Universidad de Buenos Aires
Facultad de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Teoría de Juegos y Bitcoin
Modelo de Juego de Minería Óptima para un Equilibrio Estable y Descentralizado de la Red Bitcoin

Autor: David Lajeunesse
Director: Dr. Hugo Scolnik

2020
Cohorte 2019

Declaración jurada de origen de los contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

_____

David Lajeunesse
Pasaporte: GL086416

Resumen

Este trabajo trata de la aplicación de la teoría de juegos para modelizar la minería del sistema Bitcoin. En particular, se modeliza la minería como un juego y se propone un modelo de minería óptima para soportar la descentralización y la estabilidad de la red mediante la consecución de equilibrios en los subjuegos que componen el modelo. En primer lugar, se discuten los conceptos fundamentales de la teoría de juegos, así como se hace una breve descripción de Bitcoin. Luego, se presentan dos modelos, uno estático y uno dinámico, que han sido desarrollados en otros trabajos y que sirven de base para la propuesta de un modelo de juego de minería óptima más elaborado cuyo objetivo es garantizar la descentralización y la estabilidad de Bitcoin. Una prueba de concepto se realiza utilizando simulaciones para demostrar la viabilidad del modelo propuesto. Por último, se presentan un breve análisis y observaciones que se pueden extraer del trabajo realizado.

Palabras claves: Teoría de juegos, Bitcoin, minería, modelo estocástico, juego Stackelberg, dilema social, cooperación, equilibrio estable, descentralización, seguridad.

Tabla de contenido

Tablas y Figuras

Agradecimientos

Sin orden particular:
A mi familia,
A mis amigos,
A mis colegas de la maestría,
Al cuerpo docente de la maestría,
Al coordinador académico, el Dr. Pedro Hecht,
A mí director de tesis, el Dr. Hugo Scolnik, cuyas recomendaciones y correcciones ciertamente han contribuido a mejorar el trabajo.

Indroducción

La teoría de juegos (TDJ) como formulación matemática general no fue desarrollada hasta 1944 por John Von Neumann y Oscar Morgenstern [1], pero las ideas detrás de ella han estado alimentando discusiones desde los días de la antigua Grecia, cuando algunos de los textos de Platón ya destacaron los dilemas adyacentes a los procesos de toma de decisiones y sus consecuencias en ciertas situaciones definidas. En *Laches*[1] y *Symposium*[2], Platón relata un episodio de la Guerra de Delium, en el que los soldados evalúan las consecuencias de sus elecciones en cuanto a sus contribuciones personales a la batalla sobre el resultado de esta [2]. Este tipo de análisis libre ha encontrado desde entonces una estructura y fundamentos lógicos en el desarrollo de la teoría de juegos, que generalmente se define como el estudio de los modelos matemáticos de las interacciones estratégicas entre agentes racionales (es decir, tomadores de decisiones) [3]. Todavía considerada hoy en día como una teoría que no ha alcanzado su plena madurez, es constantemente objeto de críticas, así como de nuevos desarrollos y aplicaciones. La reciente tecnología de cadena de bloques (*blockchain*) no es la excepción y muchos ven la teoría de juegos como una herramienta para analizar este tipo de sistema, incluyendo los aspectos de seguridad.

La tecnología de cadena de bloques es una aplicación específica de la tecnología de registros distribuidos (DLT)[3]. La DLT permite el mantenimiento de un registro de datos descentralizado: los datos se replican y se distribuyen entre varias entidades y no están bajo la autoridad de ninguna entidad central [4]. La tecnología de cadena de bloques agrupa los datos del registro en bloques y los vincula criptográficamente entre sí, lo que permite combinar con éxito los conceptos de descentralización, seguridad y privacidad. Fue con la publicación en 2008 del *white paper Bitcoin: A Peer-to-Peer Electronic Cash System* [5], y su implementación poco después, que Satoshi Nakamoto dio origen a la primera aplicación de cadena de bloques exitosa: Bitcoin, un sistema de moneda digital descentralizado. Aunque ninguna otra cadena de bloques ha tenido tanto éxito como Bitcoin hasta la fecha, en

[1] https://es.wikipedia.org/wiki/Laques_(di%C3%A1logo)
[2] https://en.wikipedia.org/wiki/Symposium_(Plato)
[3] *Distributed Ledger Technology*

los últimos años se han realizado importantes inversiones en el desarrollo de esta prometedora tecnología.

El objetivo de este trabajo es utilizar la teoría de juegos, primero para evaluar y entender la dinámica del proceso de minería de Bitcoin, y luego para proponer un modelo de juego de minería óptima que tenga como objetivo mejorar la seguridad del sistema, garantizando su descentralización y estabilidad mediante el alcance de equilibrios en las soluciones de los subjuegos que componen el modelo propuesto.

En cuanto a la estructura del trabajo, la sección 1 describe los fundamentos de la teoría de juegos: la sección 1.1 presenta las definiciones y premisas importantes, la sección 1.2 disecciona la tipología de la teoría de juegos, la sección 1.3 enumera los conceptos importantes para determinar las soluciones de los juegos, y la sección 1.4 resume los conceptos vistos en la sección 1 en forma de un mapa conceptual. El resto del trabajo trata específicamente de Bitcoin. La sección 2.1 proporciona una descripción general de Bitcoin y presenta los problemas de seguridad relacionados con el proceso de minería actual. Las secciones 2.2 y 2.3 presentan respectivamente un modelo estático y estocástico que se han desarrollado en otros trabajos y son aplicables a la minería Bitcoin. Estos dos modelos sirven como base para la propuesta de un modelo más completo en la sección 2.4. La sección 2.5 propone un modelo aún más amplio de minería óptima y cuya solución global conduce a un equilibrio estable y descentralizado de la red. El modelo incluye la propuesta de un protocolo de pool de minería y está compuesto por varios subjuegos que aplican el modelo propuesto de la sección 2.4. La sección 2.6 hace una prueba de concepto sobre el rendimiento y la viabilidad del modelo de juego de minería óptima. Por último, la sección 2.7 proporciona un análisis y observaciones que resultan del trabajo realizado.

El alcance del trabajo no cuestiona las premisas subyacentes a la teoría de juegos y asume los conceptos de solución de los juegos como válidos, aunque este aspecto es objeto de varios debates. Del mismo modo, aparte de una corrección realizada sobre el término $e^{-\lambda z t_i}$ del modelo estático en la sección 2.2, no se cuestiona la validez de las soluciones aplicadas de otros trabajos.

1 Teoría de Juegos

En esta sección se analizan los conceptos necesarios para comprender la aplicación de la TDJ en el resto del trabajo. La sección 1.1 formula las definiciones y premisas que rigen la TDJ. La sección 1.2 presenta la tipología y establece las divisiones principales de la TDJ. La sección 1.3 presenta los principales conceptos de solución, es decir, las reglas formales que enmarcan el análisis de las interacciones estratégicas entre los jugadores y permiten resolver los juegos. Por último, la sección 1.4 presenta un mapa conceptual que resume la sección 1 [6].

1.1 Definiciones y Premisas

Juego: Conjunto de circunstancias cuyo resultado depende de las acciones de dos o más jugadores [7].

Jugador: Tomador de decisiones estratégicas en el contexto del juego [7].

Estrategia: Conjunto de las acciones tomadas por un jugador en cada punto de decisión, a lo largo del juego, en función de las circunstancias del mismo [7], [8]. El conjunto de estrategias para todos los jugadores se llama un *conjunto de estrategias*.

Resultado: Situación que resulta de la combinación de las estrategias de los jugadores. Cada combinación de estrategias (una para cada jugador) conduce a un resultado del juego. [9]

Utilidad (o ganancia): La utilidad de un jugador asociada con un resultado del juego se refiere de manera general a su nivel de satisfacción con ese resultado. La utilidad se puede representar en cualquier forma cuantificable (por ejemplo, en dólares) [7] y se estima mediante una función matemática que cuantifica el nivel de preferencia de un jugador entre los posibles resultados del juego, según ciertos parámetros [10] (como por ejemplo, la aversión al riesgo [11]).

Según lo interpretado por la teoría de juegos, un juego debe especificar cuatro elementos esenciales: (i) los jugadores que lo componen, las posibles estrategias para esos jugadores (basado en (ii) la información y (iii) las acciones disponibles para ellos

en cada punto de decisión), y (iv) las utilidades para cada resultado posible del juego. Estos elementos se utilizan junto con un *concepto de solución* para analizar las *interacciones estratégicas* entre los jugadores. [3] Un concepto de solución es un método matemático que permite determinar un conjunto de estrategias, llamado *conjunto de estrategias de equilibrio*, en el que ningún jugador puede mejorar su utilidad modificando su estrategia [3]. La adopción por todos los jugadores de la estrategia de equilibrio conduce a un resultado estable del juego, y es una de las principales motivaciones de la teoría de juegos [9].

La TDJ estudia las interacciones estratégicas entre los jugadores, en las que (i) cada acción tomada por uno debe tener un efecto en el resultado, (ii) que debe ser de interés para todos, es decir, cada jugador debe tener preferencias en cuanto al resultado del juego. La naturaleza estratégica de las interacciones significa que los jugadores toman sus decisiones considerando el efecto de sus acciones y de las de los demás en el resultado. Para estructurar las interacciones y determinar un concepto de solución que asigne poder predictivo a la teoría de juegos, se establecen dos premisas para gobernar el comportamiento de los jugadores: la racionalidad y el conocimiento común. [12]

La premisa de racionalidad establece que los jugadores son racionales: adoptan la mejor estrategia para lograr los resultados que prefieran. En otras palabras, tienen preferencias bien definidas y conocidas sobre los posibles resultados del juego, y pueden determinar y aplicar la mejor estrategia para sí mismos dependiendo de las circunstancias. [12] El principio de conocimiento común amplía aún más la implicación de la naturaleza estratégica de las interacciones definida anteriormente, que dice que los jugadores son conscientes de que sus acciones y las de los demás tienen un efecto en el resultado. El conocimiento común establece que las reglas del juego, incluyendo la naturaleza estratégica de las interacciones y la racionalidad de los jugadores, son conocidas por todos [12]. Resulta en la aplicación de un razonamiento en bucle en el análisis de las interacciones (el jugador 1 sabe que el jugador 2 sabe que el jugador 1 sabe, y así sucesivamente) que permite deducir en cascada las acciones de cada uno y determinar un concepto de solución del juego.

1.2 Tipología

La teoría de juegos establece una clasificación que permite categorizar cada situación de acuerdo con sus características para determinar los métodos de resolución apropiados. Los parámetros principales que se evalúan para la clasificación y el análisis de un juego se definen a continuación.

1.2.1 Cronología del Juego – Simultáneo vs Secuencial

En un juego simultáneo, los jugadores deciden sus estrategias simultáneamente o, de manera conceptualmente equivalente, sin tener ninguna información sobre las acciones de los demás. Los juegos simultáneos normalmente están representados por una matriz que identifica la utilidad de cada jugador para cada combinación posible de estrategias, es decir, para cada resultado posible del juego. [3], [13], [14]

Un juego secuencial implica una secuencia de acciones entre jugadores, los cuales pueden elegir sus estrategias en cada punto de decisión en función de las acciones disponibles, de la información que tienen sobre las acciones previas de los demás y de las utilidades asociadas con cada resultado posible [13], [15]. Sin embargo, esto no implica que la información sea perfecta (sección 1.2.5): un jugador puede tener información parcial[4] sobre las acciones tomadas por otro [3], [16]. Los juegos secuenciales se representan como un árbol de decisiones[5], en el que cada intersección corresponde a un punto de decisión de un jugador y cada rama a una acción posible. En la base del árbol, es decir, las hojas, se encuentran las distintas utilidades para cada combinación posible de estrategias. En teoría, cualquier juego secuencial también puede representarse en la forma normal, pero la complejidad de la matriz que presenta todas las posibles combinaciones de resultados y utilidades puede hacer que sea poco práctico. [3]

[4] Por ejemplo, un jugador puede saber que otro no realizó ciertas acciones, pero sin saber exactamente qué acción tomó. [3], [16]
[5] i.e. representación extensiva.

La simultaneidad y secuencialidad también se refieren a las nociones más generales de juego estático y dinámico. Un juego es dinámico si proporciona información al menos a un jugador; de lo contrario, es estático [17].

