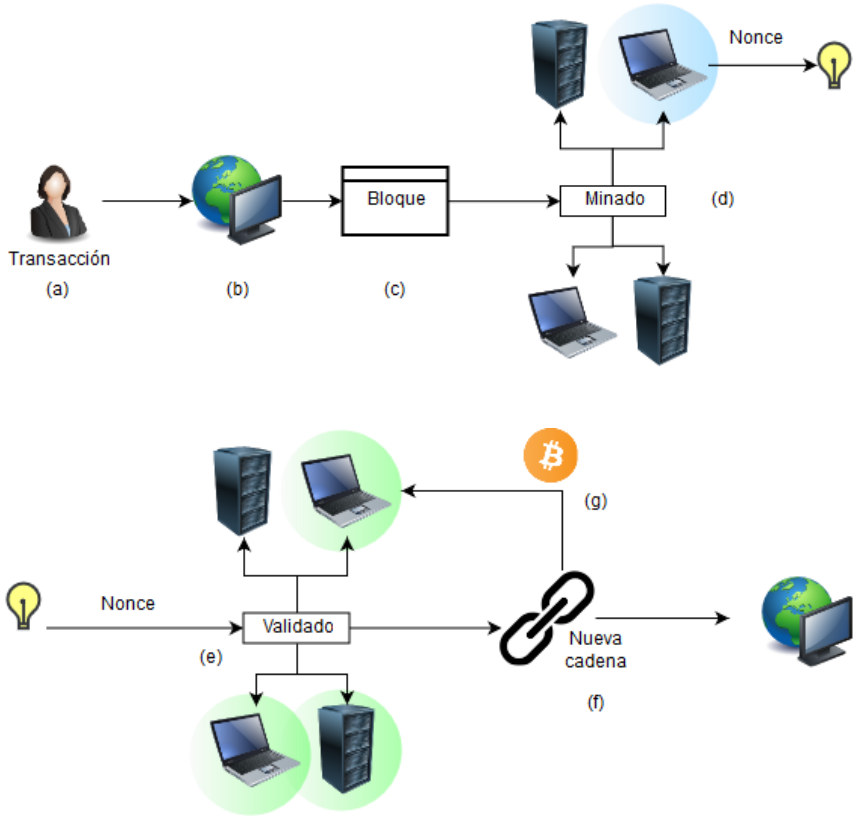


Figura 3: Representación del funcionamiento de la red Ethereum

Cuando un usuario quiere hacer una transacción (a), ésta se sube a la red de Ethereum (b). El software de Ethereum agrupa las transacciones de éste y otros usuarios en un bloque (c). El bloque se distribuye por cada uno de los mineros de la red Ethereum (d). Es aquí, donde los mineros tratan de obtener un *Nonce* lo más rápido posible. Cuando un usuario encuentra un *Nonce*, tiene que ser validado por al menos el 51 % de la red (e) para que se considere correcta. El proceso

de validación es muy rápido. Cuando la solución es correcta, se añade el bloque a la cadena y se aplica el contenido del bloque (contratos, transacciones, ...) (f). Finalmente, se recompensa económicamente al primer minero cuya solución haya sido validada por la red (g) [13]. En el Capítulo 3 se verá en detalle cómo es la estructura de un bloque y cómo es el proceso de minado de bloques.

A continuación, se muestran los distintos dispositivos que se utilizan actualmente para el minado de bloques.

2.2 DISPOSITIVOS DE MINADO

El proceso de minado son un conjunto de operaciones matemáticas discretas que tratan de encontrar un *Nonce* que cumpla una serie de condiciones. El problema matemático cambia con cada bloque que hay que añadir en la cadena de bloques que depende de: la información que contiene, cuánto tiempo costó minar el bloque anterior, la información del bloque actual (datos contenidos en el propio bloque) y del *Nonce*, que es el objetivo del minero.

Debido a las características del problema de búsqueda del *Nonce*, para su resolución, se pueden usar distintos dispositivos de cálculo como la CPU, GPU, FPGA y dispositivos dedicados ASICs. Como se dijo anteriormente, el objetivo del proyecto es el estudio del consumo y eficiencia energética de dispositivos de cálculo.

A continuación, se muestran las características de los dispositivos de cálculo usados actualmente en la industria, mostrando sus fortalezas y debilidades ante el minado, cuya complejidad varía con el tiempo función del número de mineros en la red.

2.2.1 *CPU*

De un modo simplificado, la Unidad de Procesamiento Central (CPU) es la parte de un computador que dirige y gestiona el orden de ejecución de las instrucciones de los programas. Es un dispositivo de cálculo de propósito general. El circuito integrado de una CPU está formado por dos elementos:

- Unidad de control: coordina y controla las operaciones que se hagan con los datos. Lee los datos necesarios de la memoria y activa los circuitos necesarios de la ALU.

- Unidad lógico-aritmética (ALU): realiza las operaciones aritméticas y lógicas con los datos que recibe de la unidad de control; procedentes de la memoria principal.

Además, este dispositivo está conectado con otras partes de gran importancia como son:

- Memoria principal: estructuras en el que se almacena datos e instrucciones, así como meta-información de la ejecución.
- Dispositivos de Entrada/Salida: permiten la comunicación con elementos ajenos al programa.

En la Figura 4 se muestra un esquema de un circuito integrado de una CPU.

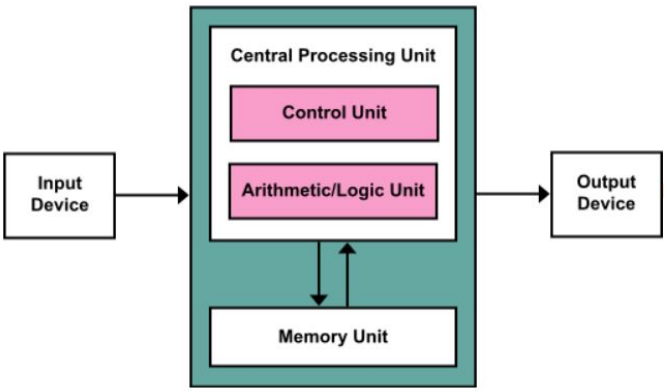


Figura 4: Esquema simplificado de la arquitectura de un circuito integrado de una CPU [31]

Se trata de un dispositivo muy flexible ya que se puede reprogramar. En cambio, es un dispositivo muy lento pese a trabajar a frecuencias elevadas, ya que trabaja de forma secuencial.

2.2.2 *GPU*

Una GPU es un circuito integrado originalmente concebido para generar imágenes. A partir del 2000 se empezaron a utilizar en otros problemas ya tiene una elevada capacidad de cálculo y se pueden utilizar en muchas aplicaciones. Por ejemplo, se utilizan para programas que requieran realizar muchas operaciones a la vez. A esta propiedad se le llama paralelismo. Funcionan muy bien en programas regulares. Con los irregulares, por ejemplo, un compilador, la CPU funciona mejor.

En la Figura 4 se representa el esquema de la arquitectura de una GPU

Figura 5: Esquema de la arquitectura de una GPU Maxwell GM204 [15]

Cada uno de los bloques verdes, representa una unidad de cálculo. Gracias a la arquitectura de una GPU se pueden paralelizar miles de operaciones. Concretamente, la GPU que se ha usado en el proyecto, dispone de 3072 cores. Pero en cambio, la capacidad de memoria por core que dispone es limitada.

La GPU tiene un amplio uso en la industria de simulaciones numéricas y videojuegos. Sectores donde las aplicaciones son intensivas en cálculo. Aprovechan las GPUs para paralelizar sus códigos y acelerar la ejecución de los mismos.

2.2.3 *FPGA*

La matriz de puertas programables (FPGA) es un dispositivo intermedio en rendimiento entre las CPUs o GPUs y los dispositivos ASICs. A partir de la programación de las puertas lógicas (CLB y *Switch Matrix*) de una única placa se consigue crear diferentes circuitos físicos. Se pueden programar tanto las operaciones aritméticas que ejecuta cada ALU, como con qué ALUs se comunica cada una de ellas. Gracias a ello, se pueden crear circuitos integrados especializados en realizar una única tarea. De este modo, las FPGA disponen de cierta flexibilidad.

En la Figura 6 se representa el esquema de la arquitectura de una GPU.

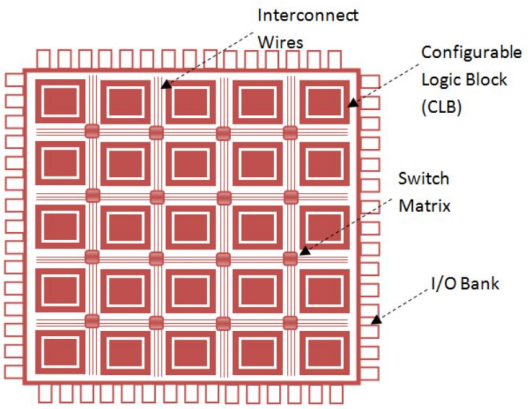


Figura 6: Esquema simplificado de la arquitectura de una FPGA [16]

Tanto las CPUs, como las GPUs y FPGAs son dispositivos que disponen de memoria donde cargar las instrucciones que tienen que realizar. Esto permite adaptar estos dispositivos a casi cualquier aplicación a través del software de programación. Por el contrario, existen dispositivos diseñados para un único propósito y con una programabilidad baja. A estos dispositivos se les denomina ASICS.

2.2.4 *ASICS*

Los Circuitos Integrados de Aplicaciones Específicas (ASICs) son dispositivos que integran un circuito específico para realizar un único algoritmo. Como inconveniente, estos dispositivos son muy poco flexibles. A diferencia de los dispositivos anteriores, estos no tienen la capacidad de programación.

La Figura 7 muestra un dispositivo ASIC que se usa hoy en día para minar Ethereum. Este dispositivo está creado exclusivamente y está optimizado para el minado de Ethereum, pero no se puede adaptar a otros algoritmos de minado.

Figura 7: Antminer E3

2.3 CARACTERÍSTICAS DE LOS DISPOSITIVOS

A modo de resumen, la Tabla 1 recoge las propiedades de los dispositivos mencionados anteriormente.

Cuadro 1: Consumo nominal energético de los distintos dispositivos de cómputo

Dispositivo	Fabricante	Modelo	Potencia (W)	Nucleos	Programable
CPU	INTEL	Skylake 6700k	91	4-8	Si
GPU	NVIDIA	GTX TITAN X	250	3072	Si
FPGA	Altera	Statix V	45	-	Si
ASIC	Antminer	E3	760	-	No

Como se puede observar en la Tabla 1 el dispositivo ASIC es el que mayor potencia consume. Del mismo modo, es el que, a priori, más rápido mina ya que se trata de un dispositivo diseñado exclusivamente para minar bloques. Esta familia de dispositivos son los que utilizan las grandes empresas dedicadas exclusivamente al minado.

En este proyecto se ha realizado el estudio energético sobre dos dispositivos de cómputo: CPU y GPU. Se quiere ver el consumo energético que llevan asociados durante el proceso de minado y cuál es la eficiencia energética de cada uno de ellos midiendo el número de transacciones que pueden validar por Julio y segundo.

3

PROCESO DE MINADO DE BLOQUES EN ETHEREUM

Ethereum es una red distribuida de nodos, como se ha descrito en el capítulo Capítulo 1. Estos nodos se pueden clasificar en dos tipos de usuarios: externos y mineros. Los usuarios externos utilizan la red Ethereum como plataforma de software. Realizan transacciones, implementan *Smart Contracts* o hacen cualquier otro uso de la red es decir, se aprovechan o explotan la red. Los mineros son los que mantienen la red *Blockchain* en funcionamiento. Son estos los que forman parte del sistema de consenso, manteniendo así la integridad de la red.

