
UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques i Informàtica

**GRADO DE MATEMÁTICAS**

**Trabajo de fin de grado**

# La teoría de juegos aplicada a la minería de criptomonedas

**Autor: Óscar Pulido Castillo**

**Facultat de matemàticas i informàtica**
**Barcelona, 12 de junio de 2023**

# Índice general

## Abstract

In this final degree project, we aim to explain cryptocurrency mining from the perspective of game theory. First, we will understand what cryptocurrencies are and how they came into existence. We will also explain how they operate, with a particular emphasis on the aspect of security.

Next, on a theoretical level, we will attempt to establish a direct relationship between congestion games and the competition among miners that arises from cryptocurrency mining, such as Bitcoin.

Finally, on a more practical level, we will try to determine the behavior that miners may exhibit over time. We will present strategies to maximize rewards. We will also see that adopting these strategies can pose a problem for the security of the blockchain.

## Resumen

En este trabajo de final de grado, pretendemos explicar la minería de criptomonedas desde el enfoque de la teoría de juegos. En primer lugar, entenderemos qué son las criptomonedas y cuál es su origen. También explicaremos cuál es su manera de funcionar, poniendo énfasis en el aspecto de la seguridad.

Posteriormente, a nivel teórico, trataremos de establecer una relación directa entre los juegos de congestión y la competición entre mineros que surge de la minería de criptomonedas, como el Bitcoin.

Finalmente, a nivel más práctico, trataremos de averiguar qué comportamiento podrían tener los mineros a lo largo del tiempo. Presentaremos estrategias con las que maximizar recompensas. También veremos que adoptar estas estrategias puede significar un problema para la seguridad de la *blockchain*.

# Capítulo 1

# Introducción

Las criptomonedas aparecen constantemente en todos los medios de comunicación, y no es para menos. Millones de individuos de todo el mundo están invirtiendo en ellas. Cada segundo, una cantidad inimaginable de dólares se transforma en criptodivisas. Cada año, nuevos nombres salen al mercado y se añaden a los ya inconfundibles: Bitcoin, Ethereum, Cardano... [3]

En las siguientes páginas de este documento pretendemos dar respuesta a las siguientes preguntas. ¿Qué puede explicarnos la Teoría de Juegos sobre el funcionamiento del mercado de criptomonedas? ¿Qué modelos matemáticos pueden usarse para definir los patrones de comportamiento de los individuos que participan en ese mercado? ¿Cómo afectan las decisiones individuales, aparentemente racionales, al conjunto de un sistema descentralizado que supuestamente "nadie controla"?

Para intentar resolver esas cuestiones, estudiaremos las decisiones de los mineros de criptomonedas desde dos perspectivas distintas. Ambas pretenden dar respuesta a una pregunta global:

**¿Qué puede hacer un minero para maximizar su rentabilidad?**

En primer lugar, modelizaremos una competición no cooperativa entre mineros. En esta competición, los mineros deben decidir qué servicio en la nube contratar para minar qué criptomoneda. Definiremos cuál es la probabilidad de que un minero sea el primero en resolver el puzle de la criptomoneda minada. En este primer escenario nos centraremos en la utilidad que puede tener el minero entre puzles dentro de una época. Para ello plantearemos tres juegos diferentes. En el primero, habrá una única criptomoneda $k$ y $S$ servicios en la nube que los

mineros podrán contratar para minarla. En el segundo plantearemos el juego inverso, múltiples criptomonedas $K$ y un único SN $s$. Finalmente, estudiaremos un juego no atómico con múltiples criptomonedas y SNs. Para cada uno de los juegos daremos las condiciones necesarias para la existencia de un equilibrio (y unicidad en algunos casos) puro de Nash.

En segundo lugar, trataremos un contexto más determinista. En este, hay una única criptomoneda que minar y cada minero dispondrá de un poder de minado máximo. En este contexto, propondremos estrategias para maximizar la rentabilidad del usuario a lo largo de varias épocas. Veremos que lo que intuitivamente podría parecer un equilibrio, donde los mineros minan con el poder total, no es realmente un equilibrio. Demostraremos que a veces dejar de minar entre épocas es una estrategia mejor que minar en cada una de ellas. La idea básica tras esta lógica aparentemente contraintuitiva es que el poder total de minado determina la dificultad del los puzles y, en consecuencia, determina también la recompensa obtenida. Este hecho genera situaciones en las que la mejor opción es dejar de minar. Mostraremos una estrategia en la que minar en épocas alternas da mejores recompensas (es decir: minar una época sí, una época no). En secciones posteriores, trataremos de optimizar esta estrategia de minar en épocas alternas. Veremos también que seguir este tipo de estrategias puede comprometer la seguridad de la blockchain, principalmente en las épocas en las que se deja de minar. Daremos resultados que nos permitirán ver cuando es rentable optar por estas estrategias.

Finalmente, tras analizar ambas perspectivas, plantearemos posibles líneas de investigación para el futuro y expondremos brevemente las tendencias hacia las que se mueve el mercado de las criptomonedas.

# Capítulo 2

# Contexto histórico y relevancia de las criptomonedas

Si existe un elemento que es el denominador común de todas las civilizaciones y que ha determinado el rumbo de lo que hoy en día se conoce como sociedad, ese elemento es el dinero. Hace 5000 años, en Mesopotamia, las dificultades para realizar trueques obligaron a los sumerios a idear una nueva manera de intercambiar materiales. Según los historiadores, en ese momento surgió la idea del dinero, cuya definición primigenia era "algo material que permite cuantificar el valor de los productos y hacer transacciones". Desde entonces, el ser humano no ha dejado de buscar maneras más eficaces de comerciar y, en esa búsqueda, la complejidad de las definiciones del dinero no ha dejado de aumentar. Hoy en día, incluso se plantea el fin del dinero en efectivo como algo no solo posible, sino inevitable.

En 2007-2008 (con el estallido de la burbuja inmobiliaria), una persona o un grupo de personas aún desconocidas bajo el seudónimo de Satoshi Nakamoto, encontraron otra manera posible de realizar intercambios. Esa nueva manera se publicó online en forma de artículo, bajo el título "Bitcoin: A Peer-to-Peer Electronic Cash System"[8] . Igual que los sumerios hace miles de años, Nakamoto descubrió que el sistema monetario actual conlleva algunas dificultades que podrían resolverse con un cambio de paradigma. ¿Y si no fuera necesario confiar en los bancos para mantener el valor del dinero? ¿Y si hubiera una versión totalmente electrónica del dinero que permitiese intercambios directos entre dos partes sin tener que atravesar una institución financiera? ¿Y si hubiera un nuevo tipo de moneda que cualquiera puede controlar, y que, por tanto, nadie controla realmente? [12]

En enero de 2009 se realizó la primera transacción de Bitcoin. Hoy, 14 años

después, el número total de transacciones alcanza los 800 millones. Este incremento exorbitante demuestra que la confianza de la sociedad en las instituciones financieras ha ido decreciendo tras cada crisis. En consecuencia, cada día más personas (tanto físicas como jurídicas) apuestan por otras alternativas de gestionar su capital. Esas otras alternativas, entre las cuales se incluye el Bitcoin (que fue la primera), reciben el nombre de criptomonedas. Este nombre tiene su raíz en la voz griega *kryptos* que significa "escondido, protegido". Las criptomonedas utilizan sistemas encriptación para asegurar las transacciones entre usuarios, a diferencia del dinero tradicional, cuya confianza se deposita en las instituciones financieras [1].

En el momento en el que se escriben estas líneas (abril de 2023) las criptomonedas tienen una capitalización total de mercado de 1,2 trillones de dólares, siendo Bitcoin [8] y Ethereum [1] las monedas más dominantes, con un 45 % y un 18 % de cuota de mercado respectivamente. Por si fuera poco, nuevas monedas se unen al mercado digital diariamente, lo que se traduce en un crecimiento constante del mercado de la minería.

En definitiva, sea el lector detractor o partidario de las criptomonedas y de sus posibilidades en el futuro, es innegable que hoy en día son una realidad.

[1] A lo largo de este documento, se utilizará la expresión "dinero tradicional" para referirse al dinero utilizado mayoritariamente a día de hoy en el mundo, tanto el físico como el digital (datos almacenados en los servidores de las entidades bancarias).

# Capítulo 3

# Conceptos Previos

En este apartado responderemos a algunas preguntas sobre conceptos que se utilizarán a lo largo del documento. De esta manera, facilitaremos la comprensión de los capítulos posteriores.

## 3.1. Preguntas clave

### 3.1.1. ¿Qué es la *blockchain*?

La *blockchain* es una tecnología basada en una cadena de bloques de operaciones descentralizadas y pública. Es una gran base de datos compartida a la que cualquier persona tiene acceso. Todas y cada una de las transacciones registradas en la *blockchain* pueden ser rastreadas. Podríamos decir que es como un gran libro de contabilidad inmutable modificado por muchos ordenadores (nodos, mineros) simultáneamente. Cuando un usuario realiza una transacción en la *blockchain*, esta es validada por los mineros. A continuación, se añaden los datos (quién, qué, cuándo, dónde, cuánto, etc.) a un bloque de datos que los almacena. Posteriormente, este se añade a la cadena de bloques. El contenido de las transacciones es muy variado y depende de la *blockchain* en la que se opera. Los casos más comunes son el intercambio de monedas digitales o la compra-venta de activos digitales.

### 3.1.2. ¿Cómo se mantiene la seguridad de las criptomonedas?

Volviendo a la comparativa entre el dinero tradicional y las criptomonedas, surge una pregunta obvia. ¿Cómo se mantiene la seguridad del sistema de intercambios de criptomonedas? O, dicho de otra manera, si la humanidad actualmente confía en los bancos para almacenar y mover su dinero, ¿en qué confían realmente las personas que afirman confiar en la *blockchain*?

Para mantener la seguridad de la criptomonedas existen los llamados **protocolos de consenso**. Un protocolo de consenso es cualquier método utilizado para conseguir confianza (o "acuerdo") a través de una red informática descentralizada. Existen múltiples protocolos de consenso para regular y validar los bloques que se añaden a la *blockchain*. Los más usados son el protocolo Prueba de Trabajo (PoW, por sus siglas en inglés *'Proof of Work'*) y el protocolo Prueba de Participación (PoS, por sus siglas en inglés *'Proof of Stake'*). El lector que desee conocer de una manera más amplia los protocolos de consenso puede consultar [6].