Juego Stackelberg

Un juego Stackelberg es un modelo particular de juego secuencial utilizado para representar situaciones donde hay un líder y un seguidor: el líder juega primero y el seguidor decide su acción de acuerdo con la acción del líder. Por ejemplo, en una relación venta-compra, el vendedor es el líder que decide el precio de venta y el comprador es el seguidor que decide cuánto comprar en función del precio de venta. [18], [19]

1.2.2 Frecuencia del Juego – Ordinario vs Repetido

Un juego ordinario es un juego simultáneo que se juega sólo una vez, mientras que un juego repetido constituye varias iteraciones del mismo juego ordinario [20] y puede ser representado por la forma extensiva [21], [22]. La distinción entre estos dos tipos de juegos influye directamente en el análisis de las interacciones entre los jugadores y la determinación de un concepto de solución. En un juego ordinario, ya que se juega sólo una vez, los jugadores a menudo se benefician de actuar según sus propios intereses para maximizar sus utilidades. En un juego repetido, sin embargo, deben considerar el impacto de sus acciones en el comportamiento futuro de los demás: es decir, deben tener en cuenta su *reputación* [23]. Esto abre la puerta a la cooperación entre ellos y a posibles estrategias que pueden aumentar sus utilidades. [24]

Juego Estocástico

Los juegos estocásticos son una generalización de los repetidos. Son una repetición de juegos ordinarios de un conjunto, y el jugado durante una iteración depende probabilísticamente del que se jugó y de las acciones tomadas por los jugadores durante la iteración anterior. Cada juego del conjunto representa un estado en el que las circunstancias difieren de los otros estados. Un juego repetido es uno estocástico con un solo estado, el del juego ordinario original. El hecho de que un

juego estocástico se repita una serie de períodos (es decir, iteraciones) finita o infinita[6] influye en las estrategias de los jugadores y la determinación del concepto de solución. [10]

Proceso de Decisión de Markov

Un proceso de decisión de Markov (MDP) es un caso especial de juego estocástico [10]. Con cada transición de estado, los jugadores eligen una acción disponible y, en función de ella, se otorga una recompensa al pasar al estado siguiente. La probabilidad de una cierta transición depende del estado actual y de las acciones tomadas por los jugadores. Formalmente, un MDP es una cuádrupla $\{S, A, P_a, R_a\}$, donde [25] :

S es un conjunto de estados;
A es un conjunto de acciones;
$P_a = P_a(S, S') = P({S_{t+1}}'|S_t, a_t)$ es la probabilidad de transitar al estado S' desde el estado S tomando la acción a ;
$R_a = R_a(S, S')$ es la recompensa, o recompensa esperada, cuando el sistema transita del estado S al estado S' tomando la acción a

1.2.3 Cooperación en el Juego – Cooperativo vs No Cooperativo

Un juego no cooperativo no permite formar alianzas, es decir, coaliciones: las acciones son individuales y el análisis está orientado a predecir las estrategias de los jugadores y sus utilidades. Por el contrario, cuando estos últimos pueden coordinarse y comprometerse entre sí para adherirse a una estrategia definida con el fin de obtener mejores resultados para el grupo, se dice que el juego es cooperativo [26]. El análisis se centra entonces en la predicción de las alianzas que se formarán, de las acciones que tomarán y de las utilidades colectivas [3].

Sin embargo, la cooperación es una noción distinta de las preferencias individuales de los jugadores, las cuales pueden converger o divergir tanto en los

[6] El concepto importante no es que el juego esté realmente finito o infinito, sino más bien la percepción que los jugadores tienen del juego. [10]

juegos cooperativos que los no cooperativos [10]. En un juego cooperativo, las preferencias individuales se tienen en cuenta, pero son las acciones de las alianzas las que se modelan en lugar de las de los jugadores individuales. [27]

Competencia de Cournot

Una competencia de Cournot es un caso especial del llamado juego no cooperativo agregativo, en el que la utilidad de un jugador es función de su propia estrategia y del conjunto de estrategias de todos los jugadores. Formalmente, podemos expresar la siguiente dependencia:

$$U_i = f\left(x_i, \sum_{j=1}^{n} x_j\right) \tag{1}$$

donde U_i es la utilidad del jugador i, n es el número de jugadores, f es una función que vincula la estrategia x_i del jugador i y el conjunto de estrategias de todos los jugadores a U_i. [28]

1.2.4 Simetría del Juego – Simétrico vs Asimétrico

La definición más común de simetría es la de juego simétrico ordinario (*ordinary symmetric game)*. Básicamente, Brandt et al. (citado en [29]) definen un juego simétrico ordinario como un juego en el que todos los jugadores tienen el mismo espacio de estrategias disponibles y esencialmente las mismas utilidades. En este tipo de juego, los jugadores no distinguen entre los demás, es decir, las identidades individuales no importan. Lo que importa es conocer la distribución del número de jugadores que adoptan cada estrategia. Además, obtener "esencialmente las mismas utilidades" no significa que sean las mismas para todos, sino que están determinadas de la misma manera.

1.2.5 Conciencia de la Información – Perfecta vs Imperfecta

Un juego se considera con información perfecta cuando no se mantiene ninguna información en secreto y un jugador sabe, en el momento de tomar sus decisiones, el estado inicial del juego y todos los eventos que han ocurrido

previamente. De lo contrario, la información se considera imperfecta. Los juegos de información perfecta son una subcategoría de los secuenciales: los simultáneos generalmente no se consideran con información perfecta porque implica que los jugadores deben tomar decisiones ignorando las acciones tomadas simultáneamente por otros. [2], [3], [30]

1.2.6 Conocimiento de la Información – Completa vs Incompleta

Un juego con información completa implica el conocimiento común por parte de todos los jugadores de las funciones de utilidad de cada uno, de la estructura del juego, de las estrategias disponibles y de los resultados asociados. Por el contrario, un juego con información incompleta implica que los jugadores carecen de información para modelizar adecuadamente el comportamiento de los demás y para decidir sobre su propia estrategia óptima[7]. Deben especificar creencias sobre las posibles características de los otros[8] y sus comportamientos se definen probabilísticamente: el juego se llama entonces un juego *bayesiano*[9]. [11], [31]

[7] La estrategia óptima de un jugador es la que optimiza su utilidad.
[8] Estas creencias toman la forma de una distribución de probabilidades.
[9] En este tipo de juego, los jugadores actualizan la distribución de sus creencias en función de las elecciones realizadas por los otros jugadores utilizando la regla de Bayes [110], [31].

1.3 Conceptos de Solución

La tipología proporciona una estructura para analizar las interacciones entre los jugadores y deducir las estrategias que estos adoptarán para maximizar su utilidad. Este conjunto de estrategias, llamado *conjunto de estrategias de equilibrio* o *solución* [6], conduce al resultado del juego: un estado estable en el que ningún jugador se beneficia si cambia su estrategia [9]. Un *concepto de solución* es un conjunto de reglas formales que permiten predecir la solución de un juego y que varía según el tipo de juego [6]. A continuación, se presentan los principales conceptos de solución utilizados en la teoría.

1.3.1 Equilibrio de Nash

El equilibrio de Nash (EN) es el concepto de solución más común e importante de la teoría de juegos y se aplica bien a juegos no cooperativos [32] simultáneos [13] y no cooperativos secuenciales con información perfecta [10]. Un EN se alcanza cuando ningún jugador puede aumentar su utilidad cambiando unilateralmente su estrategia, dadas las adoptadas por los demás. Se dice entonces que cada jugador dio su mejor respuesta a las estrategias de los otros. El teorema de Nash afirma que cualquier juego con un número finito de jugadores y de estrategias puras[10] admite al menos un punto de equilibrio. Sin embargo, esto implica que las estrategias mixtas, basadas en distribuciones de probabilidades[11] de estrategias puras, sean posibles [10], [32], [33]. Por otra parte, si el espacio de estrategias disponibles es no compacto[12] y continuo, en cuyo caso el número de estrategias puras es infinito, la existencia de un EN no está asegurada y debe verificarse [34].

Un punto de equilibrio de Nash se dice *estricto* cuando todos los jugadores tienen una única respuesta óptima posible dadas las estrategias de los demás. De lo contrario, el punto de equilibrio es *débil* y al menos un jugador tiene otra mejor respuesta que no coincide con la estrategia de equilibrio y que le permite conseguir la

[10] Una estrategia pura proporciona una definición completa de cómo jugará un jugador [82].
[11] Ver los juegos bayesianos mencionados en la sección 1.2.6. El subconjunto de acciones a las que se le asigna una probabilidad positiva en la estrategia mixta se llama el *soporte* [10].
[12] Un espacio compacto es un subconjunto del espacio euclidiano cerrado y delimitado. Por ejemplo, [0,2] es un espacio compacto mientras $(-\infty, 2]$ y (3,6) no lo son [108].

misma utilidad. Con la excepción de los casos raros en los que sólo hay una mejor respuesta, que entonces es necesariamente una estrategia pura, el número de mejores respuestas siempre es infinito ya que cualquier estrategia mixta que sea una combinación de mejores respuestas también es una mejor respuesta[13]. Siguiendo la misma lógica al revés, un equilibrio de Nash mixto (ENM)[14] surge cuando la estrategia mixta de un jugador es una mejor respuesta, y por lo tanto cada una de las estrategias puras que la componen también es una mejor respuesta [13]. Entonces, un ENM es necesariamente débil, ya que por definición implica múltiples mejores respuestas, mientras que un equilibrio de Nash puro (ENP)[15] puede ser estricto o débil, dependiendo del juego. [10], [33]

En [32], Coleman señala con un ejemplo la inestabilidad inherente a un ENM por ser débil. Esto se debe al principio de conocimiento común que implica que los jugadores saben que pueden desviarse de la estrategia de equilibrio mixto y optar por una mejor respuesta alternativa sin ser penalizados. Por lo tanto, la existencia de un ENM no significa necesariamente que será alcanzado, e incluso, de manera más general, la existencia de una EN no significa que será alcanzado. Los EN son soluciones convincentes para juegos estrictamente competitivos (juegos finitos, dos jugadores, suma cero[16]) ya que los puntos de equilibrio son equivalentes[17] e intercambiables[18]. En estos casos, un jugador puede elegir cualquier estrategia de equilibrio y el resultado siempre será un punto de equilibrio con la misma utilidad[19]. Pero en los otros tipos de juegos, a menudo existen varios equilibrios que no son

---

[13] Shoham y Leyton-Brown [10] usan el juego de guerra de los sexos (https://en.wikipedia.org/wiki/Battle_of_the_sexes_(game_theory)) para explicar bien este concepto, demostrando que en un equilibrio de Nash obtenido cuando al menos un jugador adopta una estrategia mixta, esta hace que el oponente sea indiferente en cuanto a su elección de estrategia. Es decir, la distribución de probabilidades en la cual el jugador basa su estrategia mixta hace que la utilidad esperada del oponente sea la misma independientemente de la estrategia que elija, ya sea pura o mixta que sea cualquier combinación de estrategias puras. Por lo tanto, se deduce que hay un número infinito de mejores respuestas.

[14] Un ENM se obtiene cuando al menos un jugador adopta una estrategia mixta [83].

[15] Un ENP se obtiene cuando todos los jugadores adoptan una estrategia pura.

[16] Un juego de suma cero es uno en el que la suma de las utilidades de los jugadores es igual a cero para todos los resultados posibles [107].

[17] Las utilidades son las mismas [32].

[18] Si (A,B) y (C,D) son puntos de equilibrio intercambiables, (A,D) y (C,B) también son puntos de equilibrio [32].