Un minero, tiene dos funciones: minar y validar. Estos procesos se pueden visualizar en la Figura 3 del Capítulo 2. Corresponden a las actividades (d) y (e) respectivamente. Durante el minado, los mineros compiten entre si para ser los primeros en resolver el problema matemático de búsqueda del *Nonce*. Este problema matemático es necesario para unir los bloques a la cadena y mantener en funcionamiento la red. Para atraer a usuarios a participar en esta actividad, la resolución del problema de búsqueda tiene un incentivo económico asociado. Cuando una solución es válida, el bloque se añade a la cadena y el minero que ha resuelto el problema se lleva una recompensa de 3 Ether [32].

Este problema matemático es muy complejo. De modo que para verlo en detalle, en primer lugar, es necesario explicar algunos conceptos como: qué es una función *hash*, cuál es la estructura de un bloque de la cadena y cómo es una transacción de Ethereum.

El objetivo del problema matemático consiste en encontrar un número, *Nonce*, que cumpla una característica determinada. El resultado (*target*) de aplicar una función (*hashimoto—full*) al *Nonce*, junto con otros parámetros, tiene que empezar por un número determinado de ceros. Este número de ceros define la dificultad del problema matemático que hay que resolver. El algoritmo de minado se verá en detalle al final del capítulo.

3.1 FUNCIONES HASH

Una función *hash* es una función inyectiva. Por lo tanto, a elementos distintos del conjunto X (dominio) les corresponden elementos distintos en el conjunto Y (codominio). La siguiente figura Figura 8 representa una función inyectiva.

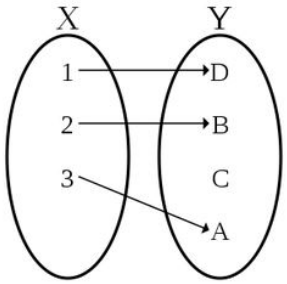


Figura 8: Esquema de una función inyectiva

Como se verá posteriormente, en la red Ethereum, se aplica esta función múltiples veces, a través de los distintos modelos de funciones *hash*. Es una función que permite crear una firma única a cualquier tipo de dato, ya sean imágenes, música, números o texto. En definitiva, cualquier tipo de información que se pueda expresar en una secuencia de bits.

Además, estas funciones tienen otras tres características importantes de mencionar:

- La primera de ellas es que, independientemente de la longitud de la cadena de entrada (dominio), el conjunto de salida (codominio) es siempre de longitud constante. En el caso de la función *hash* SHA-256, la salida serán 256 bits. En la figura Figura 9 se muestra un ejemplo de esta propiedad, donde la salida serán siempre 256 bits. Existen otras funciones *hash* como SHA-1, SHA-348 y SHA-512 [27].

- La segunda característica implica que, conocido el resultado de una función *hash* (codominio), es prácticamente imposible conocer los datos originales de entrada (su imagen). De esta forma los datos quedan “encriptados" de forma segura.

- Por último, las funciones *hash* están construidas de tal forma que, si se cambia 1 único bit del mensaje de entrada, se produce una salida totalmente distinta y aparentemente aleatoria. Esto protege los datos ante una posible manipulación.

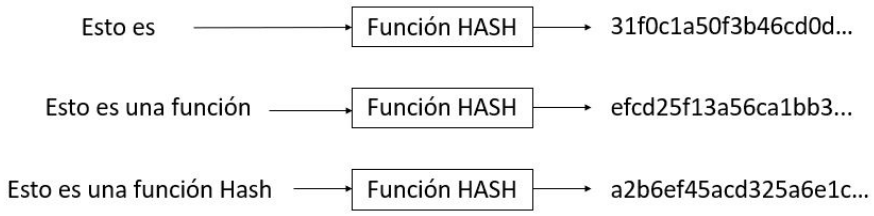


Figura 9: Ejemplos de funciones *hash*

3.2 ESTRUCTURA DE UN BLOQUE

Un bloque representa un conjunto información que se quiere a unir a la red *Blockchain*, o un conjunto de información que ya pertenece a la red y por tanto, es inmutable.

En esta sección se explica cada una de las partes de un bloque. En la figura Figura 10 se muestra la representación gráfica de un bloque de la cadena de Ethereum, diferenciando sus partes principales.

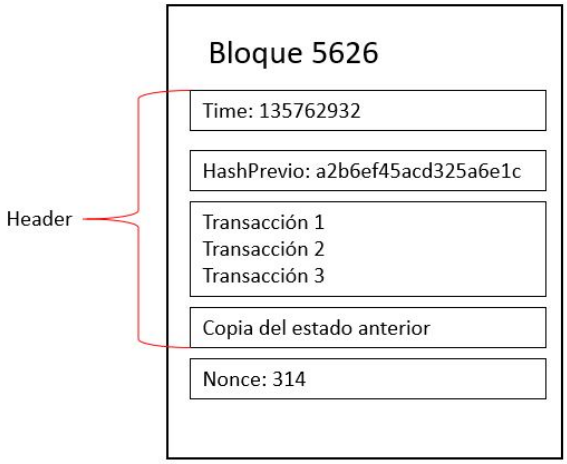


Figura 10: Representación de un bloque de Ethereum

El primer elemento de un bloque es el identificador. Este número representa qué puesto ocupa el bloque dentro de la *Blockchain*. Es un número único en la cadena.

El sello del tiempo representa el tiempo en el que la red de Ethereum creó el bloque. El sello del tiempo tiene que cumplir dos condiciones para que sea válido. En primer lugar, el tiempo de este bloque tiene que ser superior al valor del tiempo del bloque anterior. En segundo lugar, tiene que haber una diferencia máxima de 15 minutos con el bloque anterior [13]. En caso contrario, el bloque no es

válido. Acotar el tiempo entre bloques, dificulta la acción de los atacantes porque así disponen de un periodo de tiempo corto y limitado para actuar. Si la red es vulnerable, un usuario malicioso podría eliminar un bloque, por ejemplo, o incluso modidificar la información que contiene como las transacciones o los términos de un contrato.

Otro elemento importante, es el *hash* del bloque anterior. Es decir, el *hash* del bloque anterior que contiene toda la información de dicho bloque (transacciones, contratos, ...). Este es el punto en el que la red Ethereum adquiere la propiedad de cadena.

En cuarto lugar, el bloque está formado por el conjunto de transacciones que hay que ejecutar y una copia de la cadena de bloques del estado anterior.

El último elemento de un bloque es el *Nonce*, número que tendrán que encontrar los mineros mediante la ejecución de funciones *hash*. Depende de todos los datos que contenga el bloque.

A partir de ahora, se denominará *header*, al conjunto formado por las 4 primeras partes (número de bloque, sello del tiempo, *hash* del bloque anterior, transacciones y copia del estado anterior). El *header*, junto con el *Nonce* son parte de los datos necesarios para poder resolver el problema matemático.

Para terminar de ver la información que contiene un bloque, se muestran las características y la información que contiene una transacción de Ethereum.

3.2.1 *Elementos de una transacción*

Una transacción en Ethereum está formada por 5 elementos fundamentales [32]. En la figura Figura 11 se muestra la estructura de una transacción.

Figura 11: Representación de una transacción de Ethereum

Los dos primeros elementos son los usuarios involucrados en la transacción: el remitente y el destinatario. Esta información se muestra como una dirección pública de 160 bits. En caso de tratarse de un *Smart Contract*, el campo del destinatario estaría vacío [32].

Otro elemento de una transacción es el importe, medido en Ether.

El identificador es un número que asegura que una transacción se realiza sólo una vez. Así se evita lo que se denomina *Double Spend* [11]. Este número coincide con el número de transacciones que ha realizado el remitente [32].

Finalmente, se incluye información referente a la cantidad de cómputo que se le permite realizar a un minero para realizar una transacción. Se trata de una especie de comisión que cobra el sistema por cada instrucción que se tiene que realizar. De este modo, se protege a la red Ethereum ante la implementación de software que quiera atacar la red, por ejemplo, con un bucle infinito.

Los mineros realizan una serie de instrucciones para llevar a cabo una transacción. Cada instrucción tiene un coste computacional tabulado, que depende de la complejidad de estas instrucciones [32]. Cuanto más compleja sea la transacción, mayor será su coste. Por ejemplo, el coste asociado a una transacción económica es mucho menor que aquél asociado a la ejecución de un *Smart Contract* en el que intervienen varias partes y donde se corre un programa propio.

3.3 ALGORITMO DE MINADO

El algoritmo de minado realiza una serie de combinaciones entre los datos de entrada, varias funciones *hash* encadenadas y operacio-

nes matemáticas, de tal forma que se asegura que se ha realizado una cantidad mínima de computación al bloque.

El algoritmo de minado de Ethereum se recoge en Listing 1 [17].

```
1 def mine(full_size, dataset, header, difficulty):
2     target = zpad(encode_int(2^256 / / difficulty), 64)[::-1]
3     from random import randint
4     nonce = randint(0, 2^64)
5     while hashimoto_full(full_size,dataset,header,nonce)>target:
6         nonce = (nonce + 1) % 2^64
7     return nonce
```

Listing 1: Algoritmo de minado de Ethereum

A continuación, se detallan las lineas principales del algoritmo de minado:

- Linea 1: Definición de los datos de entrada del algoritmo.
- Linea 2: Cálculo del *target*, que representa el número de ceros por los que tiene que empezar la solución. La función *zpad* ajusta cualquier dato a una longitud determinada añadiendo ceros a la izquierda. En este caso, se jausta la longitud a 64 bits.
- Linea 4: Inicialización aleatoria del *Nonce* en el rango de 0 a 2^{64}.
- Linea 5 y 6: Iteración del *Nonce*, de uno en uno, hasta que se cumple la condición entre la función *hashimoto—full* y *target*. Se recorre todo el rango del *Nonce*. Cuando el valor máximo del rango se supera, se empieza de nuevo por el menor de ellos.

Para explicar el algoritmo en detalle, se ha dividido en tres partes: datos de entrada, obtención del *target* y la función *hashimoto—full*. Esta función es la que realmente comprueba si el problema se ha resuelto o no.

3.3.1 *Datos de entrada*

Los datos de entrada al algoritmo son: el *dataset*, que es una base de datos que se crea a partir de una semilla, el *header* del bloque que se quiere minar y por último, la dificultad del problema.

Ethereum está diseñado para que cada 15 segundos de media se realice una transacción [26]. Todos los usuarios que participan en el proceso de minado de la red Ethereum reciben, cada 15 segundos,

un bloque como el de la figura Figura 10 para resolver el problema matemático. Cuando el número de mineros de la red aumenta, la probabilidad de que alguno de ellos encuentre una solución válida en menos de 15 segundos, aumenta. Para que el tiempo medio entre trasacciones sea de 15 segundos, cuando un problema se ha resuelto en menos de 15 segundos, la dificultad del problema aumenta ligeramente para resolver el problema en algo más de 15 segundos. Es decir, la dificultad del problema matemático se ajusta automáticamente dependiendo del número de usuarios que haya en la red para mantener tiempo entre transacciones prácticamente constante.

Pero, ¿en qué consiste la dificultad del problema?