Según [3], la mayoría de las criptomonedas están basadas en el protocolo PoW, entre ellas Bitcoin. Por este motivo, a lo largo de este documento se tratará únicamente el PoW. La idea principal del este protocolo es que una gran cantidad de energía debe ser usada para alterar la cadena de bloques y funciona bajo el concepto de requerir un trabajo (*work*) al usuario, que posteriormente es verificado por la red. Esta característica es fundamental para mantener la seguridad, imposibilitando que un mismo dispositivo controle varias identidades y corrompa así el sistema. Los ataques informáticos de este tipo reciben el nombre de ataques Sybil. Esta característica previene también los ataques del 50 %. Este último ataque se puede dar cuando un usuario posee más del 50 % del poder de minado de una *blockchain*. Al poseer la mayoría del poder de minado podría manipular las transacciones a su favor invalidando las validaciones del resto de mineros.

¿Pero qué significa realmente, en datos empíricos, esta "gran cantidad"de energía que requiere el PoW? Según [2], la energía consumida por Bitcoin está cerca del 0,5 % de la energía consumida en todo el mundo. Este porcentaje es mayor al consumo de electricidad anual de países como Finlandia, que tiene 5,5 millones de habitantes; y es una cantidad total de energía 7 veces mayor a la consumida por las operaciones globales de Google [5].

Toda esa energía se consume en las operaciones de minería, llevadas a cabo por mineros. Los mineros son los usuarios que, mediante el poder de computación de sus ordenadores, contribuyen a la validación de bloques en la *blockchain*. Debido al elevado consumo de energía requerido, los mineros pueden contratar **servicios en la nube con hardware especializado** (en adelante, SN) en vez de utilizar una infraestructura propia.

Con el objetivo de añadir estos bloques, los mineros compiten por ser los primeros en resolver un puzle de gran complejidad. El incentivo por el cual los mineros compiten es la obtención de nuevas unidades de la criptomoneda minada. La

recompensa es proporcional a la cantidad de energía invertida entre el total de los mineros. Esta recompensa es fija y puede depender de la comisión de transacción o bien de su valor de cambio a monedas tradicionales.

### 3.1.3. ¿Cómo se determina la dificultad de un puzle?

La *blockchain* se encarga de predecir cuanto poder de minado va a haber en un momento dado basándose en datos anteriores. Esto se hace mediante la división de los ajustes anteriores entre las épocas. Cada época consiste en un número fijo tanto de bloques minados como de recompensas, y en cada época se mina un número fijo de criptomonedas.

La **dificultad** se calcula en función de la predicción del **poder de minado** (también llamado poder de hash) total de la época anterior. Como los mineros son libres, pueden decidir unirse o dejar de minar una criptomoneda en cualquier momento. Estas decisiones individuales (entrar y salir de la red de minado) afectan a todo el resto de mineros que participan en el juego.

Idealmente, si ese poder de minado fuese conocido, la dificultad se ajustaría a la vez que la situación va cambiando (es decir, cada vez que entrase o saliese un minero). Lo que sucede en realidad es que el ajuste no se realiza de manera simultánea. Es decir, los cambios durante la época no se tienen en consideración, lo que puede provocar el fenómeno conocido como "la espiral de la muerte"[11]. Una espiral de la muerte se produce cuando un número elevado de mineros deciden dejar de minar una criptomoneda en una misma época. Como el poder de hash total decrece (ya que hay menos mineros) y la dificultad se mantiene igual, finalizar la época se convierte en una tarea prácticamente interminable. Como el ajuste de dificultad no sucede, el resto de mineros decidirá dejar de minar y eventualmente la *blockchain* quedará inactiva.

Por ejemplo, en Bitcoin, cada 2016 bloques minados se recalcula la dificultad y empieza una nueva época. Actualmente, se minan 6,25 bitcoins por época. Además, cada 210000 bloques minados, la recompensa se reduce a la mitad (concepto conocido como *halving*).

## 3.2. Tipos de juegos analizados

### 3.2.1. ¿Qué son los juegos de congestión?

En esta sección definiremos los juegos de congestión (*congestion games*) y las funciones potenciales. Con estas definiciones seremos capaces de analizar los juegos que hemos presentado en la introducción.

Empecemos con los **juegos de congestión**. En este tipo de juegos hay una colección de jugadores $\mathcal{N}$ y una colección de recursos $\mathcal{R}$. Concretamente, en los juegos estudiados a continuación, los jugadores serán los mineros y los recursos serán los servicios en la nube (en adelante, SNs).

Cada jugador tendrá una colección de **estrategias** $A_i$ y escogerá una de estas $a_i \in A_i$. En nuestro caso, consideraremos los juegos en los que $A_i = A_j$ para todo $i$, $j$. Denotaremos como $a = (a_i)_{i \in \mathcal{N}}$ el perfil de estrategias (también llamado configuración) de los jugadores. El coste por usar el recurso $r \in R$ dependerá del número de jugadores que lo usen, denotado por $x_r$. Por lo tanto, tendremos que la función de coste para el recurso $r$ será $c_r(x_r)$, donde $c_r(x_r)$ es una función no negativa, creciente y continua.

Por lo tanto, el coste del jugador $i$, $c_i(a_i, a_{-i})$, será la suma de los costes de los recursos que haya utilizado. Podemos escribirlo como:

$$c_i(a_i, a_{-i}) = \sum_{r \in a_i} c_r(x_r) \tag{3.1}$$

El objetivo de cada jugador, como en cualquier juego, es minimizar el coste total. En este tipo de juego, las estrategias se escogen de manera independiente y simultánea. Esto puede resultar en una congestión y, por lo tanto, en costes más elevados.

A continuación introduciremos las **funciones potenciales.** Definimos la función potencial de un juego de congestión como la función $P(a)$ que asigna un valor para cada perfil de estrategias. Podemos escribirla como:

$$P(a) = \sum_{i \in \mathcal{N}} P_i(a_i, a_{-i}) \tag{3.2}$$

donde $P_i(a_i, a_{-i})$ es la función potencial del jugador $i$ cuando escoge la estrategia $a_i$ y el resto de jugadores están en la configuración $a$.

Las funciones potenciales tienen dos propiedades:

i. No negatividad: $P(a) \geq 0$ para toda configuración $a$

ii. Diferencia potencial: para todo $i, j \in \mathcal{N}$ y para todo $a_i, a_j \in A_i, A_j$:

$$P(a_i, a_{-i}) - P(a_j, a_{-j}) = c_i(a_i, a_{-i}) - c_j(a_j, a_{-j}) \tag{3.3}$$

Cualquier cambio de estrategia de un jugador en un juego potencial puede estar asociado con un cambio en la función potencial. La función potencial es una función real sobre el conjunto de estrategias. Además, sabemos que cualquier función continua sobre un conjunto compacto (como el conjunto de estrategias en un juego finito) tiene al menos un mínimo y este mínimo se corresponde al equilibrio de Nash. Por lo tanto, los juegos que admiten funciones potenciales (llamados juegos potenciales) tienen al menos un equilibrio de Nash.

Según [7] todo juego de congestión admite una función potencial, que se define bajo estas líneas. Para ello definimos primero $x_r$ en función de la configuración. Sea $A = \times_{i \in \mathcal{N}} A_i$. Para todo $a \in A$ y para todo $r \in \mathcal{R}$:

$$x_r(a) = \#\{i \in \mathcal{N} : r \in a_i\} \tag{3.4}$$

Ahora, para cada $a \in A$ definimos la función potencial de un juego de congestión como:

$$P(a) = \sum_{j \in \bigcup\limits_{i \in \mathcal{N}} a_i} \left( \sum_{k=1}^{x_j(a)} c_r(k) \right) \tag{3.5}$$

La prueba de que $P$ es la función potencial del juego se puede deducir de [10]. También se puede deducir usando el Corolario 2.9 de [7]. Finalmente, usando la función potencial, podemos encontrar el **equilibrio de Wardrop.** El equilibrio de Wardrop es un estado en el cual ningún jugador puede reducir su coste cambiando a una estrategia diferente.

Una configuración $a \in A$ es un equilibrio de Wardrop si y solo si:

$$P_i(a_i, a_{-i}) \leq P_i(a_i', a_{-i}), \forall i \in \mathcal{N} \text{ y } a_i \neq a_i' \tag{3.6}$$

En otras palabras, en un equilibrio de Wardrop, cada jugador escoge la estrategia que minimiza su función potencial dada la estrategia del resto de jugadores.

### 3.2.2. ¿Qué son los juegos no atómicos?

Un **juego no atómico** es un tipo de juego donde el conjunto de jugadores no tiene influencia sobre las estrategias del resto de jugadores. En el contexto de los juegos de congestión, el hecho de que el coste de utilizar un recurso dependa directamente del número de jugadores que lo usen, implica que los costes no cambiarán con ningún cambio de estrategia. En nuestro caso particular podemos asumir este comportamiento en diferentes escenarios:

i. Cuando los mineros interpreten que sus decisiones no afectan a las utilidades obtenidas de minar una criptomoneda.

ii. Cuando el número de mineros activos en una *blockchain* es muy elevado.

iii. Cuando el poder de hash total de cada minero es demasiado pequeño.

Haurie y Marcotte [4] probaron la existencia y unicidad del equilibrio no atómico (también conocido como equilibrio de Wardrop). Definieron el equilibrio de Wardrop como el limite del equilibrio de Nash de muchos jugadores. Las demostraciones de la existencia y unicidad del equilibrio se encuentran en los teoremas (3.1) y (3.2) respectivamente de [4].

# Capítulo 4

# Modelo y definiciones

Nuestro modelo consiste en una colección de **criptomonedas** $\mathcal{K} = \{1, ..., K\}$, cada una de ellas asociada a su cadena de bloques con su respectivo puzle y dificultad; una colección de **mineros** $\mathcal{N} = \{1, ..., N\}$ que compiten por ser el primero en resolver el puzle de la criptomoneda $k$; y una colección de **servicios en la nube** $\mathcal{S} = \{1, ..., S\}$ que proveen a los mineros de poder de hash para minar la criptomoneda $k$.