[19] Sin embargo, en algunos juegos como el ajedrez chino, aunque el equilibrio existe, los jugadores no tienen la inteligencia para saberlo y alcanzarlo dada la complejidad del juego [84].

equivalentes o intercambiables, y la noción de EN no basta para predecir el resultado del juego. [32]

1.3.2 Dominancia de Pareto y Óptimo de Pareto

Los conceptos de dominancia y óptimo de Pareto permiten ordenar parcialmente los conjuntos de estrategias[20] de un juego según las utilidades que generan. Un conjunto de estrategias x Pareto-domina un conjunto x' cuando genera un resultado cuya utilidad de cada jugador es mayor o igual que la de x', con al menos uno cuya utilidad es mayor. Un conjunto de estrategias x es Pareto óptimo si no existe otro conjunto que lo Pareto domine. En un juego, existe necesariamente al menos un óptimo de Pareto, y al menos uno en el que las estrategias son puras. [10]

1.3.3 Dominancia Repetida

La estrategia x_i de un jugador i domina[21] la estrategia x_i' cuando su utilidad es igual o mayor que la de x_i' independientemente de las estrategias de los demás jugadores: en este caso, cuando la utilidad de x_i es mayor que la de x_i' por al menos uno de los conjunto de estrategias, x_i domina débilmente x_i' y cuando siempre es mayor, x_i domina estrictamente x_i'. Más restrictivamente, si la estrategia de un jugador genera una utilidad igual o mayor que cualquiera otra independientemente de las elecciones de sus oponentes, se dice que es débilmente dominante y si siempre genera una utilidad mayor, es estrictamente dominante. [10]

Cuando existe un conjunto de estrategias en el que la de cada jugador es dominante (débilmente o estrictamente), resulta directamente un EN llamado *equilibrio de estrategias (débilmente o estrictamente) dominantes*. Un equilibrio de estrategias estrictamente dominantes conduce a un ENP único. En situaciones reales, sin embargo, las estrategias dominantes no son muy comunes: las dominadas son más comunes y se aplica el principio de dominancia repetida, que consiste en eliminar

[20] Es decir, las estrategias de todos los jugadores.
[21] A diferencia de la dominancia y del óptimo de Pareto que se refieren a conjuntos de estrategias (es decir, estrategias de todos los jugadores), la noción de dominancia repetida se refiere a las estrategias individuales de los jugadores [10].

sucesivamente las estrategias estrictamente dominadas[22] con el fin de reducir la matriz de los posibles resultados del juego. En ciertos casos, esto puede reducir la matriz hasta un solo resultado, que es el EN. El proceso permite la eliminación de una estrategia estrictamente dominada por una estrategia mixta, incluso si no está estrictamente dominada por ninguna estrategia pura. Por lo tanto, el EN obtenido puede ser puro o mixto. El principio de dominancia repetida también se puede usar simplemente para reducir el tamaño de la matriz para facilitar su resolución[23]. [10]

1.3.4 Inducción Hacia Atrás

En los juegos secuenciales finitos con información perfecta[24], la inducción hacia atrás permite deducir las acciones de los jugadores y anticipar el resultado del juego. Al confiar en los supuestos de racionalidad y de conocimiento común, las acciones se deducen sucesivamente al considerar las mejores respuestas de cada jugador en cada punto de decisión, subiendo por el árbol de decisiones, desde los posibles resultados en la base del árbol hasta el punto de decisión donde se hace la evaluación. [2]

1.3.5 Equilibrio de Nash Perfecto en Subjuegos

En la representación extensiva, un subjuego es una sección del árbol de decisiones que comienza en un nodo e incluye todos los puntos de decisión posteriores. Si un punto de decisión del subjuego es parte de un conjunto de información (ver sección 1.2.5 sobre información imperfecta), entonces este conjunto es parte del subjuego. [12]

El equilibrio de Nash perfecto en subjuegos (ENPS) es una generalización del EN por inducción hacia atrás para los juegos secuenciales con información imperfecta [12]. Un ENPS es un EN que también es un equilibrio en todos los subjuegos [35]. En un juego secuencial, un conjunto de estrategias es un EN si los jugadores juegan sus

---

[22] Solo en el caso de estrategias estrictamente dominadas, no importa el orden de eliminación (propiedad *Church-Rosser* [109]). En el caso de estrategias débilmente dominadas, la dominancia repetida sigue siendo aplicable, pero se debe tener en cuenta el orden de eliminación [10].
[23] Computacionalmente, resolver matrices grandes puede resultar ser complejo [10].
[24] Es decir, el jugador conoce su posición en el árbol de decisión de la representación extensiva del juego.

mejores respuestas solo en los subjuegos alcanzados por el conjunto de estrategias de equilibrio. Sin embargo, en un ENPS, los jugadores utilizan sus mejores respuestas en todos los subjuegos, incluso en aquellos que no se alcanzan con el conjunto de estrategias de equilibrio [12]. La diferencia conceptual radica en el supuesto de racionalidad de los jugadores: el ENPS hace posible considerar las acciones irracionales que se pueden tomar por error[25] o para "amenazar" o influenciar al oponente, y que no se tienen en cuenta en el EN [36]. Esto equivale a tomar en consideración la naturaleza imperfecta de la información, ya que un jugador puede no estar seguro de las decisiones tomadas por sus oponentes a lo largo del juego. En este sentido, el ENPS es un refinamiento del EN que pretende superar su insuficiencia para razonar los juegos secuenciales [3].

1.3.6 Equilibrio Perfecto de Markov

Un equilibrio perfecto de Markov (MPE) es una adaptación del ENPS para los juegos estocásticos y es equivalente a determinar la política óptima de un MDP[26]. El objetivo es determinar la política de estrategias óptima de un jugador, que es una función que define la estrategia óptima[27] que debe adoptar en cada estado, teniendo en cuenta las estrategias de los demás y anticipando el efecto de sus acciones en las transiciones entre estados y las utilidades futuras. La estrategia óptima de un jugador maximiza su utilidad esperada y es la mejor respuesta a las estrategias óptimas de los otros. Se pueden usar varios métodos para determinar el MPE. Un método común es por iteración de valores usando la ecuación recursiva de Bellman [37], [38]:

$$V(S) = \max_{x \in \Gamma(S)} \{F(S,x) + \beta V(T(S,x))\} \quad (2)$$

donde,

$V(S)$ es el valor de la utilidad al estado S, es decir, la utilidad esperada ;

[25] El concepto de *trembling hands* se refiere a los errores que los jugadores pueden cometer en sus elecciones de estrategias y que les hacen desviar de su estrategia de equilibrio [10].
[26] Una política óptima tiene la propiedad de que independientemente del estado inicial y de la decisión inicial, las decisiones futuras constituyen una política óptima en cuanto al estado resultante de la primera decisión [94].
[27] Es decir, estrategia MPE.

$F(S, x)$ es la utilidad obtenida al estado S adoptando la estrategia x ;

β es un factor para descontar las futuras utilidades;

$V\big(T(S, x)\big)$ es el valor de la utilidad al estado $T(S, x)$, luego de la transición del estado S al estado $T(S, x)$ adoptando la estrategia x

El objetivo de este método es converger iterativamente el valor de la utilidad en un punto fijo, alcanzado cuando ambos lados de la ecuación son iguales, y determinar la estrategia x al estado S que maximiza este valor. El punto fijo obtenido es el MPE y la estrategia x constituye la estrategia óptima de los jugadores, es decir, la política óptima del MDP [38], [25], [37]. Cuando la ecuación recursiva de la utilidad puede expresarse en forma cerrada, el MPE puede determinarse directamente optimizando la expresión cerrada.

1.4 Mapa Conceptual

La siguiente figura resume las nociones principales de la teoría de juegos:

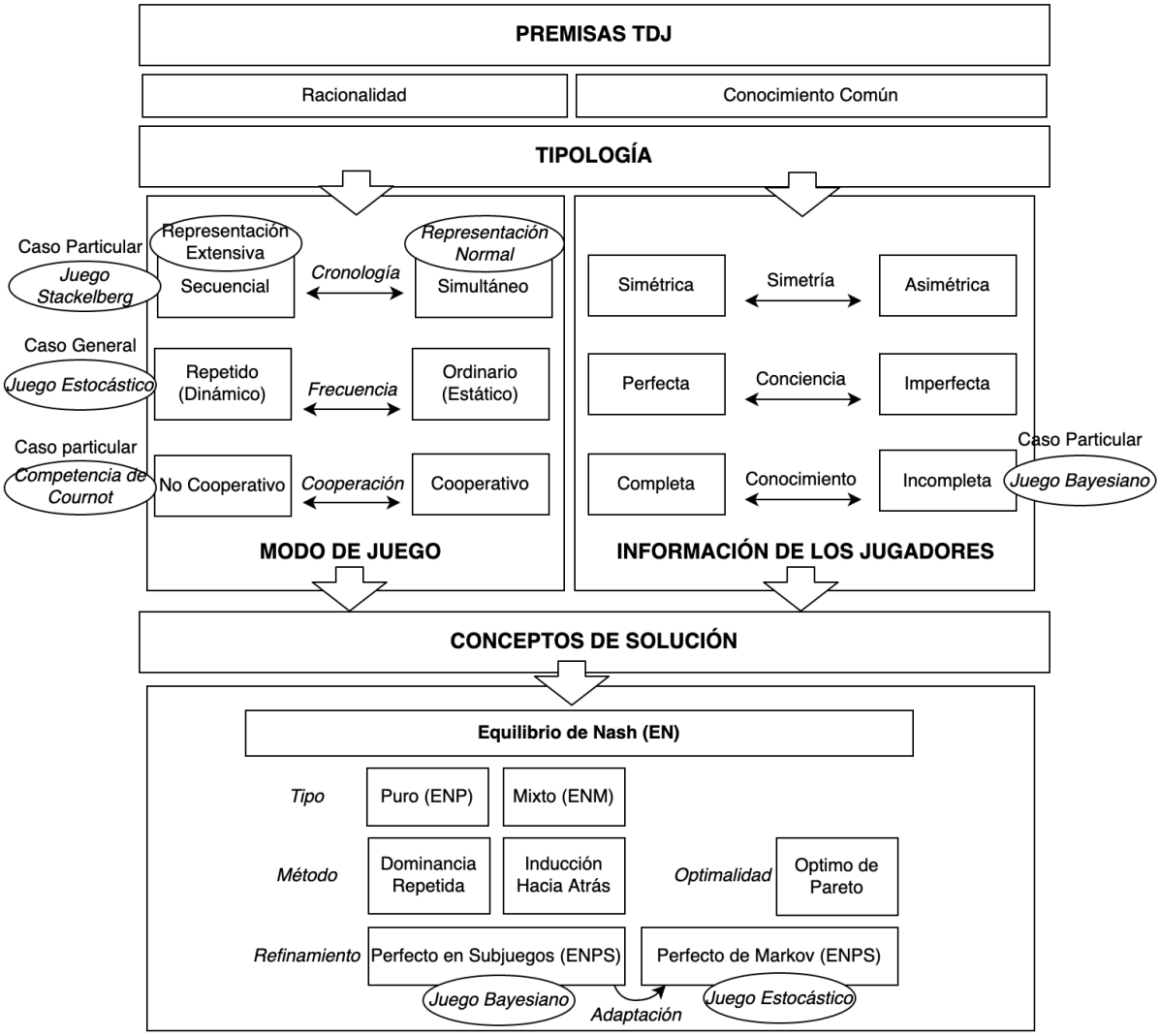


Figura 1 : Mapa conceptual de los principales conceptos de la teoría de juegos.

2 Bitcoin

En la segunda parte del trabajo, se analiza la minería de Bitcoin como un juego. La sección 2.1 explica brevemente el funcionamiento de Bitcoin y los problemas vinculados con la minería. Las secciones 2.2 y 2.3 presentan dos modelos, uno estático y otro estocástico, desarrollados en otros trabajos y aplicables a Bitcoin. La sección 2.4 les unifica y complementa para formar el modelo propuesto. Este se aplica luego en distintos subjuegos y en un protocolo de pool de minería que conforman un juego de minería óptima desarrollado en la sección 2.5. Por último, la sección 2.6 hace una prueba de concepto del modelo de juego de minería óptima y la sección 2.7 proporciona un análisis y observaciones sobre el trabajo realizado.

2.1 Funcionamiento, Minería y Problemas

Bitcoin es un sistema público de moneda digital respaldado por una red *peer-to-peer* (P2P) donde los pares, es decir, los nodos, se conectan entre sí a través de Internet. El sistema está descentralizado y sin restricciones, lo que significa que no está controlado por ninguna autoridad central y los participantes pueden conectarse y desconectarse cuando quieran. Los usuarios transfieren fondos (bitcoins) entre ellos creando transacciones que se envían a la red, donde se validan de acuerdo con ciertas reglas definidas por el protocolo de Bitcoin (Bitcoin Core) y son propagadas por los nodos que las reciben. Las transacciones válidas se agregan a una lista de espera llamada *memory pool*, y opcionalmente son seleccionadas por nodos llamados *mineros*, que los agrupan para formar bloques de transacciones. Al igual que las transacciones individuales, los bloques se validan y propagan por los pares en la red, y finalmente se agregan a una cadena de bloques que es el registro oficial de las transacciones confirmadas. Todo el proceso desde la creación de transacciones hasta sus confirmaciones constituye el mecanismo de consenso entre los pares que garantiza la seguridad del sistema sin la necesidad de una autoridad central. Para que un bloque sea válido y se agregue a la cadena, los mineros compiten para resolver primero un rompecabezas criptográfico llamado *prueba de trabajo* (PoW). La PoW se resuelve mediante prueba y error desperdiciando recursos computacionales y tiene como objetivo descentralizar el sistema al seleccionar un minero según el principio *one-CPU-one-vote* [5] para cada bloque que se agregará a la cadena.

En cuanto a los mineros, son responsables de las transacciones que se agregan a la cadena. Por lo tanto, su papel en el sistema es de primordial importancia, ya que son ellos quienes determinan quiénes son los propietarios de los fondos transferidos. Para alentarlos a adoptar un comportamiento honesto, se ofrecen incentivos económicos para la minería de cada nuevo bloque que se integra en la cadena principal: por un lado, se atribuye una recompensa fija (en bitcoins) que disminuye a la mitad cada 210,000 bloques minados [39], y por otro lado, el minero exitoso recauda los costos de transacción[28] asociados con las transacciones incluidas en los bloques minados. Los mineros pueden minar bloques como un nodo solitario o participar en un pool de minería donde combinan sus recursos computacionales con los de otros participantes para resolver la PoW. Al minar solo, es menos probable que un minero resuelva la PoW primero y entonces sus ingresos son menos constantes, sin embargo, no tiene que compartir las recompensas ganadas. En contraste, en un pool, las recompensas obtenidas son más frecuentes, pero deben compartirse entre sus miembros.