3.3.2 *Obtención del target y dificultad*

La función del minado *hashimoto–full* está diseñada para que tenga una distribución probabilística uniforme. El resultado de hacer la función *hashimoto–full* es un *hash* de 256 bits [17]. Cuando la dificultad es máxima, no hay ninguna simplificación del problema. Por tanto, existen 2^{256} diferentes combinaciones posibles. Al tratarse de una distribución uniforme, en el peor de los casos habría que recorrer completamente el dominio de 2^{256} combinaciones. En el mejor de los casos, se resolvería el problema en el primer intento, con una probabilidad de $1/2^{256}$.

La figura Figura 12 representa una solución con una dificultad elevada, ya que es necesario una combinación de 256 bits.

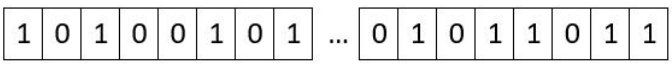


Figura 12: Representación de una solución de elevada dificultad

Cuando la dificultad del problema disminuye, el resultado de la función *hashimoto–full* tiene que empezar por un número determinado de ceros. Si, por ejemplo, el resultado tiene que empezar por 6 ceros, el problema se reduce a 2^{250} combinaciones, asegurando que el tiempo para encontrar la solución es menor que en el caso anterior. La figura Figura 13 representa una solución más fácil que la anterior.

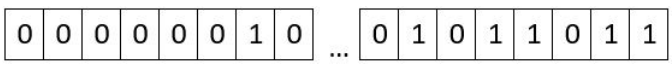


Figura 13: Representación de una solución de menor dificultad

3.3.3 *Función hashimoto-full*

Se trata de una función, que realiza funciones *hash* encadenadas, mezclado de bits entre varias variables, reordenación de bits y reducción o extensión de variables. Es decir, se ajusta la longitud de una variable a un determinado número de bits. El resultado de esta función se compara con el *target*. Cuando el resultado es mayor que el *target*, se ha encontrado el *Nonce* válido. El algoritmo completo de la función *hashimoto—full* se muestra en el Apéndice A.

El proceso de minado continua con la comprobación del resultado por al menos el 51 % de la red de Ethereum. Aquí, todos los nodos de la red reciben un bloque con un *Nonce* propuesto. Estos tienen que realizar la función *hashimoto—full* para comprobar si se cumple la condición impuesta en el algoritmo. Cuando ya se ha comprobado y validado, por el 51 % de la red, se procede a la inserción del bloque en la cadena y a recompensar al minero por haber sido el primero en dar una solución válida del problema.

La capacidad del minero de encontrar un *Nonce* válido depende de la potencia computacional que tenga disponible. Cuanto mayor sea la potencia disponible, mayor número de *Nonce* podrá realizar. Como la función *hashimoto—full* sigue una distribución probabilística uniforme, una mayor potencia computacional disponible, supone una mayor probabilidad de encontrar un *Nonce* válido. Esta es la razón por la que han nacido empresas dedicadas exclusivamente a invertir en hardware específico para minar (ASICs). Son las llamadas *Pool Miners*.

4

ENTORNO DE EXPERIMENTACIÓN

Este capítulo explica el proceso seguido para la medición del consumo energético y cálculo de la eficiencia energética en el proceso de minado en Ethereum. Además, se detallan las plataformas hardware, herramientas software y herramientas de medición que se han utilizado para el estudio del consumo energético durante el proceso de minado y posterior análisis económico.

4.1 PLATAFORMAS HARDWARE

El estudio se ha desarrollado sobre dos plataformas hardware disponibles en el departamento, instaladas en una estación de trabajo de 64 GB de memoria RAM llamada socarrat@unizar.es.

En primer lugar, se ha utilizado una CPU Intel Skylake 6700 k. Se trata de un dispositivo de cómputo de 4 núcleos, una frecuencia de reloj de 4 GHz y 8 MB de memoria cache.

El segundo dispositivo que se ha utilizado es una GPU NVIDIA GTX TITAN X. Un dispositivo de cómputo de 3072 núcleos, 1 GHz y 12 GB de memoria.

Los consumos eléctricos nominales (dados por el fabricante), se muestran en la Tabla 1 del Capítulo 2.

4.2 HERRAMIENTAS SOFTWARE

Para llevar a cabo los experimentos, se han utilizado dos aplicaciones oficiales de minado de Ethereum instaladas en socarrat. Una es específica para ejecutarla en la CPU, escrita en GO. La otra es específica para la GPU y está escrita en OpenCL. Dichas aplicaciones se obtuvieron del repositorio público *Github* [18] y [17]. En un principio se querían ejecutar la misma aplicación en ambos dispositivos, pero el código de la aplicación de la GPU no era compatible con la CPU, de modo que se optó por instalar las dos aplicaciones.

La aplicación instalada para ejecutar en la GPU tiene por defecto un modo *Benchmark* que se utiliza para comprobar la capacidad y rendimiento del dispositivo durante el proceso de minado. Además, permite configurar distintas opciones del minado, como elegir un bloque determinado para minar y establecer el tiempo disponible para encontrar el *Nonce* del bloque, entre otras. En este caso, se estableció que el tiempo disponible para encontrar el *Nonce* del bloque era de 24 horas. En la realidad, este intervalo de tiempo lo impone la red y son 15 segundos de media. Además, se modificó el código para que finalizara la simulación en el caso de haber encontrado un *Nonce* válido. Esto permitió comprobar la dificultad actual de minar un bloque con el *hardware* disponible.

La aplicación de la CPU es una aplicación de minado real, que no dispone de opción de *Benchmark*. Para ejecutarla, hubo que crear una cuenta real de Ethereum y especificar que la capacidad disponible para el programa era de 16 GB. Con menos memoria, el dispositivo no era lo suficientemente rápido como para iniciar el proceso de minado y comunicarse con la red.

4.3 HERRAMIENTAS DE ADQUISICIÓN DE DATOS

Una vez instaladas las dos aplicaciones, se realizaron ensayos de distintas duraciones para comprobar la estabilidad de los resultados en cada una de las plataformas *hardware* estudiadas. Se empezó con ensayos de larga duración. Se realizaron 3 ensayos de 24 horas y de 60, 30 y 10 minutos registrando el consumo energético [W], tanto para la CPU, como para la GPU. Se observó que los resultados permanecían muy constantes y que un ensayo de 10 minutos era suficiente para representar el comportamiento estacionario del consumo energético durante el minado de Ethereum. Así comenzó la fase de registro de datos.

Tanto para la CPU, como para la GPU, se han realizado ensayos de 10 minutos registrando las siguientes medidas:

- Potencia del dispositivo de cómputo en vacío: Potencia registrada con contadores *hardware* cuando no se está ejecutando ningún programa.
- Potencia del dispositivo de cómputo durante el proceso de minado: Potencia registrada con contadores *hardware* durante el minado. Se realizaron 2 experimentos y se calculó la media de los resultados.

- Potencia del computador (sistema completo) en vacío: Potencia registrada con el vatímetro cuando no se está ejecutando ningún programa.
- Potencia del computador (sistema completo) durante el proceso de minado: Potencia registrada con el vatímetro durante el minado. Se realizaron 2 experimentos y se calculó la media de los resultados.

Estos dispositivos disponen de unos contadores *hardware* mediante los cuales se puede acceder a los sensores internos que monitorizan la actividad del dispositivo. De este modo, se ha medido el consumo energético del dispositivo de cómputo de una forma mínimamente invasiva.

En el caso de la CPU, se tuvo que obtener permiso *root* para poder ejecutar la aplicación de minado y acceder a sus contadores y registrar el consumo energético. El comando utilizado se muestra a continuación.

```
1 perf stat -a -x, -I 1000 -e power/energy-cores/ ./geth --
      minerthreads=8
2  --mine --etherbase 5ce25cbab50b26425da2f3664630155ddcb99b05 --
      metrics  --cache 16384 2>Ensayo_CPU_X.csv
```

Listing 2: Linea de comando para medir consumo energético con el contador de la CPU

Perf es la herramienta de análisis de rendimiento utilizada, que permite la monitorización de distintas medidas. En concreto, se ha medido el consumo de la potencia de los *cores* de la CPU con un intervalo de 1 segundo. Después, se especifica la aplicación de minado sobre la cual se quiere medir y se añade una última instrucción para que se almacenen los datos registrados en un documento *.csv*. Para la ejecución de la aplicación de minado, además, hay que especificar cuál es la dirección de Etereum de socarrat y que la memoria cache son 16 GB.

Para medir el consumo energético consumido por la GPU con contadores hardware, se han utilizado las dos instrucciones que se muestran a continuación.

```
1 ./ethminer -G --opencl-platform 1 -M 1 --benchmark-trial 125
2 nvidia-smi dmon | tee Ensayo_GPU_X.txt
```

Listing 3: Linea de comandos para medir el consumo energético con el contador de la GPU

En primer lugar, se ejecuta la aplicación de minado de la GPU en modo *Benchmark*. Para ello se espcifica que se va a ejecutar sobre una GPU (-G), que está programada en OpenCL (–opencl) y que se encuentra en la plataforma 1. Además, se especifica qué bloque se quiere minar y cuál es la duración que se permite para encontrar la solución. En este ejemplo son 125 segundos.

En segundo lugar, se accede al contador *hardware* NVIDA smi y se especifica que se almacenen los datos registrados en un archivo *.txt*.

Estos resultados sólo representan una porción del consumo total del computador. En realidad, el consumo total durante proceso de minado incluye el consumo de los ventiladores, transformadores, dispositivos de cómputo, memorias, discos duros, placa madre...

Para determinar el consumo total durante el proceso de minado, se ha instalado un vatímetro YOKOGAWA WT210 (Figura 14) entre la conexión del computador y la red eléctrica. De esta forma se ha podido medir el consumo total [W] y calcular la fracción que representa el consumo del dispositivo de cómputo frente al consumo energético total.

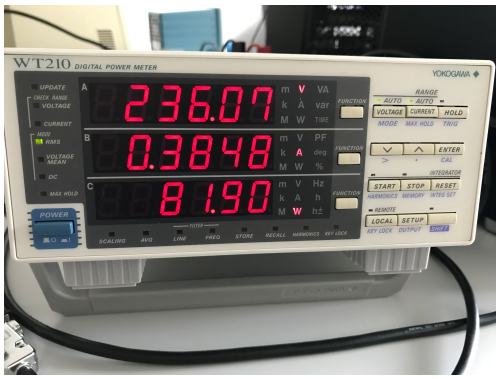


Figura 14: Vatímetro utilizado

El vatímetro utilizado, permite registrar los valores de voltaje [V], intensidad [A] y potencia [W] con un periodo de muestreo de 1 segundo y almacenarlos en un documento *.csv*. El modo de conexión para medir intensidad y voltaje del computador se muestra en la Figura 15.

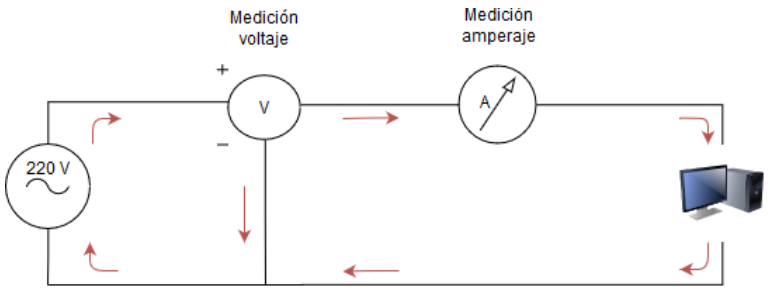


Figura 15: Vatímetro utilizado

En el siguiente capítulo se muestran los resultados del consumo energético obtenidos durante el proceso de minado en cada uno de los dispositivos de cómputo. Así como los resultados de eficiencia energética en el proceso de minado.