Denotaremos como $m_{k,s,i}$ el poder de hash proporcionado por el SN $s$ al minero $i$ para minar la criptomoneda $k$. A lo largo de este análisis asumiremos dos cosas:

i. Todo servicio en la nube proporciona un poder de hash estrictamente positivo. Esto es:
$$m_{k,s} > 0 \text{ para todo } k = 1, ..., K \text{ y } s = 1, ..., S \tag{4.1}$$

ii. Los SNs son simétricos. Esto es:
$$m_{k,s,i} = m_{k,s,j} \text{ para todo } i \text{ y } j \text{ tal que } i \neq j \tag{4.2}$$

Consideraremos también que la asociación de un jugador a un SN $s$ para resolver el puzle $k$ tendrá un coste fijo $c_{k,s}$.

A continuación definiremos la **colección de acciones** de cada minero. Sea $A_i \subset \mathcal{K} \times \mathcal{S}$ la colección de acciones del minero $i$. $A_i$ es una colección de parejas ordenadas (criptomoneda, SN) correspondiente a los servicios en la nube que el minero $i$ puede contratar para minar una criptomoneda. Estas colecciones pueden diferir entre mineros debido a diferentes factores. Entre estos factores se incluyen las limitaciones físicas o reguladoras del poder de hash y la prohibición de uso (y minado) de una criptomoneda. Por ejemplo, como sucede con Bitcoin en China, Bolivia o Bangladesh, entre otros. [9].

Denotaremos la estrategia del minero $i$ como $a_i \in A_i$ y el perfil de estrategias como el vector $a = (a_i)_{i \in \mathcal{N}}$. El perfil de estrategias producirá un vector de carga

$l = (l_{k,s})_{k,s}$ donde $l_{k,s}$ determina el número de usuarios que minan la criptomoneda $k$ con el SN $s$. Notamos que $l_{k,s}$ es equivalente a $x_{k,s}(a)$ visto en los conceptos previos (3.4).

Con esto, podemos definir el total de poder de hash, $M_k$, que se utiliza para minar la criptomoneda $k$,

$$M_k = \sum_{s \in \mathcal{S}} \sum_{i \in \mathcal{N}} m_{k,s,i} \tag{4.3}$$

Asumiendo (4.2) podemos simplificar (4.3) de la siguiente manera:

$$M_k = \sum_{s \in \mathcal{S}} l_{k,s} m_{k,s} \tag{4.4}$$

Notamos que, como el poder de hash proporcionado por una SN es el mismo independientemente del minero que se asocie a él, basta con saber cuantos mineros seleccionan el par (criptomoneda, SN). No es necesario conocer sus identidades.

Definimos a continuación la probabilidad de que el minero $i$ sea el primero en resolver el puzle de la criptomoneda $k$. Sea $\mathcal{T}_k$ el tiempo que le lleva al primer minero resolver el puzle de la criptomoneda $k$ con cualquier SN. Sea $q_k$ la probabilidad de que el puzle $k$ sea resuelto en tiempo $T$. Dada la manera en la que se ajusta la complejidad de los puzles (cada cambio de época) vemos que tanto $\mathcal{T}_k$ como $q_k$ dependen de $M_k$. Esto es debido a que el tiempo que se tarda en resolver un puzle depende del número de mineros que están tratando de encontrar la solución.

Sea $H_{k,s,i}$ la cantidad de poder de hash que el minero $i$ necesita para resolver el puzle $k$ con el SN $s$. Como anteriormente hemos asumido que los mineros son simétricos (4.2), tenemos que las variables aleatorias $H_{k,s,i}$ son independientes y están idénticamente distribuidas para todo $i \in \mathcal{N}$. Cada $H_{k,s,i}$ está distribuida exponencialmente con parámetro $m_{k,s}$. Entonces, si hay $l_{k,s}$ mineros asociados al SN $s$ minando $k$, el tiempo que necesita el minero más rápido para resolver el puzle $k$ está distribuido exponencialmente con parámetro $M_k$. Por tanto:

$$\mathcal{T}_k \sim Exp(M_k) \tag{4.5}$$

$$q_k = 1 - \exp\left(-TM_k\right) \tag{4.6}$$

Notemos que si $T$ es suficientemente grande, $q \approx 1$.

A continuación definiremos las **recompensas**, **costes** y **utilidad** de un jugador. Empecemos primero definiendo cual es la probabilidad de que el minero $i$ asociado al SN $s$ sea el primero en resolver el puzle de $k$ bajo el perfil de estrategias $a$ (con vector de carga $l$).

$$p_{k,s}(l) = 1_{l_{k,s}>0} \frac{q_k m_{k,s}}{M_k} \tag{4.7}$$

donde $1_{l_{k,s}>0}$ es 1 si algún minero está minando $k$ con $s$ o 0 en el caso contrario.

Sea $w$ la recompensa por resolver el puzle $k$. Definimos como $\mathcal{U}_{k,s}(l)$, la utilidad que recibiría cualquier minero por intentar resolver $k$ con el SN $s$. La utilidad es la diferencia entre las recompensas y los costes. Tenemos entonces:

$$\mathcal{U}_{k,s}(l) = p_{k,s}w - c_{k,s} \tag{4.8}$$

Para simplificar el análisis, fijaremos $w = 1$ y ajustaremos los costes acordemente. Por tanto, reduciremos (4.8) a:

$$\mathcal{U}_{k,s}(l) = p_{k,s} - c_{k,s} \tag{4.9}$$

Tendremos pues, que la utilidad del minero $i$ será:

$$\mathcal{U}_i(a_i, a_{-i}) = \sum_{(k,s)\in A_i} 1_{a_i=(k,s)}\mathcal{U}_{k,s}(l) \tag{4.10}$$

donde $a_{-i} = (a_1, a_2, a_{i-1}, a_{i+1}, a_N)$ es la configuración de todos los jugadores excluyendo al minero $i$. Resumiendo, el juego que analizaremos esta caracterizado por $G = \langle \mathcal{N}, \mathcal{K} \times \mathcal{S}, (A_i)_{i\in\mathcal{N}}, \mathcal{U}_{(k,s)\in(\mathcal{K}\times\mathcal{S})} \rangle$.

# Capítulo 5

# Análisis de los juegos

En este capitulo analizaremos los juegos planteados anteriormente.

## 5.1. Juego con una única criptomoneda y múltiples SNs

En esta sección estudiaremos el juego con una única criptomoneda y varios SNs. Denotaremos como $k$ la única criptomoneda en el conjunto de criptomonedas para minar. Estudiaremos un juego en el que los mineros tendrán que decidir si asociarse o no a un SN para minar $k$.

El objetivo es establecer una relación entre los juegos de congestión y el juego planteado anteriormente. Para ello, asumiremos que los SN son simétricos. Tanto el poder de hash proporcionado por $s \in \mathcal{S}$ como el coste de asociarse a $s$ serán iguales para todos los SNs. Esto es: $m_{k,s} = m_k$ y $c_{k,s} = c_k$ para todo $s$. Aunque este sea un escenario muy simplificado, nos servirá para analizar juegos más complejos a lo largo del trabajo.

Dado este contexto, adaptaremos nuestro modelo para reflejar el juego. Sea $l_k$ el número de mineros que deciden asociarse a un SN para minar $k$,

$$l_k = \sum_{s \in \mathcal{S}} \sum_{i \in \mathcal{N}} 1_{s_i = (k,s)} \tag{5.1}$$

Entonces, podemos reducir (4.7) a:

$$p_k(l_k) = 1_{l_k > 0} \frac{q_k m_k}{l_k m_k} = 1_{l_k > 0} \frac{1 - \exp\left(-TM_k\right)}{l_k} \tag{5.2}$$

**Observación 5.1.** A lo largo de este documento, asumiremos que $0/0 = 0$. En este caso tendremos que $p_k = 0$ si $l_k = 0$.

**Teorema 5.2.** *Supongamos que para todo i y j, $A_i = A_j$ (estrategias iguales entre jugadores). Entonces el equilibrio de Nash de este juego viene dado por la solución del siguiente problema de optimización:*

$$\arg\max_{l_k} \sum_{l=1}^{l_k} (p_k(l) - c_k) \tag{5.3}$$

$$\textit{sujeto a:} \quad l_k \leq N, \quad l_k \geq 0 \tag{5.4}$$

*donde $l_k$ es el número de jugadores que deciden minar k y la ecuación* (5.3) *es la función potencial del juego.*

*Demostración.* En efecto, el juego presentado es un juego de congestión como el definido en los conceptos previos (véase 3.2.1). Por lo tanto, el juego admite una función potencial (3.5). Finalmente, cualquier juego que admite una función potencial tiene al menos un equilibrio puro de Nash. □

**Observación 5.3.** En los conceptos previos hemos definido la función potencial en función de los costes. Por lo tanto, en ese caso, buscábamos minimizar la función. En este caso la hemos definido en función de la utilidad y, por lo tanto, buscamos maximizarla. Podemos darnos cuenta que la definición dada en los conceptos previos (3.5) es equivalente a la del teorema substituyendo los costes por la utilidad.

El siguiente objetivo es demostrar la existencia del equilibrio de Nash con condiciones más relajadas. Para ello consideraremos que los SN no son simétricos. El poder de hash proporcionado variará entre SNs y los costes se mantendrán iguales. Veremos que, aún así, podemos establecer una relación con los juegos de congestión.