Actualmente, en la red Bitcoin, alrededor del 65% de la potencia computacional está controlada por tres pools chinos [40]. Esto socava el principio de descentralización en el que se basa la seguridad del sistema y hace que Bitcoin sea vulnerable a ataques de la mayoría del poder computacional, como el del 51% [41], que pueden ser utilizadas como palanca para alterar el historial de las transacciones. Es difícil garantizar la descentralización de los recursos computacionales de la red cuando los mineros buscan sobre todo satisfacer sus intereses personales y toman sus decisiones con el fin de maximizar sus ganancias, en función de la información a su disposición. A este respecto, falta la transparencia general de los datos relacionados con la minería ya que los participantes no tienen ningún incentivo para compartir su información. Resulta que no hay elementos suficientes para basar una decisión económica óptima. Al final, los mineros a menudo optan por el ingreso estable que ofrece un pool, y sus elecciones a menudo terminan con los mismos pools cuyos métodos de operación satisfacen mejor sus necesidades. Como resultado, la

[28] El monto de los cargos de transacción queda a discreción del creador de la transacción. Sin embargo, cuanto más altos sean los cargos, mayor será el incentivo para que un minero incluya la transacción en un bloque y la confirme.

arquitectura actual de la minería Bitcoin no basta para garantizar la descentralización y la estabilidad de la red, mientras que ningún método sólido respalda estos principios más allá de la PoW.

En este trabajo se trata de modelar la minería Bitcoin como un juego, cuya solución conduce a un equilibrio estable y descentralizado en beneficio de todos los participantes: pools, mineros y usuarios.

2.2 Modelo Estático

Esta sección presenta los resultados de otros trabajos que modelizan la minería de Bitcoin como un juego estático. Los equilibrios determinados se utilizan para desarrollar una solución más completa en las siguientes secciones.

2.2.1 Modelo

Dimitri [42] aplica la teoría de juegos para analizar el nivel de participación de un nodo en la minería. Asume que los mineros están interesados en maximizar sus utilidades[29]. Describe la competencia entre ellos como del tipo *all-pay contest*, en el que cada minero decide su estrategia (es decir, el poder computacional para invertir) y solo uno de ellos obtiene la recompensa del bloque minado y sus cargos de transacción asociados, mientras que los demás pierden su inversión. Su modelo define un juego simultáneo, estático, no cooperativo con suma no nula, información perfecta e incompleta. Un escenario similar también es evaluado por Xiong et al. [43] en un contexto de servicio de *edge computing* en soporte a una aplicación de cadena de bloques para dispositivos móviles. Establecen un modelo similar al de Dimitri [42], que llaman *Miners' Demand Game* (MDG), para representar el juego no cooperativo entre los mineros para obtener la recompensa. Chiu et Koeppl [44] también proponen un modelo estático. Los tres análisis llegan a resultados equivalentes[30] en cuanto al consumo de poder computacional óptimo para cada minero, sin embargo, el análisis de Xiong et al. [43] es más detallado al considerar más parámetros[31].

En el juego MDG, cada minero busca maximizar su utilidad, es decir, la diferencia entre las recompensas obtenidas y los costos invertidos para resolver la PoW, según la siguiente fórmula[32] [43]:

$$u_i(x_i, x_{-i}, p_i) = (R + rt_i)\frac{x_i}{\sum_{j=1}^{N} x_j} e^{-\lambda z t_i} - p_i x_i \qquad (3)$$

[29] La utilidad de un minero corresponde a sus ganancias monetarias.
[30] La Demostración 1 en el apéndice demuestra la equivalencia de las estrategias óptimas establecidas en [42], [43] y [44].
[31] Entre otros, los cargos de transacción y la probabilidad de minar un bloque huérfano [43].
[32] Específicamente, la fórmula presentada corresponde a la utilidad esperada, que el minero busca maximizar.

donde R es la recompensa de bloque, r corresponde a los cargos promedios de transacción de las t_i transacciones incluidas en el bloque de un minero i ; x_i es la estrategia, es decir el poder computacional invertido, del minero i ; x_{-i} es el poder computacional total de la red, excepto el del minero i ; $\sum_{j=1}^{N} x_j$ es el poder computacional total de la red ; $e^{-\lambda z t_i}$ es la probabilidad de que se incluya un bloque en la cadena una vez que se haya resuelto la PoW[33] ; p_i es el precio de una unidad de poder computacional, establecido por el proveedor. [43]

2.2.2 Existencia del Equilibrio de Nash

Xiong et al. [43] demuestran la existencia de un EN mediante el respeto de las siguientes condiciones: el espacio de estrategias $[\underline{x}, \overline{x}]$[34] es no vacío, convexo y es un subconjunto compacto del espacio euclidiano; u_i es continua y casi cóncava. Estas condiciones son las mismas que las del teorema 2.2 formulado en [45], que permiten concluir en la existencia de un punto fijo de acuerdo con el teorema de Glicksberg[35]. En cuanto a la última condición, el resultado negativo de la segunda derivada de la función de utilidad muestra que es estrictamente cóncava[36].

[33] Cuando dos bloques completan la PoW en un corto período de tiempo, uno de ellos se incluye en la cadena y el otro queda huérfano. La probabilidad de que un bloque minado quede huérfano está relacionada con la probabilidad de que otro complete la PoW mientras se propaga a través de la red. Si el tiempo de propagación de un bloque en la red varía linealmente en función del número de transacciones que contiene $(z \times t_i)$ y que el tiempo de generación de un nuevo bloque sigue una ley exponencial con $\mathrm{F}(x) = 1 - e^{-\lambda x}$, entonces la probabilidad de que un bloque se incluya en la cadena sin que se genere otro durante el tiempo de propagación y es igual a $e^{-\lambda z t_i}$, donde $z > 0$ es un factor de retraso de propagación [43].

[34] Tal que definido en [43], donde $\underline{x}$ es la demanda de poder computacional mínima decidida por el minero y $\overline{x}$ es la demanda máxima establecida por el proveedor. En este trabajo, $\underline{x}$ se puede establecer a cero ya que se supone que un minero puede decidir no participar en la minería.

[35] El teorema de Glicksberg es una generalización del teorema de punto fijo de Kakutani para espacios vectoriales tipológicos convexos localmente y de dimensión infinita [89]. Tal tipo de espacio se puede representar, por ejemplo, cuando se modela un juego estático repetido un número infinito de períodos, donde cada dimensión es el conjunto de estrategias de un período [88]. El teorema de Kakutani es en sí mismo una generalización para funciones con valores establecidos (*set-valued functions*, por ejemplo, una función de mejor respuesta) del teorema del punto fijo de Brouwer, lo cual demuestra la existencia de puntos fijos para funciones continúas definidas sobre subconjuntos convexos y compactos del espacio euclidiano [90].

[36] Si una función es cóncava o estrictamente cóncava, entonces también es casi cóncava [87].

2.2.3 Función de Mejor Respuesta

La función de mejor respuesta x_i^* del minero i en función de la estrategia de los demás mineros se obtiene optimizando la curva de utilidad, es decir aislando x_i cuando el resultado de la primera derivada es igual a cero, o sea cuando la pendiente de la tangente de la curva de utilidad es nula. Como la función de utilidad es estrictamente cóncava, x_i^* corresponde a un punto máximo de la curva y constituye la estrategia óptima del minero i, la que maximiza su utilidad. En el espacio $[\underline{x}, \overline{x}]$, la función de mejor respuesta de un minero i es la siguiente[37] [43]:

$$x_i^* = \sqrt{\frac{(R + rt_i)e^{-\lambda z t_i \sum_{i \neq j} x_j}}{p}} - \sum_{i \neq j} x_j \qquad (4)$$

Concretamente, la derivada de la función de utilidad define el beneficio marginal del minero[38]. Según un análisis de costo-beneficio, un minero debería aumentar su demanda de poder computacional hasta que su beneficio marginal sea cero, lo que corresponde a la estrategia óptima x_i^*. Cuando su poder computacional es inferior a x_i^*, debería aumentar su demanda ya que sus ingresos adicionales exceden sus costos marginales y entonces su utilidad aumenta. Por otro lado, a x_i^*, el beneficio marginal del minero es cero y cualquier inversión adicional lleva un ingreso marginal menor y una disminución de la utilidad. El análisis de costo-beneficio indica que solo el costo marginal de una unidad de poder computacional debe tenerse en cuenta en la demanda de recursos por un minero: costos no variables, como por ejemplo los costos fijos invertidos en la compra de equipos ASIC[39] especializados deben ser ignorados. [46]

---

[37] El resultado presentado en este trabajo corrige un error que se crea cometido en [43] en el signo de la potencia del término $e^{\lambda z t_i}$. Consultar el apéndice para la demostración del resultado obtenido.
[38] Es decir, el beneficio generado por la producción de una unidad adicional: Beneficio marginal = Ingreso marginal - Costo marginal [46].
[39] *Applicated Specific Integrated Circuit*. Tipo de equipo especializado en el cálculo de la función hash SHA-256 a una velocidad muy alta [91].

2.2.4 Unicidad del Equilibrio de Nash

Xiong et al. [43] hacen la prueba de la unicidad del ENP demostrando que la función de mejor respuesta $x_i{}^*$ del minero i en función de las estrategias de los demás posee las tres propiedades de una función estándar [47] : positividad[40], monotonía[41] y escalabilidad[42]. Dimitri [42] concluye que existe un ENP único luego de demostrar la estricta concavidad de la segunda derivada de la función de utilidad. También es posible llegar directamente a la misma conclusión al reconocer que el modelo de juego aplicado refleja una competencia de Cournot [48], lo que implica automáticamente la existencia de un ENP único llamado equilibrio de Cournot[43] : Chiu et Koeppl [44] parecen seguir este razonamiento.

2.2.5 Estrategia de Equilibrio

Al equilibrio, todos los mineros juegan la misma estrategia $x_i{}^*$ definida en (4) : se dice que el equilibrio es simétrico [44]. Del mismo modo que para determinar la estrategia óptima para un solo minero, el conjunto de equilibrio $X^* = (x_1{}^*, \dots, x_N{}^*)$ en el espacio $[\underline{x}, \overline{x}]$ se obtiene cuando el beneficio marginal de todas las estrategias es cero, con el resultado siguiente[44] [43]:

$$x_i{}^* = \frac{N-1}{\sum_{j \in N} \frac{p}{(R + rt_j)e^{-\lambda z t_j}}} - \left(\frac{N-1}{\sum_{j \in N} \frac{p}{(R + rt_j)e^{-\lambda z t_j}}} \right)^2 \frac{p}{(R + rt_i)e^{-\lambda z t_i}} \quad , \forall i \qquad (5)$$

[40] $x_i{}^*(x_{-i}) > 0$
[41] Si $x_{-i}{}' \geq x_{-i}$, entonces $x_i{}^*(x_{-i}{}') \geq x_i{}^*(x_{-i})$
[42] $\forall \alpha > 1,\ \alpha x_i{}^*(x_{-i}) > x_i{}^*(\alpha x_{-i})$
[43] La existencia y unicidad del EN en una competencia de Cournot ha sido demostrada varias veces, entre otras por Friedman (1977), Szidarovsky y Yakowitz (1977), Nishimura y Friedman (1981), Novshek (1985), Kolstad y Mathieson (1986), y Gaudet y Salan (1991) [48].
[44] Luego de corregir el error cometido en [43] (ver nota al pie 37).

2.3 Modelo Dinámico

En sus respectivos análisis, Dimitri [42] y Chiu et Koeppl [44] aplican un modelo estático para representar la competencia entre los mineros: solo hay un estado de juego permanente que resulta de la decisión simultánea de todos los mineros en cuanto al nivel de asignación de sus recursos a la minería. El equilibrio se logra cuando todos eligen la estrategia de equilibrio. De lo contrario, al menos un minero puede mejorar su utilidad cambiando unilateralmente su estrategia. En realidad, Bitcoin es una red abierta y cualquiera es libre de conectarse y desconectarse cuando quiera para participar en la minería o no, y puede cambiar la asignación de sus recursos en cualquier momento. El estado de la red y la distribución del poder computacional son por lo tanto intrínsecamente dinámicos y la aplicación de un modelo estático no considera el impacto de las interacciones estratégicas entre los jugadores y la naturaleza evolutiva de la asignación de los recursos que resultan de estas interacciones estratégicas. Dhamal et al. [38] proponen un modelo de juego estocástico más cercano a la realidad para representar la competencia de minería en un contexto dinámico de los jugadores involucrados.