5

ENSAYOS REALIZADOS

Este capítulo recoge los resultados del consumo energético durante el proceso de minado en los dos dispositivos de cómputo empleados en el proyecto (CPU y GPU). Para cada uno de los dispositivos, se han obtenido los consumos de potencia eléctrica del dispositivo en vacío, potencia del dispositivo durante el proceso de minado, potencia del computador en vacío y potencia total del computador, que se han detallado en el Capítulo 4.

Los datos de consumo eléctrico individual de cada dispositivo se han recopilado a través de contadores *hardware*. Los contadores *hardware* son un mecanismo arquitectónico que almacena en registros datos de la ejecución de los programas como pueden ser el número de instrucciones ejecutadas, ciclos de reloj transcurridos o incluso el consumo energético. Estos contadores pueden tener una ligera influencia en las medidas del consumo energético del dispositivo en vacío, especialmente en el caso de la CPU, cuyo consumo energético en vacío es muy bajo. Por otro lado, las potencias totales del sistema se han registrado con el vatímetro anteriormente mostrado.

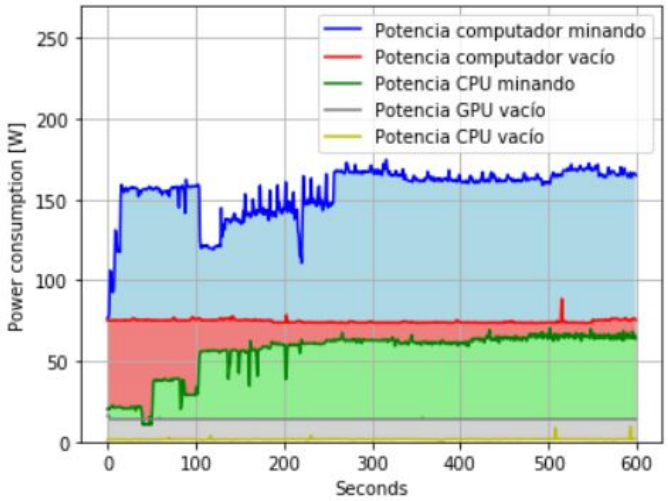
En primer lugar, se muestran en detalle de los consumos energéticos de cada uno de los dispositivos (CPU y GPU). Esto permite determinar qué partes del computador (sistema completo) consume la mayor parte de la energía.

Después, se muestra una tabla comparativa del consumo energético de los dos dispositivos de cómputo empleados: CPU y GPU. También se incluye, para ver las diferencias con un dispositivo específico de minado, el consumo del ASIC Antminer E3. Este dato no se ha comprobado ya que el coste del dispositivo es prohibitivo para nosotros. A cambio, se muestra el consumo eléctrico que aparece en la hoja de características de un fabricante de Antminer E3. [9].

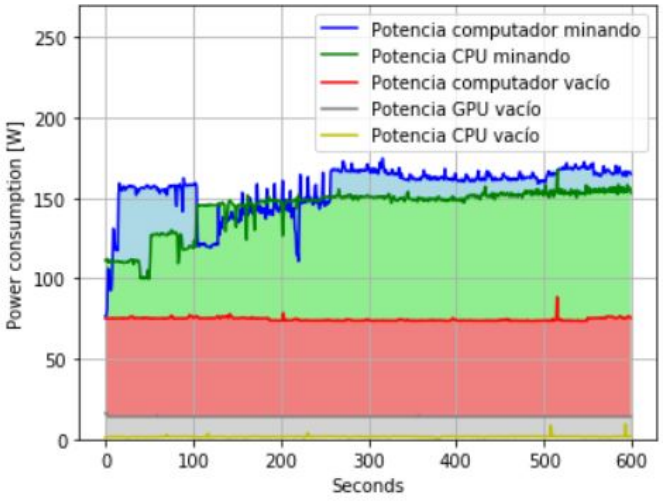
Además, se incluyen los datos referentes a la eficiencia energética obtenida en el proceso de minado en los dos dispositivos.

5.1 MINADO EN CPU

En la Figura 16 se representan los resultados del consumo energético medio medido durante dos ensayos de minado en la CPU durante 10 minutos. Se representan tanto las medidas de los contadores, como la total del vatímetro en azul.



(a) consumos energéticos individuales



(b) consumos energéticos combinados

Figura 16: Consumos energéticos durante el minado en CPU

En la figura (a) se representan, de forma individual, cada uno de los consumos eléctricos registrados durante el minado en CPU empezando desde cero. Es decir, los consumos no están apilados y tienen el mismo origen de ordenadas.

En primer lugar, se puede observar que el consumo en vacío de la CPU (amarillo), medido con contadores *hardware*, es prácticamente despreciable. Supone un consumo medio de 1.5 W.

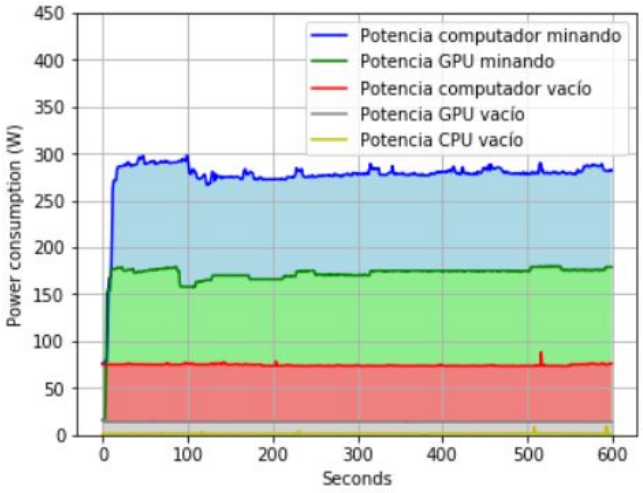
Además, se puede observar que, durante los primeros segundos, los valores registrados con el vatímetro tanto de la potencia del computador (azul), como de la CPU (verde), presentan un comportamiento transitorio similar. Este comportamiento transitorio se debe a que el proceso de minado no empieza hasta que se ha generado la base de datos (DAG) y se tiene la última versión de la cadena. Estos dos consumos tienen un comportamiento similar ya que es la CPU quien hace el trabajo (verde), y queda reflejado en el consumo total del computador (azul). A partir del segundo 250 aproximadamente, el proceso de minado comienza y por eso las potencias se estabilizan. Las potencias eléctricas medias son 164 W y 64 W, respectivamente.

La mayor parte del consumo en vacío del computador (rojo), se debe al consumo de la memoria de la GPU, ventiladores instalados en el computador, la placa base, y discos duros. Se trata de una potencia media de 79 W, consumo mayor que el consumido por la CPU durante el proceso de minado, 64 W, 2/3 del máximo de la CPU.

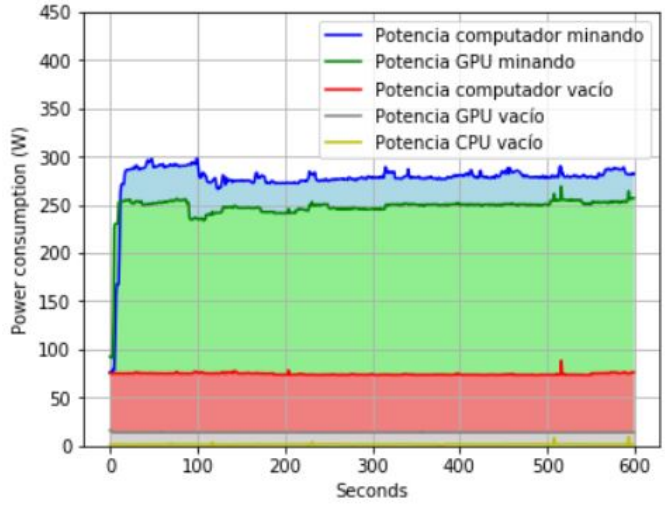
Si se suman la potencia de vacío del computador, la potencia de vacío de la GPU, y la de minado en CPU, se obtiene la potencia total teórica de minado. Se puede observar en la figura (b) que, en el tramo estacionario de la línea verde (suma de las 3 potencias anteriores), está muy cerca del consumo medido con el vatímetro (azul). Esta pequeña diferencia (en torno al 10 %) podría deberse a que los contadores realizan estimaciones del consumo energético del dispositivo, o que la propia presencia del vatímetro en el circuito tiene una pequeña influencia.

5.2 MINADO EN GPU

La Figura 17, representa los datos del consumo energético medio obtenidos durante el minado en GPU durante dos simulaciones de 10 minutos. Al igual que con la CPU, se muestran dos gráficas. La primera, representa los resultados obtenidos de forma individual. La segunda figura representa la potencia teórica de minado. Es decir, la suma de la potencia de vacío del computador, la potencia de vacío de la CPU y la de minado de la GPU.



(a) consumos energéticos individuales



(b) consumos energéticos combinados

Figura 17: Consumos energéticos durante el minado en GPU

Como se puede observar en la primera figura (a), los valores permanecen prácticamente constantes, salvo por alguna variación debida a las instrucciones internas del *Benchmark* utilizado.

Comparando con el consumo de la CPU, se puede observar que el consumo de la GPU es mucho mayor. El consumo eléctrico del computador en vacío es de 79 W y el consumo medio de la GPU durante el proceso de minado es 172 W.

En segundo lugar, el consumo total del computador se incrementa hasta los 274 W. Esto supone un incremento del 56 % con respecto a la potencia total del computador consumida durante el proceso de minado en la CPU.

Además, se puede observar, que el consumo de la GPU durante el proceso de minado (172 W) es mucho mayor que el consumo en vacío del computador (79 W).

El consumo en vacío de la GPU es de 14 W de media. Un orden de magnitud superior a la potencia en vacío de la CPU 1.5 W, pero es despreciable con respecto a la potencia registrada durante el proceso de minado.

En la segunda figura (b), se puede observar que existe una diferencia del 10 % entre el consumo real medido con el vatímetro y el obtenido sumando las potencias consumidas, que teóricamente se producen durante el proceso de minado.

5.3 COMPARATIVA DE CONSUMOS ENERGÉTICOS

En la Tabla 2, se muestran los datos obtenidos de potencia consumida durante el proceso de minado en cada uno de los dispositivos. Además, se incluye el porcentaje que representa el consumo de cada dispositivo, con respecto al consumo total del computador durante el proceso de minado.

Cuadro 2: Potencia consumida en el dispositivo y computador en el proceso de minado

Dispositivo	Consumo dsip. [W]	Vatímetro [W]	Fracción [%]
CPU	64	164	39 %
GPU	172	274	62.7 %
Antminer E3	760[1]	-	-

5.4 EFICIENCIA ENERGÉTICA DE LOS DISPOSITIVOS

Para realizar el estudio de eficiencia energética durante el proceso de minado, se han medido el número de *hash* que realizan cada segundo (*hashrate*) cada uno de los dispositivos. Estos datos se muestran durante la ejecución de las aplicaciones de minado de Ethereum. Conociendo estos datos y cuál es el consumo energético de cada dis-

1 Se han considerado sólo los datos facilitados por el fabricante del Antminer E3. No se han comprobado experimentalmente. Estos datos sólo se usaron para realizar una estimación en el estudio económico.

positivo, se obtiene la eficiencia energética, definida como *hash*/J. Estos resultados se muestran en la Tabla 5.