**Teorema 5.4.** *Supongamos que para todo i y j, $A_i = A_j$. Supongamos también que $c_{k,s} = c_{k,s'}$ y $m_{k,s} \neq m_{k,s'}$ para todo s y s′ tal que $s \neq s'$. Entonces el equilibrio de Nash viene dado por la solución del siguiente problema de optimización:*

$$\arg\max_{l_{k,s^*}} \sum_{l=1}^{l_{k,s^*}} (p_{k,s^*}(l) - c_k) \tag{5.5}$$

$$\textit{sujeto a:} \quad l_{k,s^*} \leq N, \quad l_{k,s^*} \geq 0 \tag{5.6}$$

*donde $s^* = max\{s : m_{k,s} \geq m_{k,s'} \; \forall s'\}$.*

*Demostración.* Sea $l'_{k,s}$ el número de total de mineros, excepto uno, que deciden minar $k$ con el SN $s$. Para probar el teorema necesitamos que $l'_{k,s}$ no esté en equilibrio. Tenemos que, el jugador que decidió no minar $k$ está enfrentándose al siguiente problema de optimización:

$$\text{máx} \left\{ \max_{s} \left\{ \frac{m_{k,s}(1-\exp(-T(m_{k,s}+\sum_{s'} l'_{k,s'} m_{k,s'})))}{m_{k,s}+\sum_{s'} l'_{k,s'} m_{k,s'}},\ c_k \right\} \right\} \tag{5.7}$$

donde la parte izquierda del máximo es el cambio en la utilidad que se provocaría si el minero decide minar con $s$. Para estudiar el problema consideremos la siguiente función:

$$f(x) = \frac{x(1-\exp(-T(x+\sum_{s'} l'_{k,s'} m_{k,s'})))}{x+\sum_{s'} l'_{k,s'} m_{k,s'}} \tag{5.8}$$

Vemos que $f(x)$ es una función estrictamente positiva para $x > 0$. Por lo tanto tenemos que,

$$\max_{x} f(x) = f(m_{k,s^*}) = \frac{m_{k,s^*}(1-\exp(-T(m_{k,s^*}+\sum_{s'} l'_{k,s'} m_{k,s'})))}{m_{k,s^*}+\sum_{s'} l'_{k,s'} m_{k,s'}} \tag{5.9}$$

con $s^* = max\{s : m_{k,s} \geq m_{k,s'}\ \forall s'\}$. Por lo tanto, la utilidad de cualquier jugador en equilibrio será:

$$\text{máx} \left\{ \frac{m_{k,s^*}(1-\exp(-T(m_{k,s^*}+\sum_{s'} l'_{k,s'} m_{k,s'})))}{m_{k,s^*}+\sum_{s'} l'_{k,s'} m_{k,s'}} - c_k,\ 0 \right\} \tag{5.10}$$

Resumiendo, la mejor respuesta de cualquier jugador en $l'_{k,s}$ es:

1. Asociarse a $s^*$, con $s^* = max\{s : m_{k,s} \geq m_{k,s'}\ \forall s'\}$.
2. Decidir no minar $k$.

Por lo tanto, asumiendo que ningún minero se asociará a un SN diferente a $s^*$, esté juego vuelve a ser un juego de congestión en el sentido descrito en los conceptos previos (véase 3.2.1). Finalmente, por el teorema (5.2), existe un equilibrio puro de Nash. □

### 5.1.1. Ejemplo

Consideraremos un juego con 3 mineros y 4 SNs, $N = 3$ y $S = 4$. Cada SN proporcionará un poder de hash $m_{k,s}$ de 0.1, 0.2, 0.5, 0.7 para $s = 1, 2, 3, 4$ respectivamente. Si un minero decide no asociarse a ningún SN, este tendrá un poder de hash de 0. El coste de asociarse a un SN, $c_k$, será de 0.3 y para simplificar los cálculos, $T = 1$. Por el teorema (5.4) tenemos que, en equilibrio, los mineros decidirán no minar o bien asociarse a $s^* = 4$. Entonces la utilidad de un jugador vendrá dada por:

$$U_{k,s^*} = \begin{cases} \dfrac{1-\exp(-m_{k,s^*} l_{k,s^*})}{l_{k,s^*}} - c_k & \text{si } l_{k,s^*} > 0 \\ 0 & \text{si } l_{k,s^*} = 0 \end{cases}$$

Por tanto, $U_{k,s^*}$ será igual a $0, 0.203, 0.077, -0.007$ para $l_{k,s^*} = 0, 1, 2, 3$ respectivamente. Ahora, para $l_{k,s^*} = 0, 1, 2, 3$ tenemos que la ecuación (5.5) es:

$$\sum_{l=1}^{l_{k,s^*}} (p_{k,s^*}(l) - c_k) = \begin{cases} 0 & \text{si } l_{k,s^*} = 0 \\ 0.203 & \text{si } l_{k,s^*} = 1 \\ 0.28 & \text{si } l_{k,s^*} = 2 \\ 0.273 & \text{si } l_{k,s^*} = 3 \end{cases}$$

Por lo tanto, la expresión se maximiza para $l_{k,s^*} = 2$. Entonces tenemos que, en equilibrio, dos mineros se asociaran a $s^*$ para minar $k$ y el otro decidirá no minar. Finalmente, tenemos 3 posibles equilibrios. En cada uno de ellos, uno de los mineros decide no minar $k$.

## 5.2. Juego con múltiples criptomonedas y un SN

En esta sección introduciremos el juego con múltiples criptomonedas $K$ y un único SN $s$. En este contexto, intentaremos buscar de nuevo propiedades de equilibrio.

Como en el caso anterior, adaptaremos el juego con las condiciones especificadas. En primer lugar, podemos reformular la la probabilidad de que un minero sea el primero en resolver el puzle $k$ (4.7) como:

$$p_k(l_k) = \frac{1-\exp(-T m_k l_k)}{l_k} \tag{5.11}$$

Dado $l_k$ (cantidad de mineros que deciden minar $k$), reformularemos la utilidad de un minero (4.8) al minar $k$ como:

$$U_k(l_k) = p_k - c_k \tag{5.12}$$

Para este juego añadiremos la condición de que un minero decidirá no minar $k$ si la utilidad de minar $k$ es negativa. Observaremos que teoremas similares a los presentados anteriormente nos servirán para encontrar y caracterizar las propiedades de equilibrio de este juego.

**Teorema 5.5.** *Supongamos que para todo i y j, $A_i = A_j$. El número de mineros que decide minar k, $l_k = \sum_{i \in \mathcal{N}} 1_{a_i=k}$ es solución del siguiente problema de optimización:*

$$\arg\max_{l} \sum_{k \in \mathcal{K}} \sum_{l=1}^{l_k} (p_k(l) - c_k) \tag{5.13}$$

$$\textit{sujeto a:} \quad \sum_{k \in \mathcal{K}} l_k \leq N, \quad l_k \geq 0 \tag{5.14}$$

*Demostración.* La prueba del teorema es análoga a la del teorema (5.4) substituyendo las ecuaciones (5.3)-(5.4) por las del teorema. □

## 5.3. Juegos con múltiples criptomonedas y múltiples SNs

En este capitulo estudiaremos el juego con múltiples criptomonedas y múltiples SNs. Para ello asumiremos que los mineros son jugadores no atómicos. Formularemos la utilidad de cada minero teniendo en cuenta que los mineros son no atómicos y estudiaremos el equilibrio no atómico del vector de carga $l$.

En nuestro juego, dado un vector de carga $l$, los mineros trataran de solucionar el siguiente problema de optimización:

$$\text{máx}\{\max_{k,s}\{U_{k,s}(l), 0\}\} \tag{5.15}$$

donde,

$$U_{k,s}(l) = \frac{m_{k,s}}{\sum_{s'} m_{k,s'} l_{k,s'}} q_k \left( \sum_{s'} m_{k,s'} l_{k,s'} \right) - c_{k,s} \tag{5.16}$$

En este caso, como el valor del vector de carga no se modificará con ningún cambio de estrategia, la probabilidad de que un juego sea resuelto en tiempo $T$, $q_k$, estará en función del poder total de hash inicial utilizado para minar $k$. Tendremos entonces que:

$$q_k = 1 - \exp(-TM'_k) \tag{5.17}$$

siendo $M'_k$ el poder total de hash utilizado para minar $k$ antes de cualquier cambio de estrategia de cualquier minero.

Por tanto, la mejor estrategia de un jugador dado un vector de carga $l$ cualquiera, vendrá dada por el arg max de la ecuación (5.15). A continuación caracterizaremos el vector de equilibrio no atómico $l^*$.

### 5.3.1. Caracterización del vector de equilibrio no atómico

Sea $l^*$ el vector de equilibrio no atómico. Entonces $l^*$ satisface:

$$U_{k,s}(l^*) = U_{k',s'}(l^*), \quad \text{si } l^*_{k,s} > 0,\, l^*_{k',s'} > 0,\, \forall s, s', k, k' \tag{5.18}$$

$$U_{k,s}(l^*) \geq U_{k',s'}(l^*), \quad \text{si } l^*_{k,s} > 0,\, l^*_{k',s'} = 0,\, \forall s, s', k, k' \tag{5.19}$$

$$U_{k,s}(l^*) \leq 0, \quad \text{si } l^*_{k,s} = 0,\, \forall s, k \tag{5.20}$$

$$\sum_{k,s} l^*_{k,s} \leq N \tag{5.21}$$

Antes de seguir con el estudio de las propiedades tenemos que responder la siguiente pregunta. ¿Puede un jugador estar interesado en desviarse del equilibrio $l^*$? Para resolver esta pregunta definamos primero el conjunto de mineros que están en equilibrio. Sea $A(l^*)$ el conjunto de estrategias de los mineros cuyos pares (criptomoneda, SN) están en equilibrio:

$$A(l^*) = \{(k,s) \mid l^*_{k,s} > 0,\ l^*_{k,s} \text{ solución de (5.18) } - \text{ (5.21)}\} \tag{5.22}$$

La primera ecuación (5.18) implica que para todo par (criptomoneda, SN) en $A(l^*)$ la utilidad es la misma. Si existiera cualquier otro par (criptomoneda, SN) cuya utilidad fuese mayor (teniendo en cuenta que ningún minero tiene influencia sobre el vector de carga y por tanto sobre la utilidad) nadie escogería el par inicial. Por lo tanto, si un minero decidiera desviarse del equilibrio $l^*$, el arg max de (5.15) tendría que ser un par $(k', s') \notin A(l^*)$. Pero, si un jugador decidiera escoger una estrategia $(k', s') \notin A(l^*)$ debido a la segunda ecuación (5.19) tendríamos que esta elección no es óptima. En conclusión, un minero racional siempre escogería una estrategia $(k, s) \in A(l^*)$ lo cual implica que el vector de carga $l^*$ que satisface (5.18) - (5.21) está en equilibrio.

Para las siguientes secciones, asumiremos que $l^*$ existe.

### 5.3.2. ¿A cuántos SNs decidirán los mineros asociarse?

A continuación, dada una criptomoneda cualquiera, estudiaremos que y cuantos SNs son usados por los mineros para minarla. Analizaremos bajo que condiciones los mineros deciden asociarse solo a un SN y bajo que condiciones a más de uno.

#### 5.3.2.1. ¿Qué condiciones deben darse para que los mineros decidan asociarse a un solo SN?

A continuación daremos un teorema con las condiciones necesarias para que dada una criptomoneda, los jugadores decidan asociarse tan solo a un SN.