En su estudio, Dhamal et al. [38] presentan un modelo estocástico general que permita el análisis de estrategias de inversión de poder computacional en un contexto de sistema distribuido. Analizan dos escenarios, el primero siendo una generalización del segundo: en el escenario 1, similar a la minería en las cadenas de bloques, se ofrece una recompensa por resolver un problema (la PoW en el caso de Bitcoin), y en el escenario 2, se ofrece una recompensa a los participantes en función de sus contribuciones individuales al poder computacional total, como por ejemplo en un sistema de cómputo voluntario[45]. En el primer escenario, los autores consideran que la tasa de resolución del problema varía en función del poder computacional actual de la red, mientras que en el segundo escenario, la tasa de resolución es fija e independiente del poder de la red.

[45] *Volunteer computing* [111].

A pesar de que el protocolo de Bitcoin ajusta la tasa de resolución de la PoW cada 2016 bloques, según el tiempo que llevó generarlos[46], y por lo tanto en función del poder computacional de la red [39], el modelo estocástico del escenario 2 de Dhamal et al. [38] se adapta mejor al contexto de Bitcoin ya que en el marco cerrado de un juego, es decir la minería de un bloque, la tasa constante de resolución de la PoW es independiente del poder total del sistema.

2.3.1 Modelo

Dhamal et al. [38] presentan un juego estocástico que termina cuando se mina exitosamente un bloque. Los jugadores (los mineros) pueden unirse a la minería y abandonarla en cualquier momento, cambiando así el estado del juego (del sistema) y las estrategias (asignación de recursos) adoptadas por los mineros. Específicamente, un estado del juego corresponde a un conjunto de mineros presentes en el sistema. Al igual que el modelo estático, estos buscan maximizar sus utilidades, es decir sus beneficios, y modifican sus estrategias según el estado del sistema y las estrategias de los demás. A diferencia del modelo estático, el modelo estocástico considera la posibilidad de que el sistema cambie de estado y de que no se gane la recompensa en el estado actual con el conjunto actual de estrategias de los mineros presentes en el sistema. La transición entre los estados es probabilística y continua en el tiempo. En cada transición, los mineros reevalúan sus estrategias y se define un nuevo conjunto de las mismas para el estado siguiente. Se definen dos transiciones de estados: pasar del estado S al estado S' cuando se agrega un minero en el sistema, o pasar del estado S al estado S'' cuando se retira uno. La utilidad esperada de un minero en el estado S es una ponderación de su utilidad esperada si la recompensa se consigue en el estado actual antes de cualquier transición, su utilidad esperada si el sistema pasa al estado S' y su utilidad esperada si el sistema pasa al estado S''. Cuando ocurre una transición, el nuevo estado se convierte en el actual, es decir S, y la utilidad esperada se vuelve a evaluar de la misma manera. Por lo tanto, la función es recursiva y la utilidad esperada de un minero i en el estado S

[46] Bitcoin ajusta la tasa de resolución de la PoW cada 2016 bloques (que corresponde a un tiempo de resolución teórico de dos semanas) para lograr un tiempo promedio de generación de bloques nuevos de diez minutos: $Nueva\ difficultad = Difficultad\ antigua \times \frac{tiempo\ últimos\ 2016\ bloques}{20160\ minutos}$ [39]. El nivel de dificultad es un número de 256 bits en un formato compacto [98].

para un conjunto de estrategias x se puede expresar en la siguiente forma simplificada:

$$R_i^{(S,x)} = Pr(r^S) \cdot R_i^{(S,x|r^S)} + Pr(S') \cdot R_i^{(S',x)} + Pr(S'') \cdot R_i^{(S'',x)} \quad (6)$$

donde,

$Pr(r^S) + Pr(S') + Pr(S'') = 1$;

$Pr(r^S)$ es la probabilidad de que la recompensa se atribuya al estado S;

$R_i^{(S,x|r^S)}$ es la utilidad esperada sabiendo que la recompensa se atribuye al estado S;

$Pr(S')$ es la probabilidad de que se agregue un minero y que el sistema transite al estado S' antes de que transite al estado S'' y antes de que se atribuya la recompensa al estado S;

$R_i^{(S',x)}$ es la utilidad esperada al estado S';

$Pr(S'')$ es la probabilidad de que un minero se vaya y que el sistema transite al estado S'' antes de que transite al estado S' y antes de que se atribuya la recompensa al estado S;

$R_i^{(S'',x)}$ es la utilidad esperada al estado S''.

La expresión general (6) destaca que el modelo estocástico es una generalización del modelo estático definido previamente: la utilidad esperada del modelo estático es equivalente al término $R_i^{(S,x|r^S)}$ en el modelo estocástico, es decir a la utilidad esperada sabiendo que la recompensa se atribuye al estado S. Por lo tanto, el modelo estático define solo un estado del sistema. Este es un caso especial del modelo estocástico de Dhamal et al. [38], en el que las tasas de llegada y salida de mineros son cero.

Al integrar los parámetros definidos por Dhamal et al. [38] en la expresión general (6), se obtiene la siguiente fórmula para determinar la utilidad esperada de un minero i al estado S según el conjunto de estrategias x:

$$R_i^{(S,x)} = \frac{\beta}{D^{(S,x)}} \cdot \frac{x_i^{(S)}}{\sum_{j \in S} x_j^{(S)} + l} \cdot r - \frac{c_i x_i{}^{(S)}}{D^{(S,x)}} + \sum_{j \notin S} \frac{\lambda_j}{D^{(S,x)}} \cdot R_i^{(S \cup \{j\},x)} + \sum_{j \in S} \frac{\mu_j}{D^{(S,x)}} \cdot R_i^{(S \setminus \{j\},x)} \quad (7)$$

donde los parámetros se definen en la siguiente tabla:

General (6)	Dhamal et al. (7)	Parámetros	Descripción
$Pr(r^S)$	$\frac{\beta}{D^{(S,x)}}$	β	Tasa constante de resolución de la PoW
		$D^{(S,x)}$	$\beta + \sum_{j \notin S} \lambda_j + \sum_{j \in S} \mu_j$
$R_i^{(S,x \mid r^S)}$	$\frac{x_i^{(S)}}{\sum_{j \in S} x_j^{(S)} + l} \cdot r - \frac{c_i x_i{}^{(S)}}{D^{(S,x)}}$	$x_i^{(S)}$	Poder computacional del minero i al estado S
		l	Poder computacional fijo del sistema, es decir de los mineros no estratégicos
		r	Monto de la recompensa
		c_i	Costo de una unidad de poder computacional por unidad de tiempo para el minero i
$Pr(S')$	$\sum_{j \notin S} \frac{\lambda_j}{D^{(S,x)}}$	λ_j	Tasa de llegada en el sistema del minero j por unidad de tiempo
$R_i^{(S',x)}$	$R_i^{(S \cup \{j\},x)}$	$R_i^{(S \cup \{j\},x)}$	Utilidad esperada del minero i al estado S' según el conjunto de estrategias x
$Pr(S'')$	$\sum_{j \in S} \frac{\mu_j}{D^{(S,x)}}$	μ_j	Tasa de salida del sistema del minero j por unidad de tiempo
$R_i^{(S'',x)}$	$R_i^{(S \setminus \{j\},x)}$	$R_i^{(S \setminus \{j\},x)}$	Utilidad esperada del minero i el estado S'' según el conjunto de estrategias x

Tabla 1: Notación de los parámetros del modelo estocástico de Dhamal et al. [38]

También definimos U como el conjunto universal de jugadores estratégicos y designamos $j \notin S$ el conjunto de jugadores estratégicos que no son parte del estado S. β es el parámetro de la ley exponencial que define el tiempo de resolución de la PoW, y entonces $1/\beta$ corresponde al tiempo promedio de generación de bloque. Bitcoin establece el nivel de dificultad para obtener un tiempo promedio de diez minutos[47]. Los tiempos de llegada y salida en el sistema de un minero j también siguen leyes exponenciales con parámetros λ_j y μ_j respectivamente. Por lo tanto, el tiempo mínimo requerido para resolver la PoW o transitar de estado sigue una ley exponencial

[47] Ver nota al pie 46.

de parámetro $D^{(S,x)}$ igual a la suma de los parámetros de cada una de las leyes exponenciales, o sea $\beta + \sum_{j \notin S} \lambda_j + \sum_{j \in S} \mu_j$, y $1/D^{(S,x)}$ corresponde al tiempo promedio de permanencia en el estado S. Estas variables se modelizan con la ley exponencial para su propiedad sin memoria que estipula que el tiempo requerido para encontrar una solución en un espacio de búsqueda suficientemente grande es independiente del espacio ya explorado. Por lo tanto, la probabilidad de resolver la PoW o transitar de estado es independiente del tiempo transcurrido y es proporcional a su respectiva tasa de ocurrencia.

2.3.2 Existencia y Unicidad del MPE.

Como primer paso, Dhamal et al. [38] demuestran la convergencia de la función de utilidad (7) para todos los estados y para cualquier conjunto de estrategias x con el fin de poder derivar una expresión cerrada para evaluar el MPE. Para hacer esto, se construye el vector R_i^x compuesto de las utilidades esperadas $R_i^{(S,x)}$ (7) en todos los estados para un conjunto x dado. Se demuestra iterativamente que el vector R_i^x converge y puede expresarse como una expresión cerrada cuando el número de iteraciones tiende al infinito[48]. La convergencia es intuitiva: dado que la probabilidad de transitar de estado es positiva y menor que 1, es decir subestocástica, la probabilidad de que se gane la recompensa después de t transiciones disminuye cuando t aumenta, y tiende a 0 cuando $t \to \infty$. En consecuencia, la utilidad esperada sigue la misma tendencia. Como el vector R_i^x converge, sus componentes también convergen: por lo tanto, la función de utilidad esperada (7) converge para todos los estados y para cualquier conjunto de estrategias x. Por consiguiente, un punto fijo se puede evaluar directamente optimizando la función cerrada[49] obtenida siguiente [38]:

$$\lim_{t \to \infty} R_{i(t)}^{(x)} = \left(I - W^{(x)}\right)^{-1} Z_i^{(x)} \tag{8}$$

donde,

[48] La demostración es como la realizada en [101], de la convergencia de una serie geométrica cuando el número de términos tiende al infinito y que el factor de descuento está entre -1 y 1.
[49] De lo contrario, si la función está abierta, se puede evaluar un punto fijo aplicando el método por iteraciones de valores con la ecuación de Bellman (voir section 1.3.6). [38]

$\lim_{t\to\infty} R_{i(t)}^{(x)}$ es el vector de las utilidades esperadas en todos los estados para un jugador i y para un conjunto de estrategias x;

I es la matriz identidad[50];

$W^{(x)}$ es la matriz de transición de estados compuesta por las probabilidades de pasar a los estados S' y S'' y de 0 en otra parte;

$Z_i^{(x)}$ es el vector de las utilidades esperadas de todos los estados, proveniente solo de ganancias en el estado actual S.

Además, alcanzar un estado absorbente[51] está asegurado ya que la probabilidad de resolución de la PoW es estrictamente positiva. Bajo esta condición, se demuestra que la función de utilidad óptima está limitada y constituye el punto fijo único de la ecuación de Bellman. [38]

2.3.3 Función de Mejor Respuesta

La función de mejor respuesta para un jugador i se obtiene optimizando la expresión cerrada de la utilidad esperada para todos los estados (8). Como I y $W^{(x)}$ son independientes del conjunto de estrategias x y que todos los elementos de $\left(I - W^{(x)}\right)^{-1}$ son no negativos[52], la maximización del vector $Z_i^{(x)}$ también maximiza $R_i^{(x)}$. Al reorganizar la expresión formulada por Dhamal et al. [38] para demostrar la equivalencia con (7), pero manteniendo los parámetros definidos en [38], se obtiene la siguiente expresión para $Z_i^{(x)}$, o de manera equivalente, para cada uno de sus elementos $Z_i^{(S,x)}$ [38]:

$$Z_i^{(S,x)} = \frac{\beta}{D^{(S,x)}} \cdot \frac{x_i^{(S)}}{\sum_{j\in S} x_j^{(S)} + l} \cdot r - \frac{c_i x_i^{(S)}}{D^{(S,x)}} \tag{9}$$

[50] Matriz cuadrada compuesta de 1's en la diagonal principal y de 0's en el resto [97].

[51] Estado del que no se sale [95], es decir, estado en el que se mina el bloque y se termina el juego.