Cuadro 3: Eficiencia energética de los dispositivos de minado

Dispositivo	Consumo disp. [W]	Hashrate [MH/s]	Eficiencia [H/J]
CPU	64	0.25	3906
GPU	172	18	104651

Como se puede observar, la GPU 26 veces más eficiente que la CPU. Además, la velocidad de cómputo de la GPU es mucho mayor a la de la CPU. La GPU realiza un 7100 % más de operaciones que CPU por segundo. Esto influye directamente en el tiempo necesario hasta que se encuentra una solución válida al problema matemático.

6

VIABILIDAD ECONÓMICA DEL PROCESO DE MINADO

Este capítulo recoge el desarrollo del estudio económico llevado a cabo sobre el proceso de minado.

Como se ha podido observar en el capítulo anterior, el proceso de minado lleva asociado un gran consumo energético. Esto se traduce en gasto económico, pero afortunadamente el minado tiene una recompensa económica de 3 Ether por cada bloque minado. La pregunta que surge es: ¿es rentable el proceso de minado a nivel usuario?

En primer lugar, hay que ver cómo es la situación actual de la red Ethereum y qué tendencias predominan. La figura Figura 18 muestra los valores históricos de la moneda Ether en dólares, en rojo, y la potencia computacional de la red, en azul. La potencia computacional de la red es el número de *hash* por segundo que hay que se realizan para minar un bloque en un tiempo medio de 15 segundos. Es decir, el número de cálculos necesarios que hay que realizar hasta encontrar la solución al problema matemático.

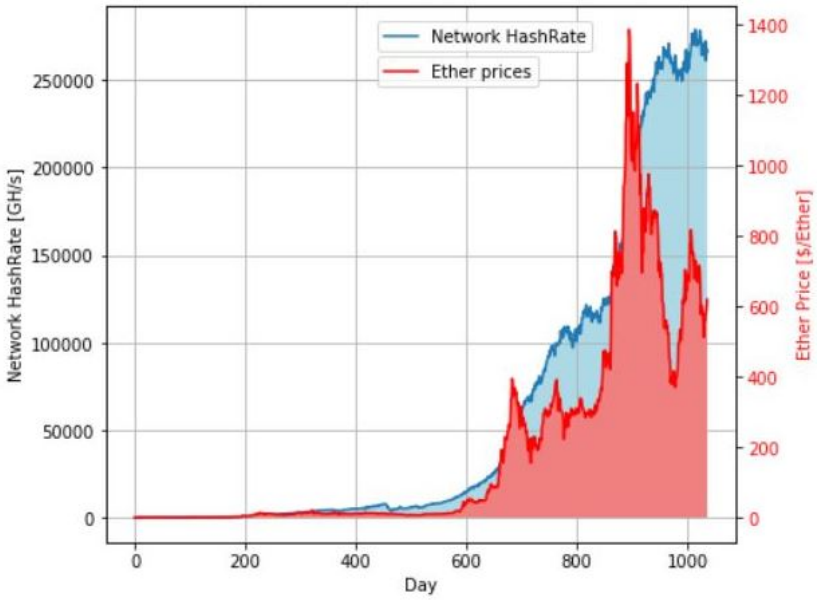


Figura 18: Potencia computacional de la red y cotización del Ether

La tendencia del precio no se ha estudiado ya que, como se puede observar en la figura, es muy volátil. En cambio, la potencia de la red ha ido creciendo desde el *Boom* de las criptomonedas, entre marzo y abril de 2017, independientemente de si el valor de la moneda subía o bajaba. De esta forma, se ha considerado que desde la fecha del *Boom* el crecimiento ha sido lineal.

Para comprobarlo, se ha calculado con una herramienta de Aprendizaje Automático (regresión lineal multivariable), programada *Python*, la línea que mejor se aproxima a la evolución de la potencia de la red desde el *Boom*. Este algoritmo calcula los parámetros de la recta que mejor se aproxima a los datos de la gráfica de forma automática. Se decidió usar este algoritmo ya que de esa forma se podría ampliar el estudio sobre la influencia conjunta de distintos factores en la red Ethereum. El código de este algoritmo se muestra en el Apéndice B.

En la figura Figura 19 se puede observar la superposición de la línea de regresión sobre los datos históricos de la potencia de la red desde el *Boom*.

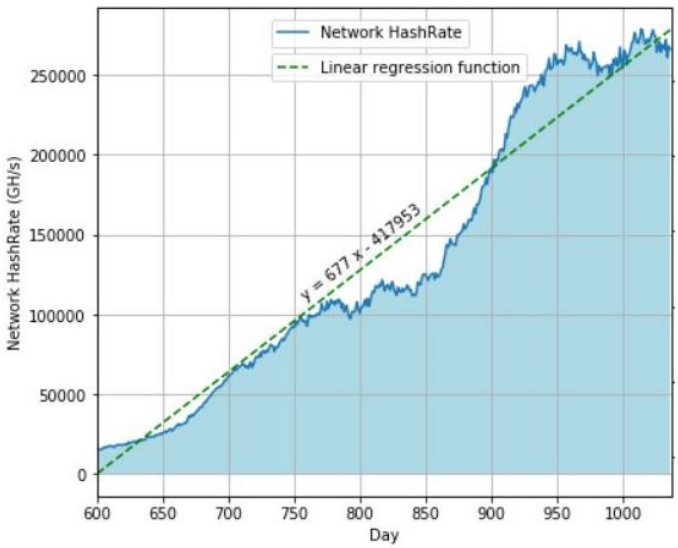


Figura 19: Potencia computacional ajustada con regresión lineal

Se puede observar, que la evolución de la potencia de la red ha experimentado un crecimiento lineal desde el *Boom* de las criptomonedas.

En este proyecto se han tomado dos referencias temporales para el estudio económico: 04/06/2018 y 31/08/2018, días 1036 y 1130 desde el inicio de la red respectivamente. Pese a la tendencia lineal observada en la figura Figura 19, la potencia de la red en este intervalo de tiempo ha permanecido prácticamente constante. En cambio, la

cotización del Ether ha sufrido grandes variaciones, como se puede observar en la figura Figura 18.

En la tabla Tabla 4 se muestran los datos del precio, potencia computacional de la red y número total de *hash* que hay que realizar para minar un bloque, suponiendo que el tiempo para minar es siempre de 15 segundos, de las dos fechas consideradas.

Cuadro 4: Cotización del Ether, potencia computacional de la red y número total de *hash* hasta encontrar la solución

Día	Precio [€/Ether]	Potencia red [GH/s]	Total [GH]
04/06/2018	532	266067	3991005
31/08/2018	206	280439	4206585

Como se puede observar en la tabla anterior, en el intervalo de tiempo considerado, el precio ha sufrido una variación del 61 %, mientras que la potencia sólo ha variado un 5.4 %. Las condiciones el 31/08/2018 son mucho más desfavorables para minar, ya que el precio ha bajado drásticamente y la potencia ha subido ligeramente. Esta potencia es la que se va a comparar con la capacidad de cálculo de cada dispositivo. Así se verá cuánto tiempo se tarda en minar un bloque con cada uno de ellos.

6.1 ESTUDIO ECONÓMICO

Se ha realizado un estudio de viabilidad económica sobre el proceso de minado tanto en CPU, como en GPU. Se incluye también los resultados teóricos del Antminer E3, como curiosidad, ya que es un dispositivo que acaba de salir al mercado y es específico para el minado de Ethereum. El estudio se divide en dos partes. En primer lugar, se ha realizado un estudio de los gastos y beneficios obtenidos en el proceso de minado. En segundo lugar, se ha hecho un análisis del plazo de recuperación de la inversión.

Como se vio en la Tabla 3 del Capítulo 5, existen grandes diferencias entre el número de *hash* por segundo que pueden realizar la CPU y la GPU. Como se verá a continuación, esto es de gran importancia.

Para ver el efecto de esta diferencia de las capacidades de cómputo entre la CPU y GPU, en primer lugar, se ha calculado el tiempo que se tardaría en minar un único bloque, el gasto energético y el beneficio que se obtendría, si se consideran los datos del 04/06/2018. Estos

resultados se muestran en la figura Tabla 5. Se incluye los datos que se obtendrían hipotéticamente del Antminer E3.

Cuadro 5: Tiempo hasta minar un bloque, gasto eléctrico y beneficio final de tres dispositivos de cómputo con las condiciones del 04/06/2018

Dispositivo	HashRate [MH/s]	Tiempo [años]	Electricidad [€]	Beneficio [€]
CPU	0.25	506	29288	-27691
GPU	18	7	1093	503
Antminer E3	190[1]	8 [meses]	457	1139

Como se puede observar en la tabla anterior, la CPU es el dispositivo menos idóneo para minar ya que es imposible conseguir resolver el problema en un periodo de tiempo razonable. Se trata de un dispositivo tan lento en el minado de bloques que necesita una enorme cantidad de electricidad para resolver el problema matemático. Como resultado, el proceso de minado con CPUs implica grandes pérdidas económicas. En cambio, minar con la GPU, de acuerdo a las constantes del día 04/06/2018 era rentable. Pese a necesitar 7 años para minar el bloque, el balance neto entre gastos en electricidad y beneficio es positivo. Lo mismo ocurre con el dispositivo Antminer E3. De la tabla anterior se puede concluir que cuanto mayor sea el HashRate del dispositivo, mayor será el beneficio obtenido.

Es importante recalcar que el tiempo mostrado en todas las tablas es el tiempo necesario para resolver el problema matemático de un único bloque en función de la potencia de la red en la fecha considerada. En el proceso de minado real, cada 15 segundos de media, se recibe un nuevo bloque a resolver. Esto significa que el problema se empieza de cero cada 15 segundos.

La tabla Tabla 6 recoge los datos obtenidos si se consideran los datos del día 31/08/2018. Como la potencia de la red ha permanecido prácticamente constante entre las dos fechas, se puede comprobar la influencia de la cotización del Ether sobre el beneficio obtenido.

Cuadro 6: Tiempo hasta minar un bloque, gasto eléctrico y beneficio final de tres dispositivos de cómputo con las condiciones del 31/08/2018

Dispositivo	HashRate [MH/s]	Tiempo [años]	Electricidad [€]	Beneficio [€]
CPU	0.25	533	30870	-30251
GPU	18	7.4	1152	-533
Antminer E3	190	8.4 [meses]	482	136

Se puede observar, que los beneficios han caído drásticamente. En el caso de minar con GPU ya no saldría rentable, ya que supondría

una pérdida de 532 €. Si se minara con el Antminer E3, teóricamente, seguiría siendo rentable. Entonces, la pregunta que aparece es, ¿a partir de qué precio es rentable minar? Para este cálculo se ha considerado que la potencia de la red permanece constante.

Como se ha comentado anteriormente, por cada bloque minado se obtienen 3 Ether. Teniendo en cuenta el coste energético asociado a cada dispositivo para minar un bloque, se puede obtener el precio mínimo del Ether para cubrir los gastos, y por tanto obtener rentabilidad en el proceso de minado. La tabla Tabla 7 recoge la cotización mínima del Ether a partir del cual sería rentable minar, si la potencia es la correspondiente al 31/08/2018.