**Teorema 5.6.** *Dada una criptomoneda k, si se cumplen las siguientes condiciones:*

*i.* $c_{k,s} = c_{k,s'}$ *para todo* $s$, $s'$

*ii.* $m_{k,s} \neq m_{k,s'}$ *para todo* $s \neq s'$

*entonces, (1) los mineros se asociaran únicamente a un SN y (2) este será el que provea de poder de hash más alto.*

*Demostración.* Supongamos que, dada una criptomoneda $k$, los costes de asociarse a un SN son los mismos para todo SN ($c_{k,s} = c_{k,s'}$ para todo $s$, $s'$) y el poder de hash proporcionado por cada SN diferente ($m_{k,s} \neq m_{k,s'}$ para todo $s \neq s'$). Vamos a demostrar el teorema por contradicción. Supongamos que en equilibrio $l^*$ existen dos elementos, $l^*_{k,s}$ y $l^*_{k,s'}$ tal que $l^*_{k,s} > 0$ y $l^*_{k,s'} > 0$ para $s \neq s'$. Pero, de acuerdo a (5.18), si $l^*_{k,s} > 0$ y $l^*_{k,s'} > 0$ observamos que:

$$\mathcal{U}_{k,s}(l^*) = \mathcal{U}_{k,s'}(l^*)$$

$$\Leftrightarrow \frac{m_{k,s}}{\sum_{s'} m_{k,s'} l_{k,s'}} q_k \left( \sum_{s'} m_{k,s'} l_{k,s'} \right) - c_{k,s} = \frac{m_{k,s}}{\sum_{s'} m_{k,s'} l_{k,s'}} q_k \left( \sum_{s'} m_{k,s'} l_{k,s'} \right) - c_{k,s'}$$

$$\Leftrightarrow m_{k,s} = m_{k,s'}$$

Por tanto, llegamos a una contradicción demostrando (1). Además, si los mineros se asocian únicamente a un SN, de acuerdo a (5.19), este será el que provea de mayor poder de hash $m_{k,s}$ demostrando así (2). □

#### 5.3.2.2. ¿A cuántos SNs se asociaran los mineros como máximo?

En esta sección nos hacemos la siguiente pregunta: ¿Cuántos SNs serán contratados por los mineros para minar $k$? A continuación veremos que la respuesta a esta pregunta es dos.

Pero antes de ver este resultado necesitamos la siguiente definición:

**Definición 5.7.** Diremos que dos pares de SNs $(s, s')$ y $(s'', s''')$ tales que, $m_{k,s} < m_{k,s'}$ y $m_{k,s''} < m_{k,s'''}$ son colineales respecto $k$ si:

$$\frac{m_{k,s} - m_{k,s'}}{c_{k,s} - c_{k,s'}} = \frac{m_{k,s''} - m_{k,s'''}}{c_{k,s''} - c_{k,s'''}} \tag{5.23}$$

Intuitivamente, diremos que dos pares de SNs son colineales cuando la diferencia entre sus poderes de hash y costes pueden ser linealmente alineados.

**Teorema 5.8.** *Si ningún par de SNs es colineal respecto a k, entonces, en equilibrio, los mineros se asociaran a un máximo de dos SNs.*

*Demostración.* Demostraremos este teorema por contradicción. Supongamos que en equilibrio, $l^*$, existen tres elementos $l^*_{k,s}$, $l^*_{k,s'}$, $l^*_{k,s''}$ tales que $l^*_{k,s}, l^*_{k,s'}, l^*_{k,s''} > 0$. Entonces, por (5.18) tenemos el siguiente sistema:

$$U_{k,s}(l^*) = U_{k,s'}(l^*)$$

$$\Leftrightarrow \frac{m_{k,s} - m_{k,s'}}{\sum_{i \in S} m_{k,i} l_{k,i}} q_k \left( \sum_{i \in S} m_{k,i} l_{k,i} \right) = c_{k,s} - c_{k,s'}$$

$$U_{k,s}(l^*) = U_{k,s''}(l^*)$$

$$\Leftrightarrow \frac{m_{k,s} - m_{k,s''}}{\sum_{i \in S} m_{k,i} l_{k,i}} q_k \left( \sum_{i \in S} m_{k,i} l_{k,i} \right) = c_{k,s} - c_{k,s''}$$

Dividiendo ambas ecuaciones, obtenemos que:

$$\frac{m_{k,s} - m_{k,s'}}{m_{k,s} - m_{k,s''}} = \frac{c_{k,s} - c_{k,s'}}{c_{k,s} - c_{k,s''}}$$

$$\Leftrightarrow \frac{m_{k,s} - m_{k,s'}}{c_{k,s} - c_{k,s'}} = \frac{m_{k,s} - m_{k,s''}}{c_{k,s} - c_{k,s''}}$$

lo que lleva a una contradicción, concluyendo la demostración. □

# Capítulo 6

# ¿Qué hará un minero a lo largo del tiempo?

A continuación definiremos el segundo modelo del trabajo. Este será una adaptación del modelo ya introducido. En vez de buscar la mejor estrategia a la hora de resolver un puzle en particular, intentaremos dar estrategias para obtener una mayor utilidad a lo largo de varias épocas. Para ello, definiremos de manera determinista cual es la recompensa de un minero por cada unidad de hash usada. Definiremos también cuanto poder de hash es necesario para finalizar una época.

Dado el modelo, demostraremos que el "equilibrio esperado" (cuya estrategia será denominada por minería genuina en las siguientes secciones) no es realmente un equilibrio. Veremos que las estrategias presentadas (en adelante, minería eficiente y minería eficiente optimizada), bajo ciertas condiciones, dominan a la minería genuina.

## 6.1. Adaptación del modelo

El modelo consiste en una única criptomoneda $k$ y una colección de **mineros** $\mathcal{N} = \{1, ..., N\}$ que minan $k$ usando su infraestructura. Cada minero tendrá un poder máximo de hash que le permitirá realizar $m_i$ hashes (computaciones) por unidad de tiempo. Los costes se dividirán en costes fijos $cf_i$ por unidad de tiempo (independientemente del poder que se use) y costes variables $cv_i$ por cada computación realizada. Los costes fijos hacen referencia al mantenimiento y actualización del hardware especializado. Los costes variables hacen referencia al consumo de energía del hardware.

Definiremos el poder total de hash de los mineros como:

$$M = \sum_{i \in \mathcal{N}} m_i \tag{6.1}$$

Como hemos mencionado en los conceptos previos (véase 3.1.3), una época consiste en un número fijo de bloques $B$ y la *blockchain* se encarga de determinar la dificultad para que esta termine en tiempo $\mathcal{T}$. Esto se consigue escogiendo la complejidad necesaria para que resolver $B$ puzles (añadir $B$ bloques) requiera $\mathcal{T} \cdot M$ computaciones. Diremos entonces que una época consiste en $\mathcal{T} \cdot M$ computaciones, siendo $\mathcal{T}$ un parámetro fijado por la *blockchain*.

El modelo progresará en épocas secuenciales $e_1$, $e_2$, .... Como los mineros son libres, puede que el número de computaciones por unidad de tiempo varíe entre épocas. Por tanto, una época $e_j$ consistirá en $H_j$ computaciones. Entonces, para $j > 0$, la época $e_j$ empezará inmediatamente después de que $H_{j-i}$ computaciones sean realizadas por todos los mineros en la época $e_{j-1}$. Denotaremos por $T_j$ el número de unidades de tiempo que tarda la época $e_j$ en ser completada. Inicialmente, tendremos que $H_1 = M\mathcal{T}$. Vemos que, si los jugadores minan con la totalidad de su poder de hash, $T_1 = \mathcal{T}$. Ahora, para las siguientes épocas, la *blockchain* se encargará de ajustar la dificultad. Tendremos que $H_{j-1}/T_{j-1}$ estimará el total de poder usado en la época $j-1$. Esto es: para cada $j > 1$, la época $e_j$ consiste en

$$H_j = \frac{H_{j-1}}{T_{j-1}}\mathcal{T} \tag{6.2}$$

computaciones totales.

A continuación definiremos las recompensas por unidad de hash. Para cada $j > 1$, la recompensa por unidad de hash en la época $j$ es:

$$RH_j = \frac{w}{H_j} \tag{6.3}$$

siendo $w$ la recompensa proporcionada por la *blockchain* en cada época. Como hemos visto en secciones anteriores, en el caso de Bitcoin, $w = 6.25$ Bitcoins.

Como hemos mencionado antes, en este modelo, los mineros podrán decidir que cantidad de poder de hash utilizar. Aunque permitiremos esto, para simplificar el análisis, asumiremos que los mineros no modifican el poder con el que minan durante una época. Diremos que $m_i(j) \leq m_i$ será el poder de hash que utiliza el minero $i$ en la época $e_j$. Dado $m_i(j)$, definiremos el coste del minero $i$ en la época $e_j$ como:

$$c_i(j) = cf_i + cv_i \cdot m_i(j) \tag{6.4}$$

y la recompensa por unidad de tiempo del minero $i$ en la época $j$ como:

$$R_i(j) = RH_j \cdot m_i(j) = \frac{w}{H_j} \cdot m_i(j) \tag{6.5}$$

Definiremos los beneficios del minero $i$ en la época $j$ como:

$$B_i(j) = R_i(j) - c_i(j) \tag{6.6}$$

Finalmente, definimos la utilidad del minero $i$ como la media de las recompensas por unidad de tiempo a lo largo de un número indefinido de épocas:

$$U_i = \lim_{J\to\infty} \frac{\sum_{j=1}^{J}(R_i(j) - c_i(j)) \cdot T_j}{\sum_{j=1}^{J} T_j} \tag{6.7}$$

A lo largo del documento supondremos que las recompensas obtenidas en las épocas en las que todo minero mina con todo su poder son $R_i(j) = \frac{m_i}{M\mathcal{T}} w = cf_i - cv_i m_i + \alpha$. Intuitivamente, los beneficios obtenidos por minar con la totalidad del poder de hash serán $\alpha$. Con el objetivo de simplificar los cálculos $\alpha \to 0$. Como consecuencia, tenemos que $w = \frac{(cf_i + cv_i \cdot m_i) M\mathcal{T}}{m_i}$. Por tanto, para determinar si una estrategia domina la minería genuina, bastará con encontrar una estrategia tal que $U_i > 0$.

## 6.2. Estrategias de minería racional

En esta sección demostraremos que lo que intuitivamente podría parecer un equilibrio (todos los mineros minan con el total de su poder), no lo es. Veremos dos estrategia que, bajo ciertas condiciones, mejoran los resultados del minero.