[52] La matriz de transición $W^{(x)}$ es estrictamente subestocástica, es decir, la suma de los valores de cada fila es menor que 1 y todos sus elementos son no negativos ya que establecen las probabilidades de transición a otro estado. [38]

$Z_i^{(S,x)}$ equivale a los términos $Pr(r^S) \cdot R_i^{(S,x|r^S)}$ de la expresión general (6), es decir al producto de la probabilidad de que la recompensa se atribuya al estado actual S y de la utilidad esperada sabiendo que la recompensa se atribuye a S. $D^{(S,x)}$ siendo independiente de $x_i^{(S)}$, se vuelve a optimizar una función de la misma forma que la función de utilidad del modelo estático (3). El resultado negativo de la segunda derivada[53] de $Z_i^{(S,x)}$ demuestra que la función es estrictamente cóncava. La optimización de $Z_i^{(S,x)}$ a partir de la primera derivada determina entonces el punto máximo de la función, o sea el MPE. Aplicando la condición de la primera derivada $\frac{\partial Z_i^{(S,x)}}{\partial x_i^{(S)}} = 0$, Dhamal et al. [38] obtienen el siguiente resultado en el espacio de estrategias $[0, \infty[$:

$$x_i^{(S)^*} = \max\left\{\psi^{(S)}\left(1 - \frac{\psi^{(S)}}{r\beta}c_i\right), 0\right\} \tag{10}$$

donde $\psi^{(S)} = \sum_{j\in S} x_j^{(S)} = \sum_{j\in S} x_{i\neq j}^{(S)} + x_i^{(S)^*}$

Este resultado es equivalente al calculado para el modelo estático[54]. La estrategia óptima de un minero i al estado S se obtiene aislando $x_i^{(S)^*}$ a la izquierda de la igualdad, con el siguiente resultado[55] :

$$x_i^{(S)^*} = \sqrt{\frac{r\beta \sum_{j\in S} x_{i\neq j}^{(S)} + l}{c_i}} - \left(\sum_{j\in S} x_{i\neq j}^{(S)} + l\right) \tag{11}$$

[53] $\frac{-2rl\beta}{\left(\sum_{j\in S} x_j^{(S)} + l\right)^3 D^{(S,x)}}$ [38].

[54] Demostración 2 en el apéndice.

[55] Demostración 2 en el apéndice.

2.3.4 Estrategia de Equilibrio

El MPE es simétrico, es decir que al equilibrio, todos los mineros juegan la misma estrategia definida por la ecuación (11) [44]. El equilibrio se alcanza cuando la utilidad esperada de todos los jugadores se maximiza, entonces cuando $\frac{\partial \sum_i Z_i^{(S,x)}}{\partial x_i^{(S)}} = 0$. Se suma $Z_i^{(S,x)}$ para todos los mineros y se determina la estrategia óptima $x_i{}^*$ que respeta la condición de la primera derivada. Se obtiene el conjunto de estrategias de equilibrio $X^{(S)^*} = \left(x_1^{(S)^*}, \dots, x_{|\hat{S}|}^{(S)^*}\right)$ en el espacio $[0, \infty[$, donde $x_i^{(S)^*}$ está determinado por la siguiente expresión [38]:

$$x_i^{(S)^*} = \max\left\{\psi^{(S)}\left(1 - \frac{\psi^{(S)}}{r\beta}c_i\right), 0\right\} \quad , \forall i \tag{12}$$

done $\psi^{(S)} = r\beta \frac{|\hat{S}|-1+\sqrt{(|\hat{S}|-1)^2+\frac{4l}{r\beta}\sum_{j\in\hat{S}} c_j}}{2\sum_{j\in\hat{S}} c_j}$

Este resultado coincide con el del modelo estático[56]. Se representa por $\hat{S}$ el conjunto de mineros estratégicos presentes en el sistema al estado S que invierten un poder computacional positivo, es decir $x_i^{(S)} > 0$, y por $|\hat{S}|$ el número de mineros que componen $\hat{S}$.

[56] Demostración 3 en el apéndice.

2.4 Modelo Propuesto

Usamos como base el modelo estocástico de Dhamal et al. [38], al que integramos parámetros del modelo estático de Xiong et al. [43], o sea los cargos de transacciones (θt_i) y la probabilidad de que un bloque minado se incluya en la cadena ($e^{-\beta z_i t_i}$). También agregamos un componente importante: un factor k de eficiencia energética para modelizar adecuadamente la probabilidad de ganar la recompensa, que está vinculada con la cantidad de soluciones probadas para la PoW en vez del nivel de recursos consumidos. El valor de k está relacionado con el tipo de equipo utilizado y puede derivarse de las características del producto[57]. Finalmente, desglosamos el valor de la recompensa al incluir una tasa de conversión de moneda τ para aislar el impacto del valor de la moneda Bitcoin en la minería. Justo como en el modelo de Dhamal et al. [38], definimos U como el conjunto universal de jugadores estratégicos, estén o no presentes en el sistema. Los cambios en el modelo de Dhamal et al. [38] no tienen impacto en la existencia y unicidad del MPE y la demostración realizada en la sección 2.3.2 sigue siendo válida. Por lo tanto, presentamos directamente la función de utilidad y la estrategia de equilibrio útiles para el resto del trabajo.

2.4.1 Función de Utilidad

La utilidad esperada para un jugador i en el estado S que adopta la estrategia x puede expresarse mediante la siguiente fórmula:

$$R_i^{(S,x)} = \frac{\beta}{D^{(S,x)}} \frac{k_i x_i^{(S)}}{\sum_{j \in S} k_j x_j^{(S)} + k_l l} \tau (r + \theta t_i) e^{-\beta z_i t_i} - \frac{c_i x_i^{(S)}}{D^{(S,x)}} + \sum_{j \notin S} \frac{\lambda_j}{D^{(S,x)}} R_i^{(S \cup \{j\}, x)} + \sum_{j \in S} \frac{\mu_j}{D^{(S,x)}} R_i^{(S \setminus \{j\}, x)} \quad (13)$$

2.4.2 Estrategia de Equilibrio

La estrategia de equilibrio del modelo propuesto para un jugador i en el estado S en el espacio estratégico $[0, \infty[$ es la siguiente[58] :

[57] Por ejemplo, la eficiencia energética de un Antminer S17+ es de 1/40 TH/J [99]. El criterio a respetar es la importancia relativa de los factores k_i entre los mineros y no el orden de valores de k_i.
[58] Demostración 4 en el apéndice.

$$x_i^{(S)^*} = \max\left\{ \psi^{(S)} \left(\frac{1}{k_i} - \frac{\psi^{(S)}}{{k_i}^2 \beta\tau(r+\theta t_i) e^{-\beta z_i t_i}} c_i \right), 0 \right\} \quad , \forall i \tag{14}$$

donde $\psi^{(S)} = \frac{|\hat{S}|-1+\sqrt{(|\hat{S}|-1)^2+\frac{4k_l l}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j(r+\theta t_j)e^{-\beta z_j t_j}}}}{\frac{2}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j(r+\theta t_j)e^{-\beta z_j t_j}}}$

2.4.3 Participación en la Minería

Basándose en la ecuación (14), un jugador no invertirá ningún poder computacional si $\frac{\psi^{(S)}}{{k_i}^2 \beta\tau(r+\theta t_i) e^{-\beta z_i t_i}} c_i \geq \frac{1}{k_i}$. Para participar en la minería, tenemos entonces la condición $\frac{\psi^{(S)}}{{k_i}^2 \beta\tau(r+\theta t_i) e^{-\beta z_i t_i}} c_i < \frac{1}{k_i}$ o de manera equivalente $c_i < \frac{k_i \beta\tau(r+\theta t_i) e^{-\beta z_i t_i}}{\psi^{(S)}}$. Al sustituir $\psi^{(S)}$, obtenemos:

$$c_i < \frac{k_i(r+\theta t_i)e^{-\beta z_i t_i} \cdot 2\sum_{j\in\hat{S}} \frac{c_j}{k_j(r+\theta t_j)e^{-\beta z_j t_j}}}{|\hat{S}| - 1 + \sqrt{\left(|\hat{S}|-1\right)^2 + \frac{4k_l l}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j(r+\theta t_j)e^{-\beta z_j t_j}}}} \tag{15}$$

Por lo tanto, hay un umbral máximo para el costo de los recursos que depende de varios parámetros y más allá del cual un jugador no minará. Es interesante notar que cuando todos los jugadores son estratégicos ($l = 0$), la recompensa es positiva y fija ($\theta = 0$) y que todos los bloques minados están incluidos en la cadena ($e^{-\beta z_i t_i} = 1$), obtenemos:

$$\frac{c_i}{k_i} < \frac{\sum_{j\in\hat{S}}(c_j/k_j)}{|\hat{S}| - 1} \tag{16}$$

Aunque la ecuación (14) determina que el poder computacional óptimo depende del valor de la recompensa, en este caso particular, la decisión de minar

depende solo de la ratio costo marginal – eficiencia energética (c_i/k_i) del jugador en comparación con la de los demás jugadores.

Sin embargo, para el resto del trabajo, en el subjuego de los pools en la sección 2.5.2 y en el contexto actual de Bitcoin, estas condiciones no se cumplen: la recompensa incluye cargos de transacción variables, la propagación de los bloques sufre un retraso, y una parte del poder de la red es necesariamente generada por mineros solitarios o pools de mineros que no tienen la capacidad suficiente para jugar la estrategia de equilibrio, es decir que $l > 0$. También, en el juego de protocolo en la sección 2.5.3.2, la capacidad computacional limitada de algunos mineros les impide poder adoptar la estrategia de equilibrio. Por lo tanto, estos no se consideran estratégicos y su poder computacional se suma en la parte fija l.

2.5 Juego de Minería Óptima

Esta sección modeliza un juego para determinar y distribuir el poder computacional de la red Bitcoin entre los pools y los mineros. La sección 2.5.1 modeliza un juego Stackelberg de minería óptima cuya solución global se deriva en parte del modelo propuesto en la sección anterior. Las secciones 2.5.2 et 2.5.4 describen los dos niveles del juego: el subjuego de los pools y el dilema de los mineros. En la sección 2.5.3, un protocolo de pool que dicta las reglas dentro de este se desarrolla y se integra en el modelo con el objetivo de proporcionar los incentivos necesarios para que los jugadores adopten la estrategia de equilibrio, lo alcancen, y favorezcan la estabilidad así como la descentralización de la red Bitcoin.

2.5.1 Modelo

El juego de minería óptima es un juego Stackelberg con dos niveles: en el primer nivel (*subjuego de los pools*), los pools son los líderes que trabajan juntos para determinar el poder computacional óptimo que cada uno debe generar y, en el segundo nivel (*dilema de los mineros*), los mineros son los seguidores que deciden sobre su participación en un pool y su inversión de poder computacional. El primero es un juego cooperativo, simultáneo, con información perfecta e incompleta, en el que los pools colaboran entre sí compartiendo la información necesaria para determinar el poder computacional óptimo que cada uno de ellos debe generar para lograr el equilibrio y maximizar su utilidad. La información compartida es el resultado de la cooperación de los mineros: al registrarse en un pool, se comprometen a compartir su costo marginal, su capacidad máxima de cálculo y su eficiencia energética, para el bien común de todos.

Luego, cada pool distribuye entre sus miembros el trabajo computacional óptimo que necesita generar en función de la información compartida y para maximizar la utilidad de cada uno. Asigna a cada minero un nivel de recursos para consumir, que representa un curso de acción en lugar de una obligación, ya que no se puede imponer. Cuando el pool gana una recompensa, se reparte entre los mineros en función del resultado de un juego simulado (*juego de protocolo*). Este último, la distribución del trabajo computacional y la repartición de la recompensa son

componentes del protocolo que gobierna las reglas del juego entre un pool y sus mineros.

El dilema de los mineros es un juego no cooperativo entre los mineros de la red Bitcoin, simultáneo, con información perfecta e incompleta, en el que ellos deciden su participación en un pool y eligen su nivel de inversión computacional.

La siguiente figura muestra el juego de minería óptima, un juego Stackelberg de dos niveles que incluye el protocolo de pool que establece las reglas del juego entre los mineros y el pool.