Cuadro 7: Precio límite del Ether de tres dispositivos de cómputo para cubrir los gastos eléctricos de minado

Dispositivo	Cotización Ether [€/Ether]
CPU	10290
GPU	384
Antminer E3	160

Hasta ahora se ha considerado el tiempo necesario para minar un único bloque, independientemente de que cada 15 segundos se empieza el problema desde cero. De modo que una pregunta interesante que surge es, ¿cuántos dispositivos se deberían tener para minar un bloque en un periodo de 15 segundos?

Este cálculo se ha realizado para el día 31/08/2018, ya que el número de unidades necesarias solo depende de la potencia de la red, que ha permanecido constante en los últimos meses.

La figura Tabla 8 muestra los resultados obtenidos.

Cuadro 8: Unidades necesarias de tres dispositivos de cómputo para minar un bloque en 15 segundos

Dispositivo	Millones de unidades
CPU	1122
GPU	16
Antminer E3	2

Como se puede observar, el número de CPUs y GPUs que se necesitan para conseguir resolver el problema matemático en 15 segundos,

de acuerdo a la potencia actual de la red, es enorme. Se trata de millones de unidades.

Finalmente, se ha calculado el plazo de recuperación de la inversión, o *Payback* en inglés, del proceso de minado en cada uno de los dos dispositivos y en las dos fechas consideradas, de acuerdo a la Ecuación 1,

$$Payback = \frac{\text{Inversión}}{\text{Beneficio}} = \frac{\text{Inversión}}{3 \cdot \frac{€}{\text{Ether}} - \text{Gastos}} \tag{1}$$

donde la inversión representa el coste del dispositivo [€], y los gastos son los costes [€] del consumo energético del dispositivo hasta minar un bloque, medido con contadores *hardware*. Cuando este gasto es superior a la recompensa económica por minar un bloque, el beneficio es negativo y por tanto el *Payback* es negativo. Estos casos se especifican en la tabla como inversiones No recuperables.

La Tabla 9 muestra el *Payback* de la inversión, con los datos del 04/06/2018.

Cuadro 9: Periodos de tiempo hasta la recuperación de la inversión inicial

Dispositivo	Inverisón [€]	Gastos [€]	Total [€]	Beneficio [€]	Payback [años]
CPU	292	29289	29581	-27984	No recuperable
GPU	817	1093	1910	-313	No recuperable
Antminer E3	886	458	1343	254	5.3

La Tabla 10 muestra el *Payback* de la inversión, con los datos del 31/08/2018.

Cuadro 10: Periodos de tiempo hasta la recuperación de la inversión inicial

Dispositivo	Inverisón [€]	Gastos [€]	Total [€]	Beneficio [€]	Payback [años]
CPU	292	30871	31163	-30544	No recuperable
GPU	817	1152	1970	-1350	No recuperable
Antminer E3	886	482	1369	-749	No recuperable

Como se puede observar en las dos tablas anteriores, si se considera la inversión inicial en *hardware* y el precio actual de la electricidad (0.12 €/kWh) no es rentable minar con ninguno de los 3 dispositivos considerados (la columna gastos depende del precio del kilovatio hora). En países con la electricidad más barata como en China, con un precio en torno a 6 €/kWh, podría seguir siendo rentable minar.

Si además se considerara el gasto eléctrico total del computador durante el minado, en vez de sólo el consumo de los dispositivos medidos con los contadores *hardware*, la situación sería todavía mucho más desfavorable ya que el gasto económico asociado al proceso de minado sería todavía mayor. Esto se puede observar en la Tabla 11 y Tabla 12.

Cuadro 11: Periodos de tiempo hasta la recuperación de la inversión inicial teniendo en cuenta el consumo del computador (04/06/2018)

Dispositivo	Inverisón [€]	Gastos [€]	Total [€]	Beneficio [€]	Payback [años]
CPU	292	75052	75345	-73747	No recuperable
GPU	817	1742	2559	-961	No recuperable
Antminer E3	886	458	1343	254	5.3

Cuadro 12: Periodos de tiempo hasta la recuperación de la inversión inicial teniendo en cuenta el consumo del computador (31/08/2018)

Dispositivo	Inverisón [€]	Gastos [€]	Total [€]	Beneficio [€]	Payback [años]
CPU	292	79106	79399	-78779	No recuperable
GPU	817	1836	2653	-2033	No recuperable
Antminer E3	886	482	1368	-749	No recuperable

Se puede observar que los gastos asociados al consumo eléctrico son casi el doble que los gastos energéticos cuando sólo se considera el consumo del dispositivo de cómputo, en el caso de la CPU. Esto se debe a que, como el consumo de la CPU es el 39 % del consumo total, se produce un error del 61 % si no se considera en los cálculos. En la GPU aumentan también el gasto, pero no tan drásticamente. Esto se debe a que el consumo de la CPU es el 62 % del consumo total. De esta forma, el error cometido es del 38 % si no se considera el consumo total en los cálculos.

A lo largo del estudio económico se ha podido observar que el precio del Ether es clave en la rentabilidad del minado a nivel usuario, ya que la potencia de la red ha permanecido prácticamente constante en el intervalo de tiempo estudiado.

6.2 CALCULADORAS ONLINE

En Internet existen calculadoras *online* que permiten conocer la rentabilidad de un dispositivo cualquiera conociendo su consumo nomina, HashRate, y la situación actual de la red, como el precio del Ether, el tiempo medio de minado y la potencia computacional. Estas cal-

culadoras actualizan de forma automática las propiedades de la red, dando una estimación en tiempo real de los beneficios que teóricamente se obtendrían en el proceso de minado con un dispositivo [14] y [10]. Los datos que ofrecen las páginas web consultadas, no ofrecen resultados históricos sobre la rentabilidad de los dispositivos, de modo que para realizar una comparativa con los datos obtenidos en el proyecto, se han considerado los datos obtenidos en dichas páginas web el 11/09/2018.

Las propiedades de la red del 11/09/2018 se muestran en la Tabla 13. La comparación se ha realizado sólo para el dispositivo Antminer E3 porque es el único dispositivo del cual se han encontrado datos sobre el *Payback*.

Cuadro 13: Propiedades de la red Ethereum el 11/09/2018

HashRate red [GH/s]	Precio [€/Ether]	Tiempo medio [s]
266052	166	14.1

De acuerdo a los datos de la red, y a las características del dispositivo Antminer E3 recogidos en la Tabla 3 del Capítulo 5, se han obtenido: el tiempo hasta minar un bloque [días], el gasto energético del dispositivo [€/día], beneficio [€/día] y *Payback*. Los resultados se muestran en la Tabla 14.

Cuadro 14: Resultados obtenidos sobre el Antmier E3

Inverisón [€]	Tiempo [días]	Gasto [€/día]	Beneficio [€/día]	*Payback* [días]
1085	228.5	1.88	0.29	3656

Para compararlos con una calculadora *online*, la Figura 21 recoge los datos obtenidos de la página de estadísticas de Ethereum (Etherscan) correspondientes al minado con el Antminer E3 el 11/09/2018. Incluye además, el tiempo necesario hasta minar un bloque.

$ Calculated Mining Earnings :

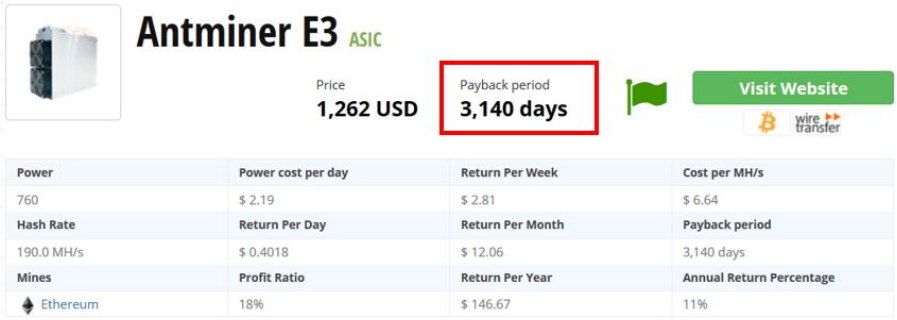
Duration	Ether Earned	Power Cost	Profit
Per Hour	0.000543151743764851 ($0.1048)	$0.0912	$0.0136
Per Day	0.0130356418503564 ($2.5161)	$2.1888	$0.3273
Per Week	0.091249492952495 ($17.6130)	$15.3216	$2.2914
Per Month	0.391069255510693 ($75.4842)	$65.6640	$9.8202

It will take you an average of 230.14 days to find 1 Block

Figura 20: Resultados obtenidos en Etherscan del minado con Antminer E3 [14]

Como se puede comprobar, los datos que se han obtenido en el proyecto sobre el tiempo hasta minar un bloque y beneficio diario, se aproximan mucho a los proporcionados por una herramienta *online* comercial.

Para completar la comparativa, la Figura 21 muestra el *Payback* proporcionado por uno de los foros de referencia en criptomonedas, CryptoCompare [10]. Este foro actualiza en tiempo real los valores de la red de Ethereum y realiza una estimación sobre el plazo de recuperación de la inversión.



Antminer E3 ASIC

Price **1,262 USD**

Payback period **3,140 days**

Visit Website

wire transfer

Power	Power cost per day	Return Per Week	Cost per MH/s
760	$ 2.19	$ 2.81	$ 6.64
Hash Rate	**Return Per Day**	**Return Per Month**	**Payback period**
190.0 MH/s	$ 0.4018	$ 12.06	3,140 days
Mines	**Profit Ratio**	**Return Per Year**	**Annual Return Percentage**
Ethereum	18%	$ 146.67	11%

Figura 21: *Payback* del Antminer E3 [10]

Se puede observar que el *Payback* es de 3140 días. Si se compara con los 3656 días, que es el resultado obtenido en el proyecto, supone una diferencia del 14 %. Estas calculadoras *online* realizan el cálculo considerando sólo el consumo nominal del dispositivo de cómputo. En realidad, habría que considerar el consumo total del computador, o de la fuente de alimentación (1600 W [23]), si se mina con el Antimer E3. Esto supone una mayor inversión y mayor consumo energético todavía.

En el Apéndice C se muestra una comparativa entre los resultados, de beneficio y gasto diario, que los fabricantes muestran y los obtenidos con el consumo real obtenido en el proyecto para la CPU y GPU. Hay que recalcar, que los fabricantes hacen el cálculo suponiendo sólo las características nominales del producto.

Para terminar, del estudio económico anterior se obtienen dos conclusiones principales.

En primer lugar, la cotización del Ether es uno de los factores clave para la viabilidad de estos proyectos. Este valor es totalmente especulativo y por tanto tiene una alta volatilidad. Como se puede observar en la Figura 22, desde que se inició el proyecto hasta hoy 11/09/2018, la cotización ha caído un 68 %. Ha pasado de valer 532 € a 170 € en apenas 3 meses. Esto hace que cada día sea más complicado obtener beneficio minando bloques en Ethereum.