### 6.2.1. Minería eficiente

En esta primera estrategia, el minero que decida desviarse de la minería genuina, minará en épocas alternas. Supongamos que para $j' < j$ cada uno de los jugadores mina con todo su poder. En este contexto, tendremos que para $j' < j$, los valores de $T_{j'}$, $H_{j'}$ y $RH_{j'}$ estarán fijos en $\mathcal{T}$, $M\mathcal{T}$ y $\frac{w}{M\mathcal{T}}$ respectivamente. Supongamos también que el minero que se desvía de esta estrategia no mina en las épocas $\{e_j, e_{j+2}, ...\}$ y mina en las épocas $\{e_{j+1}, e_{j+3}, ...\}$. A continuación analizaremos las recompensas que el minero obtiene al desviarse de la minería genuina.

**Época** $j$. Tenemos que, por definición, $T_{j-1} = \mathcal{T}$. Entonces, si el minero decide no minar en la época $j$, tenemos que:

$$H_j = M\mathcal{T}$$

$$T_j = \frac{H_j}{M - m_i} = \frac{M\mathcal{T}}{M - m_i} = \frac{\mathcal{T}}{1 - \frac{m_i}{M}}$$

$$R_i(j) - c_i(j) = \underbrace{\frac{w}{M\mathcal{T}} \cdot m_i(j)}_{0} - (cf_i + \underbrace{cv_i \cdot m_i(j)}_{0}) = -cf_i$$

La recompensa del minero $i$ en la época $j$ es:

$$B_i(j) \cdot T_j = -\mathcal{T} \cdot cf_i \cdot \frac{M}{M - m_i}$$

**Época** $j+1$. Ahora, como $T_j = \frac{\mathcal{T}}{1-\frac{m_i}{M}} > \mathcal{T}$ el ajuste de dificultad reduce la complejidad de los puzles y, por lo tanto, incrementa la recompensa por unidad de computación. En la época $j+1$ el minero mina con todo su poder:

$$H_{j+1} = \frac{H_j}{T_j}\mathcal{T} = M\mathcal{T}\left(1 - \frac{m_i}{M}\right)$$

$$T_{j+1} = \frac{H_{j+1}}{M} = \mathcal{T}\left(1 - \frac{m_i}{M}\right)$$

$$RH_{j+1} = \frac{w}{H_{j+1}} = \frac{w}{M\mathcal{T}(1-\frac{m_i}{M})} = \frac{w}{M\mathcal{T} - \mathcal{T}m_i} = \frac{w}{\mathcal{T}(M - m_i)}$$

$$R_i(j+1) - c_i(j+1) = RH_{j+1}m_i - (cf_i + cv_i \cdot m_i) = \frac{wm_i}{\mathcal{T}(M-m_i)} - (cf_i + cv_i \cdot m_i)$$

La recompensa del minero $i$ en la época $j+1$ es:

$$\begin{aligned} B_i(j+1) \cdot T_{j+1} &= \mathcal{T} \cdot \left[\frac{wm_i}{\mathcal{T}(M-m_i)} - (cf_i + cv_i \cdot m_i)\right] \cdot \frac{M - m_i}{M} \\ &= \mathcal{T} \cdot \left[\frac{(cf_i + cv_i \cdot m_i)M}{M - m_i} - (cf_i + cv_i \cdot m_i)\right] \cdot \frac{M - m_i}{M} \\ &= \mathcal{T} \cdot (cf_i + cv_i \cdot m_i) \cdot \frac{m_i}{M} \end{aligned}$$

**Época** $\geq j+2$. Ahora, $T_{j+1} = \mathcal{T}(1 - \frac{m_i}{M})$. En esta época el minero no mina:

$$H_{j+2} = \frac{H_{j+1}}{T_{j+1}}\mathcal{T} = \frac{M\mathcal{T}(1-\frac{m_i}{M})}{\mathcal{T}(1-\frac{m_i}{M})}\mathcal{T} = M\mathcal{T} = H_j$$

$$T_{j+2} = \frac{H_{j+2}}{M - m_i} = \frac{\mathcal{T}}{1-\frac{m_i}{M}} = T_j$$

$$RH_{j+2} = \frac{w}{H_{j+2}} = \frac{w}{M\mathcal{T}} = RH_j$$

$$R_i(j+2) - c_i(j+2) = -cf_i = R_i(j)$$

Observamos que en las épocas $\{e_{j+2}, e_{j+4}, ...\}$ obtenemos los mismos resultados que en la época $e_j$ y en las épocas $\{e_{j+3}, e_{j+5}, ...\}$ los mismos resultados que en la época $e_{j+1}$.

Veamos ahora cual es la utilidad del minero $i$ a lo largo de un número indefinido de épocas.

$$\begin{aligned}
\mathcal{U}_i &= \lim_{J\to\infty} \frac{\sum_{j=1}^{J} B_i(j)\cdot T_j}{\sum_{j=1}^{J} T_j} \\
&= \lim_{J\to\infty} \frac{\sum_{j=1}^{J} B_i(2j+1)\cdot T_{2j+1} + \sum_{j=1}^{J} B_i(2j)\cdot T_{2j}}{\sum_{j=1}^{J} T_j} \\
&\overset{*}{=} \frac{B_i(2j+1)\cdot T_{2j+1} + B_i(2j)\cdot T_{2j}}{T_{j+1}+T_j} \\
&= \frac{(cf_i + cv_i\cdot m_i)\cdot \frac{m_i}{M} - cf_i\cdot\frac{M}{M-m_i}}{1-\frac{m_i}{M}+\frac{1}{1-\frac{m_i}{M}}}
\end{aligned}$$

donde en $\overset{*}{=}$, podemos considerar únicamente una época de cada tipo para calcular la media.

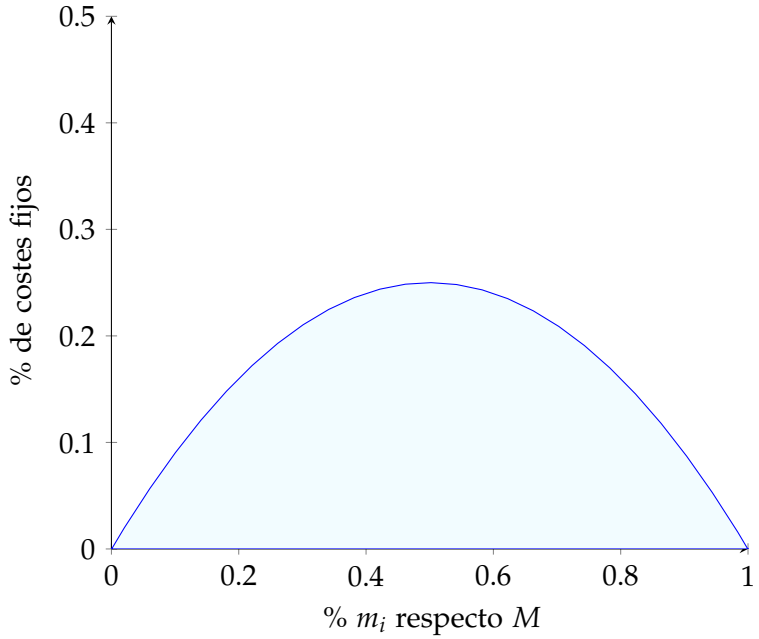
Ahora queremos ver cuando $U_i > 0$. Las condiciones que cumplan la inecuación serán las que determinarán cuando la minería eficiente domina a la minería genuina.

$$\begin{aligned}
&U_i > 0 \\
&\Leftrightarrow (cf_i + cv_i\cdot m_i)\cdot\frac{m_i}{M} > cf_i\cdot\frac{M}{M-m_i} \\
&\Leftrightarrow \frac{m_i}{M}\cdot\frac{M-m_i}{M} > \frac{cf_i}{cf_i+cv_im_i}
\end{aligned}$$

Denotaremos por $y = \frac{cf_i}{cf_i+cv_im_i}$ el porcentaje de costes fijos respecto el total de los costes y por $x = \frac{m_i}{M}$ el porcentaje de poder de minado del jugador $i$ con respecto al total de poder de minado $M$. Tenemos entonces que esta estrategia domina a la minería genuina cuando $x\cdot(1-x) > y$ para $(x,y)\in(0,1)\times(0,1)$.

En la Figura 6.1 podemos observar la estructura de costes con los que la minería eficiente domina a la minería genuina. La estrategia es dominante en cualquier punto por debajo de la curva de la Figura 6.1. Por ejemplo, cuando los costes fijos del minero $i$ representan el 20 % del total obtendrá un mayor beneficio si tiene entre un 20 % y un 72 % del poder de minado total aproximadamente.

Figura 6.1: Minería eficiente




#### 6.2.1.1. ¿Se beneficia el resto de mineros?

A continuación comprobaremos si los mineros que deciden mantener la minería genuina se benefician de que otro minero se desvíe hacia la minería eficiente. Supongamos que el minero $k$ adopta la minería eficiente y el minero $i$ la minería genuina. Queremos ver si la utilidad del minero $i$, $U_i$, es mayor que 0. Debido a la semejanza entre los escenarios, utilizaremos algunos de los resultados obtenidos.

**Época** $j$. En esta época el minero $k$ decide no minar. Por lo tanto, todos los resultados excepto el de las recompensas son equivalentes a los de la época $j$ del análisis anterior. En cambio, la recompensa del minero $i$ en la época $j$ es:

$$B_i(j) \cdot T_j = \mathcal{T} \cdot \left[\frac{w}{M\mathcal{T}} \cdot m_i - (cf_i + cv_i \cdot m_i)\right] \cdot \frac{M}{M - m_k} = 0$$

**Época** $j+1$. En esta época el minero $k$ decide minar de nuevo. Equivalentemente a la época $j$, podemos utilizar los resultados del caso anterior. Por tanto tenemos que la recompensa del minero $i$ en la época $j$ es:

$$B_i(j+1) \cdot T_{j+1} = \mathcal{T} \cdot \left[\frac{wm_i}{\mathcal{T}(M - m_k)} - (cf_i + cv_i \cdot m_i)\right] \cdot \frac{M - m_k}{M}$$

$$= \mathcal{T} \cdot (cf_i + cv_i \cdot m_i) \cdot \frac{m_k}{M}$$

De la misma manera, observamos que en las épocas $\{e_{j+2}, e_{j+4}, ...\}$ obtenemos los mismos resultados que en la época $e_j$ y en las épocas $\{e_{j+3}, e_{j+5}, ...\}$ los mismos resultados que en la época $e_{j+1}$.