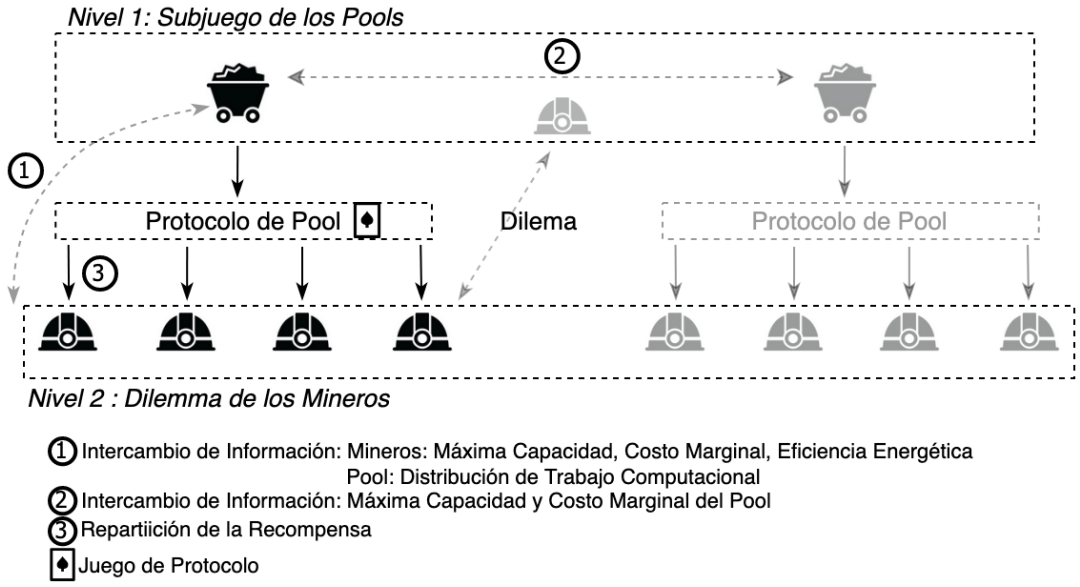


Figura 2 : Diagrama del modelo de juego de minería óptima.

2.5.2 Subjuego de los Pools

El subjuego de los pools es la competencia en la que estos compiten entre sí por la recompensa asociada con la minería de un bloque que se agrega a la cadena principal. La solución del subjuego conduce a un equilibrio dado por el modelo propuesto en la sección 2.4.

Función de Utilidad

En la ecuación (13), fijamos $\lambda_j = \mu_j = 0$ ya que los pools se consideran siempre presentes en el sistema. Por lo tanto, obtenemos un modelo estático con la siguiente ecuación simplificada para determinar la utilidad esperada de un pool p_i en el estado S con el conjunto de estrategias x :

$$R_{p_i}^{x} = \beta \cdot \frac{k_{p_i} x_{p_i}}{\sum_{j \in S} k_{p_j} x_{p_j} + k_l l} \cdot \tau\left(r + \theta t_{p_i}\right) e^{-\beta z_{p_i} t_{p_i}} - \frac{c_{p_i} x_{p_i}}{\beta} \qquad (17)$$

donde S es el conjunto de pools presentes en el sistema con recursos suficientes para jugar la estrategia óptima; l es la potencia de cálculo residual en la red que no es generada por S ; k_{p_i} es la eficiencia energética del pool p_i y corresponde a un promedio de las eficiencias energéticas de sus miembros ponderadas por sus niveles de contribución a la estrategia óptima[59] ; c_{p_i} es el costo marginal del pool p_i y es un promedio de los costos marginales de sus miembros ponderados por sus niveles de contribución a la estrategia óptima; θ corresponde a los cargos promedios por transacción de las t_{p_i} transacciones incluidas en un bloque del pool p_i; z_{p_i} es el factor de retraso de propagación de un bloque del pool p_i en la red.

Estrategia de Equilibrio

La estrategia de equilibrio es la del modelo propuesto (14) con los parámetros correspondientes del subjuego, donde $\hat{S}$ es el conjunto de los pools que invierten un poder computacional positivo.

[59] Los costos marginales y la eficiencia energética de los pools influyen en sus estrategias óptimas. Una estrategia óptima definida puede hacer que un pool revise su costo marginal y la estimación de eficiencia energética para alcanzarlo. La colaboración entre los pools permite un cálculo iterativo para determinar sus costos marginales, sus eficiencias energéticas y sus estrategias óptimas.

Participación a la Minería

Todos los pools invierten un poder computacional positivo suponiendo una distribución relativamente uniforme de los mineros con distintos costos marginales y eficiencias energéticas entre los distintos pools. Por lo tanto, definimos sin distinción $\hat{S} = S = U$.

2.5.3 Protocolo de Pool

Los pools de minería utilizan protocolos especializados que definen sus métodos de operación. Entre las reglas importantes que se establecen están las relativas a la distribución del trabajo computacional entre los mineros [49] y el método de repartición de las recompensas ganadas entre ellos[60]. En esta sección, proponemos un esquema de protocolo orientado al uso óptimo de los recursos computacionales de los mineros. Este es un ejemplo de aplicación del modelo propuesto en la sección 2.4 del que se pueden desarrollar múltiples variaciones. Definimos tres componentes del protocolo: la distribución del trabajo computacional, el juego de protocolo y la repartición de la recompensa.

2.5.3.1 Distribución del Trabajo Computacional

El pool asigna a cada uno de los mineros un nivel de recursos computacionales para consumir según su ratio c_i/k_i. Para maximizar la utilidad del pool, la distribución del trabajo computacional se realiza en orden creciente de ratios c_i/k_i e igualmente entre los mineros, de acuerdo con la capacidad máxima de cada uno y hasta que se alcance la estrategia de equilibrio del pool.

2.5.3.2 Juego de Protocolo

Este componente del protocolo simula una competencia entre los mineros del pool por la recompensa ganada por este. La solución del juego simulado conduce a un equilibrio dado por el modelo propuesto en la sección 2.4 y se usa para determinar la fracción de la recompensa obtenida que se otorgará a cada minero.

---

[60] Por ejemplo, *Pay-Per-Share (PPS), Pay-Per-Last-N-Shares (PPLNS), Proportional, Geometric Method*. [100]

Función de Utilidad

Ponemos en cero los parámetros θ, t_i y z_i en la ecuación (13) dado que la propagación del bloque minado tiene lugar en el subjuego de los pools y que solo la cabecera del bloque se transmite a los mineros por el pool para que logren la PoW. Por lo tanto, obtenemos la siguiente ecuación simplificada para la utilidad esperada simulada de un minero i al estado S según el conjunto de estrategias x:

$$R_{sim_i}^{(S,x)} = \frac{\beta}{D^{(S,x)}} \cdot \frac{k_i x_i^{(S)}}{\sum_{j \in S} k_j x_j^{(S)} + k_l l} \cdot \tau r - \frac{c_i x_i{}^{(S)}}{D^{(S,x)}} + \sum_{j \notin S} \frac{\lambda_j}{D^{(S,x)}} \cdot R_{sim_i}^{(S \cup \{j\},x)} + \sum_{j \in S} \frac{\mu_j}{D^{(S,x)}} \cdot R_{sim_i}^{(S \setminus \{j\},x)} \quad (18)$$

donde S es el conjunto de los mineros registrados en el pool que tienen recursos suficientes para jugar la estrategia óptima; k_i es la eficiencia energética del minero i; l es el poder computacional generado por los mineros del pool que no forman parte de S; λ_j y μ_j refieren a las tasas de llegada y salida en el sistema de los mineros del pool; c_i es el costo marginal del minero i en el pool.

Estrategia de Equilibrio

La estrategia de equilibrio simulada es la del modelo propuesto (14), donde $\hat{S}$ es el conjunto de los mineros del pool que invierten un poder computacional positivo. Al establecer en cero los parámetros θ, t_i y z_i, obtenemos la siguiente ecuación simplificada:

$$x_{sim_i}^{(S)^*} = \max\left\{ \psi^{(S)} \left(\frac{1}{k_i} - \frac{\psi^{(S)}}{k_i{}^2 \beta \tau r} c_i \right), 0 \right\} \quad , \forall i \quad (19)$$

donde $\psi^{(S)} = \frac{|\hat{S}| - 1 + \sqrt{(|\hat{S}|-1)^2 + \frac{4k_l l}{\beta \tau r} \sum_{j \in \hat{S}} \frac{c_j}{k_j}}}{\frac{2}{\beta \tau r} \sum_{j \in \hat{S}} \frac{c_j}{k_j}}$

Participación a la Minería

El conjunto $\hat{S}$ de los mineros que invierten un poder computacional positivo se puede determinar iterativamente por el pool integrándolos de manera gradual en el conjunto, en orden creciente de ratio c_i/k_i, hasta que no se cumpla la condición de la ecuación (15) [38].

2.5.3.3 Repartición de la Recompensa

La recompensa obtenida por el pool se distribuye entre los mineros de acuerdo con el costo de sus recursos consumidos y en proporción al rendimiento relativo óptimo que habrían tenido si hubieran participado en una competencia intra-pool para su obtención, tal que modelizada por el juego de protocolo. La fracción de la recompensa atribuida a un minero corresponde a la proporción de su recompensa esperada ($E[r]_i^{x_i}$) sobre la recompensa esperada del pool ($E[r]_p^{x_p^*}$). En cada caso, la recompensa esperada corresponde a la utilidad esperada menos los costos esperados. Dentro de un pool, obtenemos entonces la siguiente fórmula para determinar la tasa α_i de la recompensa atribuida al minero i:

$$\alpha_i = \frac{E[r]_i^{x_i}}{E[r]_p^{x_p^*}} = \frac{\mathbb{I}_i \cdot R_p^{x_p^*} + \frac{c_i x_i}{\beta}}{R_p^{x_p^*} + \frac{c_p x_p^*}{\beta}} \tag{20}$$

donde $\mathbb{I}_i = \frac{I_i^C \cdot I_i^{ROI}}{\sum_{j \in p} I_j^C \cdot I_j^{ROI}}$

I_i^C es el índice relativo[61] del costo de los recursos consumidos por el minero i; I_i^{ROI} es el índice relativo de la tasa de rendimiento (ROI)[62] esperada del minero i; p es el conjunto de los mineros del pool presentes en el sistema; $R_p^{x_p}$ es la utilidad esperada del pool calculada en el subjuego de los pools; x_i es el nivel de recursos asignado al

[61] En general, el índice relativo de un parámetro para una clase es el ratio del valor del parámetro para ella sobre el de la clase de referencia. Por lo tanto, la clase de referencia tiene un índice relativo igual a uno. Por ejemplo, si tomamos como clase de referencia el minero k, el índice relativo de costo I_i^C del minero i es igual al ratio de los costos del minero i sobre los costos del minero k.

[62] $ROI = Utilidad\ esperada / Costos\ esperados$ [106].

minero i por el pool; x_p^* es la estrategia de equilibrio del pool. Los índices relativos de ROI se calculan a partir de las utilidades esperadas de los mineros en el juego de protocolo (18) cuando adoptan su estrategia óptima.

Los índices de costos relativos se utilizan para repartir equitativamente la recompensa ganada entre los mineros, considerando que no todos invierten los mismos recursos dado el método de distribución del trabajo computacional. En cuanto a los índices relativos de ROI, permiten a los mineros obtener una tasa de rendimiento óptima relativamente a la de los demás en el pool. Este método determinista para repartir la recompensa, basado en un juego simulado, evita una competencia real entre los mineros y la consiguiente reducción de sus utilidades esperadas.

Juntos, los métodos para distribuir el trabajo computacional y repartir la recompensa hacen posible minimizar el costo de la estrategia óptima del pool y maximizar su utilidad esperada al asignar primero los recursos para consumir a los mineros más eficientes, es decir aquellos con ratios c_i/k_i más bajos, sin afectar la tasa de rendimiento óptima relativa de los mineros.

2.5.4 Dilema de los Mineros

Este subjuego forma el segundo nivel del juego Stackelberg de minería óptima. La estrategia de un minero es dividir sus recursos entre distintos pools o minar en solitario. Esto constituye un *dilema social* en el que deben elegir entre sus intereses individuales y el interés colectivo de todos los mineros.

Establecimiento del Dilema Social

Sobre la base de evaluación de un solo bloque minado, la utilidad esperada de un minero i que adopta una estrategia x corresponde a la suma de sus utilidades esperadas en los pools y de su utilidad esperada como minero solitario, y puede expresarse mediante la siguiente fórmula:

$$R_i^x = \sum_{j \in S} \left(\mathbb{I}_{i,p_j} \cdot R_{p_j}^{x_{p_j}} \right) + R_i^x \tag{21}$$

donde $\mathbb{I}_{i,p_j}$ es la tasa de los índices relativos del minero i del pool p_j, tal que definido en la sección 2.5.3.3; $R_{p_j}^{x_{p_j}}$ es la utilidad esperada (17) del pool p_j que adopta la estrategia x_{p_j} al estado S en el subjuego de los pools; R_i^x es la utilidad esperada del minero i que adopta la estrategia x al estado S como nodo solitario en el subjuego de los pools. R_i^x está determinado por la ecuación (17), en la que el minero es parte del conjunto S si tiene suficientes recursos para jugar la estrategia de equilibrio, o de l en el caso contrario.