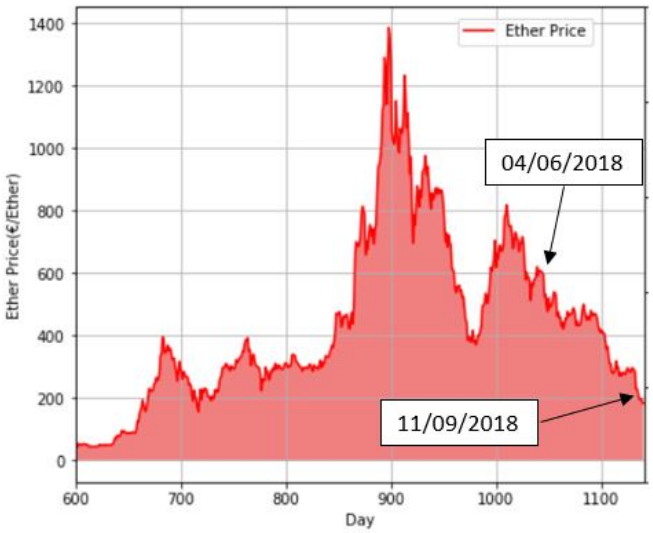


Figura 22: Evolución de la cotización del Ether

En segundo lugar, el consumo energético del computador tiene una gran influencia en el *Payback* de la inversión. Así, el objetivo para un minero es ser capaz de crear un centro de minado, ya sea industrial o a nivel usuario, con el menor consumo energético por computador posible.

7

CONCLUSIONES

Blockchain es una tecnología que ofrece la descentralización datos en un registro inmutable, pero con una dificultad conceptual muy elevada. El proceso, desde que se realiza una transacción hasta que se une el bloque a la cadena, está creado sobre una serie de algoritmos complejos que permite que la red sea de confianza. Este proceso es el minado de bloques, que tiene asociada una recompensa por cada bloque que se mina (3 Ether).

Existen varios dispositivos con los que se puede minar *Blockchain*: CPUs, GPUs, FPGAs y ASICs. Cada uno de ellos tiene unas características de operación determinadas que influyen directamente sobre el beneficio obtenido en el minado de bloques. Las dos principales son: HashRate (número de *hash* que realiza por segundo) y consumo energético.

Se ha comprobado tanto en la CPU, como en la GPU, que existen grandes diferencias entre el consumo eléctrico nominal, dado por el fabricante del dispositivo, y el que realmente se consume durante el minado. El consumo de la CPU en el minado representa el 39 % de la energía total consumida por el computador (64 W frente a los 164 W totales). En cambio, la GPU consume el 62.7 % de la energía total consumida por el computador durante el minado (172 W frente a los 274 W totales).

La diferencia que existe entre el consumo del dispositivo y el total del computador se debe a que existen otros muchos componentes en un computador que consumen energía para minar como: memorias, discos duros, ventiladores, placas madre, transformadores. Además, se podría realizar una labor de optimización del *software* para utilizar el máximo de las capacidades de la CPU y GPU.

A la vista de los resultados obtenidos sobre los consumos energéticos y velocidades de cálculo de los dispositivos, se puede concluir que la GPU es 26 veces más eficiente que la CPU. La GPU realiza 204651 *hash* por cada Julio consumido, frente a los 3906 *hash* por Julio de la CPU. En cuanto a velocidad de cálculo, la GPU realiza un 7100 % más de operaciones por segundo que la CPU.

Desde el *Boom* de las criptomonedas, entre marzo y abril del 2017, ha aumentado de forma lineal el número de usuarios que quieren participar en el proceso de minado de bloques debido a la recompensa económica que lleva asociada. Debido a la alta competitividad que se ha creado, conseguir minar un bloque es cada vez más complicado, consumiendo así más energía por cada bloque minado.

La cotización del Ether es, actualmente, la barrera para la rentabilidad en el proceso de minado. De acuerdo a la situación actual (09/11/2018), no es rentable minar con ninguno de los dispositivos de cómputo estudiados, si se considera la inversión inicial en *hardware*. Incluso si se minara con el Antminer E3, se tardarían unos 8 años en recuperar la inversión, suponiendo que no cambiaran ni la cotización del Ether, ni la potencia computacional de la red. Pero esta situación va a peor ya que la tendencia del precio desde mayo del 2018 es totalmente decreciente. La cotización mínima del Ether para que el proceso de minado sea rentable son 10295 €, 384 € y 160 €, para la CPU, GPU y Antminer E3 respectivamente. Actualmente, el precio se sitúa en 170 €.

Los cálculos realizados tanto del gasto energético, como del beneficio por día y del periodo de recuperación de la inversión, se aproximan en gran medida a los mostrados en los foros especializados. Además, estas calculadoras *online* no tienen en cuenta el consumo real del computador, sino que sólo tienen en cuenta la potencia nominal del dispositivo. Esto ofrece una visión muy optimista del *Payback* que muestran.

BIBLIOGRAFÍA

[1] Heraldo de Aragón. *La DGA impulsará un proyecto de contratación pública utilizando 'blockchain'*. https://www.heraldo.es/noticias/aragon/2018/03/07/la-dga-impulsara-proyecto-contratacion-publica-utilizando-blockchain-1228833-300.html. [Online; 07/03/2018].

[2] BarbaraN. *Bitcoin no fue la primera, descubre las 7 Criptomonedas anteriores*. https://bitcoin.es/noticias/bitcoin-no-fue-la-primera-descubre-las-7-criptomonedas-anteriores/. [Online; 18/12/2017].

[3] IBM Blockchain. *IBM Blockchain*. https://www.ibm.com/blockchain. [Online; 25/02/2018].

[4] Bloomberg. *Google Is Working on Its Own Blockchain-Related Technology*. https://www.bloomberg.com/news/articles/2018-03-21/google-is-said-to-work-on-its-own-blockchain-related-technology. [Online; 21/03/2018].

[5] Buriedone. *GPU Mining Hashrates*. https://www.buriedone.com/hashrates.html. [Online; 2018].

[6] CNBC. *Why Mark Zuckerberg just put some of his best execs on blockchain*. https://www.cnbc.com/2018/05/09/zuckerberg-invests-in-blockchain-to-keep-facebook-relevant.html. [Online; 09/05/2018].

[7] CoinMarketCap. *CoinMarketCap*. https://coinmarketcap.com/all/views/all/. [Online; 2018].

[8] Power Compare. *Bitcoin Mining Electricity Consumption Vs Countries*. https://powercompare.co.uk/bitcoin/. [Online; 2017].

[9] CryptoCompare. *Antminer E3*. https://www.cryptocompare.com/mining/bitmain/antminer-e3/.

[10] CryptoCompare. *Antminer E3*. https://www.cryptocompare.com/mining/bitmain/antminer-e3/.

[11] Micah Dameron. *Beigepaper: An Ethereum Technical Specification*. Version 0.7.3. Github, 11/05/2018.

[12] El Economista. *La banca se suma al "blockchain* .http://www.eleconomista.es/empresas-finanzas/noticias/8962817/02/18/La-banca-se-suma-al-blockchain.html. [Online; 25/02/2018].

[13] Ethereum. *A Next-Generation Smart Contract and Decentralized Application Platform*. Github, 2014.

[14] Etherscan. *Ether Mining Calculator*. https://etherscan.io/ether-mining-calculator.

[15] ExtremeTech. *NVDIA launches Maxwell*. https://www.extremetech.com/computing/190417-nvidia-launches-maxwell-a-next-gen-gpu-that-will-make-everyone-an-nvidia-fanboy. [Online; 28/09/2014].

[16] ALL ABOUT FPGA. *FPGA Architecture*. https://allaboutfpga.com/fpga-architecture/. [Online; 16/04/2014].

[17] Github. *Ethash*. https://github.com/ethereum/wiki/wiki/Ethash.

[18] Github. *go ethereum*. https://github.com/ethereum/go-ethereum/wiki.

[19] Peter Harrington. *Machine Learning in Action*. Version 1. MANNING, 19 de abril de 2012.

[20] Jason Hoelscher. *Diffused Art and Diffracted Objecthood: Painting in the Distributed Field*. https://www.researchgate.net/publication/260480880_Diffused_Art_and_Diffracted_Objecthood_Painting_in_the_Distributed_Field?_sg=l5hCc63M4BKlglS4e9Ao_xqAb7-wt4uNIQTIn1r_6dPYXj0P7xePG8QtGIrq1VhBY8JOdszGyg. [Online; 01/02/2014].

[21] IBM. *IBM*. https://www.ibm.com/blockchain/industries. [Online; 2018].

[22] IBM. *Top five blockchain benefits transforming your industry*. https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/. [Online; 22/02/2018].

[23] Joo. *Fuente alimentación Antmier*. https://www.joom.com/es/products/1502353374278125507-151-1-709-2366532663.

[24] Microsoft. *Under the sea, Microsoft tests a datacenter that's quick to deploy, could provide internet connectivity for years*. https://news.microsoft.com/features/under-the-sea-microsoft-tests-a-datacenter-thats-quick-to-deploy-could-provide-internet-connectivity-for-years/. [Online; 05/06/2018].

[25] Andrew Ng. *CS229 Lecture notes*. http://cs229.stanford.edu/notes/cs229-notes1.pdf. [Online; 2012].

[26] Afri Schoedon y Vitalik Buterin. *EIP-649: Metropolis difficulty bomb delay and block reward reduction*. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-649.md. [Online; June 2017].

[27] National Institute of Standards y Technology. *Secure Hash Standard (SHS)*. Gaithersburg, MD 20899-8900: U.S. Department of Commerce, 2015.

[28] Techradar.pro. *Best mining CPU 2018*. https://www.techradar.com/news/best-mining-cpu. [Online; 2018].

[29] Shekhar Tripathi. *Ethereum mining is profitable, but not for long*. https://www.techinasia.com/talk/ethereum-mining-profitability. [Online; 28/8/2017].

[30] THE VERGE. *Mark Zuckerberg shares pictures from Facebook's cold, cold data center*. https://www.theverge.com/2016/9/29/13103982/facebook-arctic-data-center-sweden-photos. [Online; 29/09/2016].

[31] Computer Science Wiki. *Central processing unit*. https://computersciencewiki.org/index.php/Architecture_of_the_central_processing_unit_(CPU). [Online; 25/02/2018].

[32] Dr. Gavin Wood. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BYZANTIUM*. Creative Commons Attribution Share-Alike (CC-BY-SA) version 4.0, 6/05/2018.

[33] steemit. *Who controls crypto currencies?* https://steemit.com/crypto/@jfgrissom/who-controls-crypto-currencies.

LISTADO DE FIGURAS

LISTADO DE CUADROS

A

FUNCIÓN HASHIMOTO

En este Apéndice, se muestra el código correspondiente a la función *Hashimoto* [17]. Se trata de la función que se ejecuta masivamente en la red Ethereum durante el proceso de minado de bloques y que supone un elevado consumo energético debido a su complejidad. .

```
1  def hashimoto(header, nonce, full_size, dataset_lookup):
2      n = full_size / HASH_BYTES
3      w = MIX_BYTES // WORD_BYTES
4      mixhashes = MIX_BYTES / HASH_BYTES
5
6      s = sha3_512(header + nonce[::-1])
7
8      mix = []
9      for _ in range(MIX_BYTES / HASH_BYTES):
10         mix.extend(s)
11
12     for i in range(ACCESSES):
13         p = fnv(i ^ s[0], mix[i \% w]) \% (n // mixhashes) *
               mixhashes
14         newdata = []
15         for j in range(MIX_BYTES / HASH_BYTES):
16             newdata.extend(dataset_lookup(p + j))
17         mix = map(fnv, mix, newdata)
18
19     cmix = []
20     for i in range(0, len(mix), 4):
21         cmix.append(fnv(fnv(fnv(mix[i], mix[i+1]), mix[i+2]), mix
               [i+3]))
22     return {
23         "mix digest": serialize_hash(cmix),
24         "result": serialize_hash(sha3_256(s+cmix))
25     }
```

Listing 4: Función Hashimoto

B

ALGORITMO DE REGRESIÓN LINEAL MULTIVARIABLE

Aprendizaje Automático es una rama de la Inteligencia Artificial, que crea sistemas que aprenden automáticamente. Concretamente, trata de identificar patrones o tendencias en un conjunto de datos muy grande. En este proyecto se ha usado para realizar el análisis de los datos computacionales de la red Ethereum y su posterior estimación de costes.