Veamos ahora cual es la utilidad del minero $i$ a lo largo de varias épocas:

$$\mathcal{U}_i = \frac{B_i(2j+1) \cdot T_{2j+1} + B_i(2j) \cdot T_{2j}}{T_{j+1} + T_j} > 0$$

$$\Leftrightarrow \frac{\mathcal{T} \cdot (cf_i + cv_i \cdot m_i) \cdot \frac{m_k}{M}}{1 - \frac{m_k}{M} + \frac{1}{1 - \frac{m_k}{M}}} > 0$$

$$\Leftrightarrow (cf_i + cv_i \cdot m_i) \cdot \frac{m_k}{M} > 0$$

La inecuación se cumple en cualquier caso. Obtenemos entonces que cualquier minero se beneficia del desvío de otro minero hacia la minería eficiente.

### 6.2.2. Minería eficiente optimizada

En esta sección intentaremos mejorar la estrategia minería eficiente. Veremos que, con un único cambio y bajo ciertas condiciones, el minero podrá obtener mayores beneficios. Aumentaremos el espacio de estrategias del minero $i$ habilitando la posibilidad de minar con poder de hash $m'_i(j) \in [0, m_i]$ en la época $j$.

Con el objetivo de aumentar la utilidad total del minero, intentaremos reducir el gasto generado en las épocas de no minado. ¿Cómo lo haremos? Como en el escenario anterior, el jugador minará en épocas alternas con diferentes poderes de hash. Pero en lugar de decidir no minar en ciertas épocas, el minero $i$ minará con poder de hash $m'_i(j) \in [0, m_i]$. Gracias a este cambio reduciremos los gastos a cambio de reducir también los beneficios en las épocas en las que mina con el total del poder de hash. El minero que optimice $m'_i(j)$ de manera inteligente gozará de mayores recompensas a lo largo del tiempo.

De la misma manera que en los casos anteriores, analizaremos las recompensas obtenidas siguiendo esta estrategia. En las épocas $\{e_j, e_{j+2}, ...\}$ el jugador minará con poder de hash $m'_i(j)$ y en las épocas $\{e_{j+1}, e_{j+3}, ...\}$ minará con el total. Denotaremos $\Delta m_i = m_i - m'_i(j)$ como la cantidad de poder de hash no usada durante las épocas $\{e_j, e_{j+2}, ...\}$.

**Época** $j$. Tenemos que, por definición, $T_{j-1} = \mathcal{T}$. Entonces, si el minero decide minar con $m'_i$ en la época $j$, obtenemos los siguientes resultados:

$$H_j = M\mathcal{T}$$

$$T_j = \frac{H_j}{M - \Delta m_i} = \frac{M\mathcal{T}}{M - \Delta m_i} = \frac{\mathcal{T}}{1 - \frac{\Delta m_i}{M}}$$

$$RH_j = \frac{w}{H_j} = \frac{w}{M\mathcal{T}}$$

$$\begin{aligned} B_i(j) &= \frac{w}{M\mathcal{T}} - (cf_i + cv_i \cdot m_i'(j)) \\ &= \frac{(cf_i + cv_i \cdot m_i) \cdot m_i'(j)}{m_i} - (cf_i + cv_i \cdot m_i'(j)) \\ &= cf_i \cdot \left(\frac{m_i'(j)}{m_i} - 1\right) \end{aligned}$$

La recompensa del minero $i$ en la época $j$ es:

$$\begin{aligned} B_i(j) \cdot T_j &= \left[cf_i \cdot \left(\frac{m_i'(j)}{m_i} - 1\right)\right] \cdot \frac{\mathcal{T}}{1 - \frac{\Delta m_i}{M}} \\ &= \frac{(m_i'(j) - m_i)M}{m_i(M - \Delta m_i)} \cdot cf_i \cdot \mathcal{T} \\ &= -\frac{\Delta m_i}{m_i} \cdot \frac{M}{M - \Delta m_i} \cdot cf_i \cdot \mathcal{T} \end{aligned}$$

**Época** $j+1$. Como $T_j = \frac{\mathcal{T}}{1 - \frac{\Delta m_i}{M}}$, la dificultad se reduce y por tanto aumentan las recompensas. En esta época el jugador $i$ mina con el total de su poder. Por tanto los resultados que obtenemos son:

$$H_{j+1} = \frac{H_j}{T_j}\mathcal{T} = (M - \Delta m_i) \cdot \mathcal{T}$$

$$T_{j+1} = \frac{H_{j+1}}{M} = \frac{M - \Delta m_i}{M} \cdot \mathcal{T}$$

$$RH_{j+1} = \frac{w}{H_{j+1}} = \frac{w}{(M - \Delta m_i)\mathcal{T}}$$

$$\begin{aligned} B_i(j+1) &= \frac{wm_i}{(M - \Delta m_i)\mathcal{T}} - (cf_i + cv_i \cdot m_i) \\ &= (cf_i + cv_i \cdot m_i) \cdot \left(\frac{M}{M - \Delta m_i} - 1\right) \end{aligned}$$

La recompensa del minero $i$ en la época $j+1$ es:

$$B_i(j+1) \cdot T_{j+1} = \left[(cf_i + cv_i \cdot m_i) \cdot \left(\frac{M}{M - \Delta m_i} - 1\right)\right] \cdot \frac{M - \Delta m_i}{M} \cdot \mathcal{T}$$

$$= \left[ cf_i + cv_i \cdot m_i - \frac{(cf_i + cv_i \cdot m_i) \cdot (M - \Delta m_i}{M} \right] \mathcal{T}$$

$$= \mathcal{T}(cf_i + cv_i \cdot m_i) \left( 1 - \frac{M - \Delta m_i}{M} \right)$$

$$= \frac{\mathcal{T} \cdot \Delta m_i}{M} (cf_i + cv_i \cdot m_i)$$

**Época** $\geq j + 2$. Como, $T_j = \frac{M - \Delta m_i}{M} \cdot \mathcal{T}$, $H_{j+2} = M\mathcal{T} = H_j$. Como en los casos anteriores, observamos que los resultados de las épocas $\{e_{j+2}, e_{j+4}, ...\}$ son equivalentes a los de la época $j$ y los resultados de las épocas $\{e_{j+3}, e_{j+5}, ...\}$ son equivalentes a los de la época $j + 1$.

Veamos ahora cual es la utilidad del minero $i$ si adopta esta estrategia:

$$\mathcal{U}_i = \lim_{J \to \infty} \frac{\sum_{j=1}^{J} B_i(j) \cdot T_j}{\sum_{j=1}^{J} T_j}$$

$$= \lim_{J \to \infty} \frac{\sum_{j=1}^{J} B_i(2j+1) \cdot T_{2j+1} + \sum_{j=1}^{J} B_i(2j) \cdot T_{2j}}{\sum_{j=1}^{J} T_j}$$

$$= \frac{B_i(2j+1) \cdot T_{2j+1} + B_i(2j) \cdot T_{2j}}{T_{j+1} + T_j}$$

$$= \frac{\frac{\cdot \Delta m_i}{M}(cf_i + cv_i \cdot m_i) - \frac{\Delta m_i}{m_i} \cdot \frac{M}{M - \Delta m_i} \cdot cf_i}{\frac{M - \Delta m_i}{M} + \frac{M}{M - \Delta m_i}}$$

Ahora queremos ver bajo que condiciones esta estrategia domina a la minería genuina.

$$U_i > 0$$

$$\Leftrightarrow \frac{\Delta m_i}{M}(cf_i + cv_i \cdot m_i) > \frac{\Delta m_i}{m_i} \cdot \frac{M}{M - \Delta m_i} \cdot cf_i$$

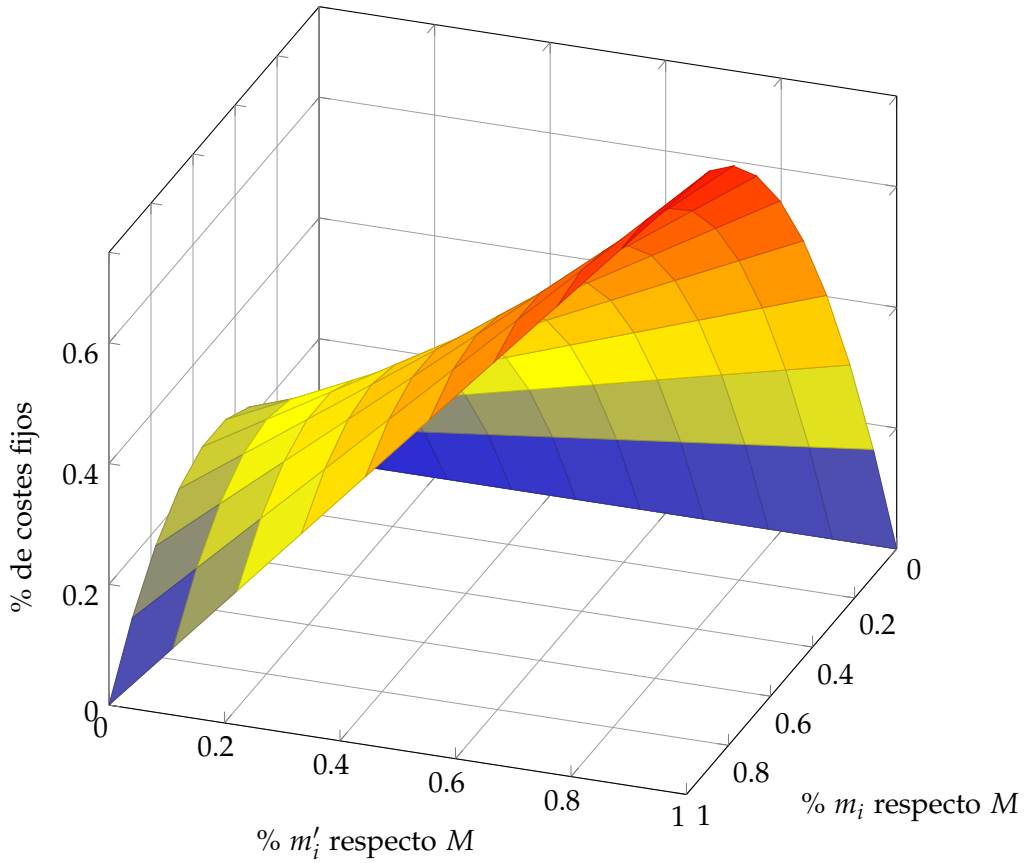
$$\Leftrightarrow \frac{m_i(M - \Delta m_i)}{M^2} > \frac{cf_i}{cf_i + cv_i \cdot m_i}$$

$$\Leftrightarrow \frac{m_i M - mi^2 + m_i m_i'}{M^2} > \frac{cf_i}{cf_i + cv_i \cdot m_i}$$

$$\Leftrightarrow -\left(\frac{m_i}{M}\right)^2 + \frac{m_i}{M}\left(1 + \frac{m_i'}{M}\right) > \frac{cf_i}{cf_i + cv_i \cdot m_i}$$

Denotaremos por $z = \frac{cf_i}{cf_i + cv_i m_i}$ el porcentaje de costes fijos respecto al total de los costes. Denotaremos también por $x = \frac{m_i}{M}$ y por $y = \frac{m_i'}{M}$ el porcentaje de $m_i$ y $m_i'$ respectivamente del jugador $i$ con respecto al total de poder de minado $M$. Tenemos entonces que esta estrategia domina a la minería genuina cuando $-x^2 + x(1+y) > z$ para $(x, y, z) \in (0,1) \times (0,1) \times (0,1)$.

Figura 6.2: Minería eficiente optimizada




En la Figura 6.2 podemos ver que combinaciones de $x, y$ y $z$ cumplen la inecuación. Cualquier combinación por debajo de la curva domina la estrategia de minería genuina.

## 6.3. ¿Puede verse comprometida la seguridad de una *blockchain*?

Como hemos visto en la Sección 6.2.1.1 que un minero decida desviarse de la minería genuina beneficia al resto de mineros. Esto sucede debido a que la dificultad se reduce en las épocas posteriores a las que el minero que se desvía decide no minar o minar con menos poder de hash. Por tanto, los mineros que decidan seguir la minería genuina no tienen ningún motivo para oponerse a este comportamiento. De lo contrario, podrían decidir unirse al ataque obteniendo mayores beneficios. Esto puede comprometer seriamente la seguridad de cualquier criptomoneda.

#### ¿Por qué puede verse comprometida la seguridad de una blockchain?

Como hemos comentado en los conceptos previos (véase 3.1.2) cualquier criptomoneda está sujeta a los ataques del 50 %.

Supongamos que el minero $i$ posee el 25 % del poder total de minado. Supongamos también, que los costes fijos del minero representan el 10 % del total. Como hemos visto en la Sección 6.2.1, este se beneficiaría de adoptar la estrategia de minería eficiente. En las épocas en las que decidiera no minar, bastaría con tener más del 37,5 % del poder de minado para que este tipo de ataque fuera efectivo. La vulnerabilidad crece más si consideramos al resto de mineros. Como hemos mencionado antes, el resto de mineros podrían decidir adoptar esta estrategia de la misma manera que lo hace el minero $i$.

Contra-intuitivamente observamos también que la unión de nuevos mineros a la *blockchain* empeora los problemas de seguridad. Suponiendo que los mineros son racionales, estos decidirán unirse en las épocas con mayores recompensas. De la misma manera, aquellos que se unan en estas épocas, se irán en las siguientes evitando así las épocas con menores recompensas. Esta situación aumentaría drásticamente la dificultad en las épocas con menor recompensas provocando el abandono de los mineros cuya estrategia es la minería genuina. Consecuentemente, el abandono masivo de mineros de la *blockchain*, abre la puerta a los ataques del 50 %. También podría provocar una época eterna llevando a la criptomoneda al colapso.

# Capítulo 7

# Conclusiones y trabajo futuro

La competición entre los mineros es fundamental en los sistemas de *blockchain* públicos. La competencia es uno de los elementos fundamentales para garantizar que los mineros se esfuercen por alcanzar un consenso sobre el estado actual de la *blockchain*. En la primera parte de este trabajo hemos modelado la competición entre mineros como un juego no cooperativo. Usando resultados de los juegos de congestión hemos sido capaces de mostrar propiedades del equilibrio de Nash. En particular, hemos caracterizado dichos equilibrios a través de problemas que admiten soluciones algorítmicas.

Posteriormente, hemos demostrado que un minero totalmente racional puede optar por no minar en ciertos momentos con el objetivo de maximizar sus recompensas. En algunos casos, adoptar las estrategias de minería eficiente y minería eficiente optimizada resulta una mejor opción. Finalmente, hemos mostrado como la seguridad de la *blockchain* puede verse comprometida. Ataques como el del 50 % resulta más sencillo de ejecutar cuando los mineros adoptan este tipo de estrategias.

Creemos que este trabajo abre varias direcciones interesantes para futuras investigaciones. Como ampliación de la primera parte, podríamos permitir la contratación de una fracción del poder de hash proporcionado por un servicio en la nube. En otra posible extensión del trabajo, podríamos añadir variables que determinen las limitaciones física de un minero. Por ejemplo, la legislación podría imponer límites al consumo de energía. También podríamos considerar limitaciones a nivel global. En cuanto a la segunda parte del trabajo, podríamos ampliar la investigación encontrando nuevas estrategias que mejoren las planteadas. Finalmente, podríamos comparar las estrategias entre sí y ver en qué casos es mejor adoptar una u otra.

# Capítulo 8

# Agradecimientos

Para finalizar el Trabajo de Fin de Grado, quiero agradecer el apoyo de Josep Vives Santa Eulalia, encargado de la tutoría del proyecto, cuyos consejos han sido esenciales para el buen desarrollo de todas las fases.

En general, agradecer a todo el equipo docente del Grado de Matemáticas de la UB.

# Apéndice A

# Notación

## A.1. Tabla de notación del modelo

| Valor | Descripción |
|---|---|
| K | Número de criptomonedas (puzles) |
| N | Número de jugadores (mineros) |
| S | Número de servicios en la nube (SN) |
| $m_{k,s}$ | Poder de hash proporcionado por el SN $s$ para minar $k$ |
| $A_i \subset \mathcal{K} \times \mathcal{S}$ | Acciones del minero $i$ (criptomoneda, SN) |
| $a_i \in A_i$ | Estrategia del minero $i$ |
| $l_{k,s}$ | Número de mineros que minan $k$ con el SN $s$ |
| $l$ | Vector de carga asociado al perfil de estrategias |
| $\mathcal{T}_k$ | Tiempo que tarda el primer minero en resolver $k$ con cualquier SN |
| $q_k$ | Probabilidad de que el puzle $k$ se resuelva en tiempo $T$ |
| $p_{k,s}$ | Probabilidad de que el minero asociado a $s$ sea el primero en minar $k$ |
| $w_k$ | Recompensa por ser el primero en resolver $k$ |
| $c_{k,s}$ | Coste de minar $k$ asociado a $s$ |
| $U_{k,s}$ | Utilidad del minero que se asocia a $s$ para minar $k$ |

## A.2. Tabla de notación del modelo adaptado

| Valor | Descripción |
|---|---|
| M | Poder de hash total de los mineros |
| $\mathcal{T}$ | Duración deseada de una época (fijada por la *blockchain*) |
| $T_j$ | Duración real de la época $j$ |
| $H_j$ | Computaciones necesarias para completar la época $j$ |
| $RH_j$ | Recompensa por unida de hash de la época $j$ |
| w | Recompensa total proporcionada por la *blockchain* en cada época |
| $\mathfrak{m}_i(j) \in [0, m_i]$ | Poder de hash usado por el minero $i$ en la época $j$ |
| $cf_i$ | Costes fijos del minero $i$ |
| $cv_i$ | Costes variables del minero $i$ |
| $c_i(j)$ | Costes totales del minero $i$ en la época $j$ |
| $R_i(j)$ | Recompensa por unidad de tiempo del minero $i$ en la época $j$ |
| $B_i(j)$ | Beneficio por unidad de tiempo del minero $i$ en la época $j$ |
| $U_i$ | Utilidad del minero $i$: media de las recompensas por unidad de tiempo a lo largo de un número indefinido de épocas |

# Bibliografía


[1] Vitalik Buterin et al. "A next-generation smart contract and decentralized application platform". En: *white paper* 3.37 (2014), págs. 2-1.

[2] *Comparación de uso de energia de Bitcoin con otros paises*. Accedido el 10/04/2023. URL: https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html.

[3] *Estado del mercado de las criptomonedas*. Accedido el 10/04/2023. URL: https://coin360.com/.

[4] Alain Haurie y Patrice Marcotte. "On the relationship between Nash—Cournot and Wardrop equilibria". En: *Networks* 15.3 (1985), págs. 295-308.

[5] *La minería de Bitcoin consume el 0,5 de toda la electricidad utilizada a nivel mundial y 7 veces el uso total de Google, según un análisis*. Accedido el 13/04/2023. URL: https://www.businessinsider.es/mineria-bitcoin-consume-05-electricidad-nivel-mundial-927499.

[6] *MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols*. Accedido el 27/03/2023. URL: https://ieeexplore.ieee.org/document/9444429?denied=.

[7] Dov Monderer y Lloyd S Shapley. "Potential games". En: *Games and economic behavior* 14.1 (1996), págs. 124-143.

[8] Satoshi Nakamoto. "Bitcoin: a peer-to-peer electronic cash system". En: (2008).

[9] *Prohibición de Bitcoin: estos son los países donde las criptomonedas están restringidas o son ilegales*. Accedido el 12/04/2023. URL: https://www.euronews.com/next/2022/08/25/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2.

[10] Robert W Rosenthal. "A class of games possessing pure-strategy Nash equilibria". En: *International Journal of Game Theory* 2 (1973), págs. 65-67.

[11] *The Death Spiral: How Terra's Algorithmic Stablecoin Came Crashing Down*. Accedido el 18/04/2023. URL: https://www.forbes.com/sites/rahulrai/2022/05/17/the-death-spiral-how-terras-algorithmic-stablecoin-came-crashing-down/?sh=34f44b9e71a2.

[12] *The idea and a brief history of cryptocurrencies*. Accedido el 11/04/2023. URL: https://guardian.ng/technology/tech/the-idea-and-a-brief-history-of-cryptocurrencies/.