El Aprendizaje Automático engloba una serie de técnicas y algoritmos, cada uno con un propósito distinto. En este proyecto se ha utilizado la ecuación normal de la regresión lineal multivariable, que permite obtener la función matemática que mejor se aproxima a unos datos dados. Los parámetros de la función se obtienen automáticamente gracias a este algoritmo. La ventaja de la ecuación normal frente a la técnica del descenso del gradiente es que no hace falta iterar para obtener los parámetros de la recta que mejor se adapta a los datos.

La ecuación matricial Ecuación 2 permite obtener los parámetros de la recta que mejor se adapta a los datos [25].

$$\Theta = (X^T X)^{-1} X^T y \tag{2}$$

donde y es un vector que recoge las medidas de la variable dependiente, y X representa una matriz de los valores de las variables independientes.

A continuación se muestra la implementación del algoritmo de la ecuación normal, implementada en Python.

```
1 #Funcion del Coste dado X, Y y theta
2
3 def computeCost(X_i, y_i, theta_i):
4     m_i = len(y_i);
5     J_i = 0;
6     H_i= np.matmul(X_i,theta_i);
7     A_i = (H_i - y_i)
```

```
8     J_i = (sum(A_i*A_i))/(2*m);
9     return (J_i);
10
11 #Funcion Gradient descent (Normal Equation)
12
13 def gradientDescent(X_a, y_a, theta_a):
14     theta = inv(np.matmul(np.transpose(X_a),X_a));
15     theta_intermedio = np.matmul(theta,np.transpose(X_a));
16     theta_final = np.matmul(theta_intermedio,y_a)
17     return (theta_final);
18
19 #Funcion que minimiza el Coste y devuelve los parametros de la
       recta
20
21 def gradientReg(X_o, y_o):
22     f = np.size(X_o,1);
23     initial_theta = np.zeros(f);
24     coste = computeCost(X_o, y_o, initial_theta);
25     theta_o = gradientDescent(X_o,y_o, initial_theta);
26     return (theta_o);
27
28 #Vector que contiene los parametros X e Y de la recta que mejor
       se ajusta a los datos
29
30 theta_optimo = gradientReg(X1,y1)
```

Listing 5: Algoritmo de Regresión lineal multivariable en forma de ecuación normal

C

COMPARATIVA CALCULADORAS ONLINE

En este Anexo, se hace un estudio más detallado de la comparativa entre los datos (beneficio y gasto diario) que proporcionan los fabricantes y los que realmente se obtienen, tras considerar el consumo real del computador.

En la siguiente tabla se muestran los datos proporcionados por los fabricantes con las características de 11/09/2018.

Cuadro 15: Características nominales de los dispositivos

Dispositivo	Modelo	HashRate [H/s]	Consumo [W]
CPU	Skykake 6700k [28]	0.5	91
GPU	NVIDIA GTX TITAN X [5]	35	250
ASIC	Antminer E3 [9]	190	760

Introduciendo estos datos en la calculadora, se obtienen los consumos y beneficios que teóricamente se obtendrían durante la actividad de minado con cada uno de los dispositivos.

Cuadro 16: Resultados de la calculadora del proyecto con los datos nominales

Dispositivo	Tiempo minado [días]	Consumo [€/día]	Beneficio [€/día]
CPU	87453	0.225	-0.20
GPU	1249	0.619	-0.22
ASIC	230,13	1.88	0.28

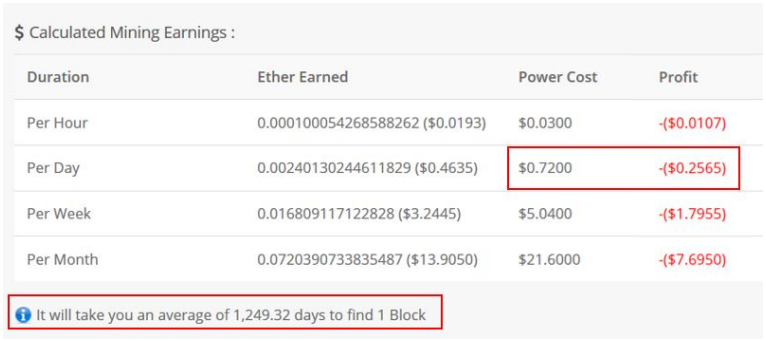
Las tres siguientes imágenes, representan los datos obtenidos con una calculadora *online* con los datos nominales de la CPU, GPU y Antminer E3, respectivamente.

$ Calculated Mining Earnings :

Duration	Ether Earned	Power Cost	Profit
Per Hour	1.42934669411803E-06 ($0.0003)	$0.0109	-($0.0106)
Per Day	3.43043206588327E-05 ($0.0066)	$0.2621	-($0.2555)
Per Week	0.000240130244611829 ($0.0463)	$1.8346	-($1.7882)
Per Month	0.00102912961976498 ($0.1986)	$7.8624	-($7.6638)

It will take you an average of 87,452.54 days to find 1 Block

Figura 23: Resultados de una calculadora *online* con datos nominales de la CPU



$ Calculated Mining Earnings :

Duration	Ether Earned	Power Cost	Profit
Per Hour	0.000100054268588262 ($0.0193)	$0.0300	-($0.0107)
Per Day	0.00240130244611829 ($0.4635)	$0.7200	-($0.2565)
Per Week	0.016809117122828 ($3.2445)	$5.0400	-($1.7955)
Per Month	0.0720390733835487 ($13.9050)	$21.6000	-($7.6950)

It will take you an average of 1,249.32 days to find 1 Block

Figura 24: Resultados de una calculadora *online* con datos nominales de la GPU

$ Calculated Mining Earnings :

Duration	Ether Earned	Power Cost	Profit
Per Hour	0.000543151743764851 ($0.1048)	$0.0912	$0.0136
Per Day	0.0130356418503564 ($2.5161)	$2.1888	$0.3273
Per Week	0.091249492952495 ($17.6130)	$15.3216	$2.2914
Per Month	0.391069255510693 ($75.4842)	$65.6640	$9.8202

It will take you an average of 230.14 days to find 1 Block

Figura 25: Resultados de una calculadora *online* con datos nominales del Antminer E3

Se puede observar que tanto los tiempos hasta que se consigue minar un bloque, como los valores de coste y beneficio diarios son muy parecidos en los tres dispositivos.

Pero en la realidad, no sólo el dispositivo consume energía, sino que hay otros, como se ha visto en el Capítulo 5.

La siguiente tabla recoge los datos de consumo y HashRate obtenidos experimentalmente.

Cuadro 17: Características medidas experimentalmente de los dispositivos

Dispositivo	Modelo	HashRate [H/s]	Consumo [W]
CPU	Skykake 6700k	0.25	164
GPU	NVIDIA GTX TITAN X	18	274
ASIC	Antminer E3	190	2360

Como se puede observar, el consumo total durante el minado es mucho mayor que el nominal especificado por los fabricantes. Entonces, ¿qué ocurre si en vez de considerar el consumo nominal se utilizan los datos reales de consumo y HashRate? En la siguiente tabla se recogen los datos de tiempo hasta minar un bloque, consumo y beneficio diarios, de cada los tres dispositivos.

Cuadro 18: Resultados de la calculadora del proyecto con los datos reales

Dispositivo	Tiempo minado [días]	Consumo [€/día]	Beneficio [€/día]
CPU	173673	0.409	-0.403
GPU	2412	0.679	-0.472
ASIC	228	5.85	-3.67

Como se puede observar en la tabla anterior, actualmente no es rentable minar con ninguno de los dispositivos. Tanto el consumo como el beficio por día, son mucho más desfavorables que en la comparativa anterior.

D

DIAGRAMA DE GANTT

La ejecución del proyecto se divide en siete etapas: recopilación de información, medición del consumo energético de los dispositivos con los contadores *hardware*, desarrollo del código de análisis de datos en Python, medición del consumo energético de los dispositivos y computador con el vatímetro, realización del curso *online* de Machine Learning de Coursera y, finalmente, el desarrollo del estudio económico y redacción de la memoria.

Algunas de ellas, como la realización del cuso *online* y la medición de consumo energético con contadores *hardware* se han podido realizar en paralelo, ya que se disponía de tiempo libre entre ensayos.

Los *scripts* de Python se crearon una vez se terminó el curso *online* y se disponía de datos de consumo energético de alguno de los dispositivos.

Se tuvo que esperar hasta después de verano para poder realizar las medidas de consumo energético con el vatímetro, porque estaba ocupado por otro estudiante.

En la siguiente tabla, se recoge la estimación del número de horas totales invertidas en este proyecto.

Cuadro 19: Estimación de horas invertidas en el proyecto

Días del proyecto	Horas diarias	Horas totales
122	6-7	793

La siguiente figura representa el diagrama de Gantt del proyecto, especificando las distintas subtareas y la duración estimada de las mismas.

PROYECTO BLOCKCHAIN	**122 días**	**lun 02/04/18**	**mar 18/09/18**
Recopilación Información	**54 días**	**lun 02/04/18**	**jue 14/06/18**
Confirmación del proyecto	0 días	lun 02/04/18	lun 02/04/18
Lectura Blockchain	19 días	mar 03/04/18	vie 27/04/18
Lectura Código	22 días	mié 02/05/18	jue 31/05/18
Ensayos Dispositivos	**65 días**	**mié 16/05/18**	**mar 14/08/18**
Ensayos GPU	19 días	mié 16/05/18	lun 11/06/18
Ensayos CPU	17 días	lun 23/07/18	mar 14/08/18
Scripts Python	**64 días**	**mar 12/06/18**	**vie 07/09/18**
Datos GPU	10 días	mar 12/06/18	lun 25/06/18
Datos CPU	5 días	lun 20/08/18	vie 24/08/18
Datos GPU Vatímetro	4 días	jue 30/08/18	mar 04/09/18
Datos CPU Vatímetro	3 días	mié 05/09/18	vie 07/09/18
Precio y potencia Ethereum	12 días	mar 07/08/18	mié 22/08/18
Ensayos Vatímetro	**9 días**	**vie 24/08/18**	**mié 05/09/18**
Ensayos GPU	2 días	vie 24/08/18	lun 27/08/18
Ensayos CPU	2 días	lun 03/09/18	mar 04/09/18
Curso Machine Learning	**59 días**	**mié 16/05/18**	**lun 06/08/18**
Curso Machine Learning	59 días	mié 16/05/18	lun 06/08/18
Estudio económico	**7 días**	**vie 07/09/18**	**lun 17/09/18**
Estudio económico	7 días	vie 07/09/18	lun 17/09/18
Redacción de memoria	**49 días**	**mié 11/07/18**	**lun 17/09/18**
Memoria	49 días	mié 11/07/18	lun 17/09/18
Entrega final	**1 día**	**mar 18/09/18**	**mar 18/09/18**
Entrega de la memoria	0 días	mar 18/09/18	mar 18/09/18