Para un pool dado y siempre en la evaluación de una sola iteración del juego, es decir de un bloque minado, un minero minará en solitario si su utilidad esperada es mayor que la del pool ($R_i^x > \mathbb{I}_{i,p} \cdot R_p^{x_p}$). Sin embargo, debido a la estructura establecida por el juego de minería óptima, esta condición siempre se cumple y no es suficiente para que el minero tome una decisión estratégica que maximiza su utilidad sobre varias iteraciones del juego. El modelo cooperativo del subjuego de los pools resulta de alianzas que permiten el análisis mediante la evaluación de las acciones de los pools en lugar de las acciones individuales de los mineros, que pueden tener preferencias individuales divergentes de las de la coalición. En el dilema de los mineros, esta divergencia de preferencias está en el corazón de la elección estratégica del minero. La consecuencia directa de la formación de alianzas es reducir el número de jugadores en el subjuego de los pools y aumentar la utilidad esperada de cada uno al reducir el nivel de competencia. Cuando todos los mineros cooperan participando en un pool, la utilidad de cada uno de ellos es mayor que la de un escenario no cooperativo. Sin embargo, uno que deserta para minar en solitario aumenta su utilidad esperada al beneficiarse de la competencia reducida en el subjuego de los pools, sin tener que compartir las recompensas que gana. Así, en base a la racionalidad individual [50], la estrategia óptima para un minero siempre es desertar. Por otro lado, si todos siguen el mismo razonamiento, la cooperación cesa, el nivel de competencia aumenta y la utilidad esperada de cada uno se vuelve más baja que la de un escenario cooperativo[63]. En la teoría de juegos, este tipo de problema constituye un dilema social

[63] La utilidad de un jugador varia según un factor proporcional a $1/S^2$ [43].

y encuentra su nombre en el dilema generado para los jugadores por la matriz de las utilidades asociadas con los conjuntos de estrategias[64]. Formalmente, en un juego donde j otros jugadores cooperan, si denotamos a_j la utilidad de un minero que coopera y b_j la utilidad de uno que deserta, tenemos las siguientes propiedades de las utilidades de un dilema social [51]:

1- Los mineros prefieren que los demás cooperen: $a_{j+1} \geq a_j$ y $b_{j+1} \geq b_j,\ \forall j$
2- La deserción genera una utilidad esperada estrictamente superior a la cooperación: $b_{j+1} > a_j,\ \forall j$
3- La cooperación mutua se favorece a expensas de la deserción mutua: $a_{n-1} > b_0$

Cuando el juego se juega solo una vez, la paradoja del dilema social es que la única solución y el estricto equilibrio de Nash es la deserción mutua de los jugadores, que es un conjunto de estrategias estrictamente Pareto dominantes, pero que no es un óptimo de Pareto. Más bien, este último es el conjunto de estrategias donde los jugadores cooperan entre sí [52]. Para evaluar adecuadamente el dilema de los mineros, es necesario modelizarlo como un juego repetido donde las utilidades de los jugadores corresponden a la suma de sus utilidades esperadas sobre todas las iteraciones futuras del juego.

Modelo

El dilema de los mineros es un juego simultáneo, multijugador, no cooperativo, repetido al infinito, con información perfecta e incompleta, en el que la minería de un bloque constituye una iteración del juego. La utilidad esperada de un minero es la suma de sus utilidades esperadas, definidas por la ecuación (21), sobre todas las iteraciones futuras y depende de sus propias acciones y de las de los demás. En cada iteración, las posibles acciones son la cooperación (C), es decir la participación a un pool, o la deserción (D), es decir minar en solitario. Existen 2^n posibles estados de una iteración, de acuerdo con las elecciones de los n mineros presentes en el sistema.

[64] En teoría de juegos, el dilema social más famoso y ampliamente estudiado es el del *dilema del prisionero* [52]. El dilema de los mineros es similar a una versión multijugador repetida al infinito del dilema del prisionero o del juego *public goods game* [51].

Si estos últimos tienen la misma estructura de utilidades, entonces el espacio se limita a n estados.

Estrategia de Equilibrio

Cuando el número de iteraciones del juego es finito, los jugadores pueden usar la inducción hacia atrás para determinar sus estrategias, tratando de predecir las elecciones que harán sus oponentes en la última iteración y deduciendo las respuestas óptimas subiendo en el árbol de decisiones. Cuando el juego se repite al infinito como en el dilema de los mineros, los jugadores a menudo definen sus estrategias en función de los comportamientos pasados de sus oponentes[65]. Numerosos trabajos teóricos y experimentales (por ejemplo, [53], [54], [55] y varios citados en [51]) han sido hechos para entender los comportamientos de los jugadores en distintos contextos de dilemas sociales y establecer equilibrios basados en la cooperación. Para lograr un equilibrio en el dilema de los mineros, confiamos en la teoría desarrollada por Hilbe et al. [51] para las estrategias *zero-determinant* (ZD)[66] en los dilemas sociales repetidos multijugador sin límite en el número de jugadores[67]. Las estrategias ZD son *memory-one*[68], es decir que se basan únicamente en el resultado de la iteración previa de un juego.

Definimos la estrategia *memory-one* $\boldsymbol{p} = (p_{C,n-1}, \dots, p_{C,0}, p_{D,n-1}, \dots, p_{D,0})$ donde $p_{S,j}$ es la probabilidad de que un minero coopere en la próxima iteración habiendo elegido la acción $S \in \{C, D\}$ en la ronda anterior mientras que j otros cooperaron[69]. Definimos $v_{S,j}(t)$ la probabilidad de que el resultado de la iteración t sea (S, j) y $v(t) = [v_{C,n-1}(t), \dots, v_{D,0}(t)]$ el vector de estas probabilidades. Cuando $t \to \infty$, la distribución

[65] Esta rama de la teoría de juegos se llama teoría evolutiva de juegos (EGT), que se aplica al estudio de poblaciones cambiantes [102].
[66] Press and Dyson [104].
[67] Para grupos grandes, los mecanismos desarrollados para mantener un equilibrio son a menudo ineficaces porque se hace difícil para un jugador analizar el comportamiento de sus oponentes y tener influencia sobre ellos. [51]. Por lo tanto, la teoría de Hilbe et al. [51] se adapta bien al contexto de Bitcoin debido a que el número de mineros es grande.
[68] Por ejemplo, *Tit for Tat* [105] y *Win-Stay, Lose-Shift* [58].
[69] Por simplicidad, aquí se supone que todos los mineros son idénticos y que la probabilidad de cooperar depende solo del número que han cooperado sin distinción individual entre ellos. Hilbe et al. [51] también presentan una extensión cuando se necesita hacer la distinción.

límite $\boldsymbol{v} = [v(1) + \cdots + v(t)]/t$ representa las fracciones del número de iteraciones con el resultado (S, j). Para un minero i, $\boldsymbol{g}^i = \left(g^i_{S,j}\right)$ es el vector de posibles utilidades durante una iteración del juego, y denotamos $g^i_{C,j} = a_j$ y $g^i_{D,j} = b_j$. De manera similar, $\boldsymbol{g}^{-i} = \left(g^{-i}_{S,j}\right)$ corresponde a la utilidad promedia de los demás, con $g^{-i}_{C,j} = \left[ja_j + (n-j-1)b_{j+1}\right]/(n-1)$ y $g^{-i}_{D,j} = \left[ja_{j-1} + (n-j-1)b_j\right]/(n-1)$. Entonces, la utilidad esperada del minero i en el dilema de los mineros es $\pi^i = \boldsymbol{g}^i \cdot \boldsymbol{v}$ y la de los demás es $\pi^{-i} = \boldsymbol{g}^{-i} \cdot \boldsymbol{v}$. A partir del resultado general de Akin [56][70] demostrando la relación entre una estrategia *memory-one* y la distribución límite, Hilbe et al. [51] establecen la siguiente relación cuando el minero i aplica una estrategia ZD de la forma $\boldsymbol{p} = \boldsymbol{p}^{Rep} + \alpha\boldsymbol{g}^i + \beta\boldsymbol{g}^{-i} + \gamma\mathbf{1}$[71]:

$$0 = (\boldsymbol{p} - \boldsymbol{p}^{Rep}) \cdot \boldsymbol{v} = \left(\alpha\boldsymbol{g}^i + \beta\boldsymbol{g}^{-i} + \gamma\mathbf{1}\right) \cdot \boldsymbol{v} = \alpha\pi^i + \beta\pi^{-i} + \gamma\mathbf{1} \tag{22}$$

La ecuación (22) demuestra la relación lineal entre la utilidad de un minero y la de los demás, independientemente de sus estrategias. Al elegir bien los valores de los parámetros α, β y γ, uno puede entonces ejercer un cierto control sobre la relación entre sus utilidades y las del resto. Haciendo las manipulaciones $l = -\gamma/(\alpha + \beta)$, $s = -\alpha/\beta$ y $\phi = -\beta$, la misma relación se puede expresar en las dos siguientes formas equivalentes [51] :

$$\pi^{-i} = s\pi^i + (1-s)l \tag{23}$$

$$\boldsymbol{p} = \boldsymbol{p}^{Rep} + \phi\left[(1-s)\left(l\mathbf{1} - \boldsymbol{g}^i\right) + \boldsymbol{g}^i - \boldsymbol{g}^{-i}\right] \tag{24}$$

El parámetro l es una utilidad de referencia y s es la pendiente de la curva de estrategia que determina cómo varía la utilidad promedia del resto en función de la utilidad de un minero. De la ecuación (23), si todos aplican la misma estrategia $\boldsymbol{p}$, se deduce que $\pi^{-i} = \pi^i$ y todos obtienen la utilidad de referencia l. Hilbe y al. [51], [57] muestran que las estrategias ZD que permiten alcanzar un equilibrio de Nash estable

[70] $(\boldsymbol{p} - \boldsymbol{p}^{Rep}) \cdot \boldsymbol{v} = 0$, donde $\boldsymbol{p}^{Rep}$ es la estrategia *memory-one Repeat* con $p^{Rep}_{C,j} = 1$ y $p^{Rep}_{D,j} = 0$.

[71] Según la forma general de una estrategia ZD ($\boldsymbol{p} = \alpha\boldsymbol{g}^i + \beta\boldsymbol{g}^{-i} + \gamma\mathbf{1}$) definida por Press and Dyson [104], donde $\beta \neq 0$ y **1** es el vector de 2^n dimensiones compuesto de 1 en todas las posiciones.

de cooperación deben respetar dos criterios: $l = a_{n-1}$ y $s \geq (n-2)/(n-1)$. En el contexto de Bitcoin, donde el número de mineros es grande, s debería por lo tanto tender hacia 1. Cuando $s = 1$, se dice que la estrategia ZD es justa[72] y se asegura que el minero obtenga una utilidad igual a la utilidad promedia de los otros, independientemente de sus estrategias. En cuanto al parámetro ϕ, determina la velocidad, en términos del número de iteraciones del juego, en la que las utilidades convergen hacia la relación lineal (23). Como las probabilidades de cooperar $p_{S,j}$ están necesariamente entre 0 y 1 inclusive, los valores de los parámetros l, s y ϕ deben elegirse en consecuencia y los valores permisibles dependen del tipo de dilema social. Si suficientes mineros adoptan una estrategia justa, pueden mantener un equilibrio estable de cooperación y prevenir la deserción mutua causada por un grupo de recalcitrantes o en caso de deserción accidental. [51], [57]

Del resultado de Akin [56], Hilde et al. [51] también extienden sus resultados más allá de las estrategias ZD y definen cuatro condiciones que las estrategias *memory-one* puras[73] deben respetar para sostener un equilibrio estable de cooperación en los dilemas sociales. Por lo tanto, en el dilema de los mineros, las estrategias *memory-one* puras de equilibrio de los mineros (que definen las probabilidades de cooperación y deserción) deben respetar las siguientes condiciones [51]:

$$\begin{aligned} p_{C,n-1} &= 1 \\ p_{C,n-2} &= 0 \\ p_{D,1} &\leq \frac{a_{n-1} - a_0}{b_{n-1} - a_{n-1}} \\ p_{D,0} &\leq \frac{a_{n-1} - b_0}{b_{n-1} - a_{n-1}} \end{aligned} \tag{25}$$

No se impone ninguna restricción sobre los otros valores $p_{S,j}$ que definen la estrategia. Sin embargo, es posible que una estrategia *memory-one* pura no permita la cooperación después de la deserción mutua debido a las dos últimas condiciones

[72] i.e. *fair strategy*.
[73] Una estrategia *memory-one* pura tiene todas sus probabilidades iguales a 0 o 1. [57]

de (25) y no pueda sostener la cooperación en caso de deserción voluntaria o accidental de algunos mineros. En este sentido, Hauert y Schuster (citados en [51]) determinan que las estrategias *memory-one* puras efectivas para alcanzar un equilibrio de Nash estable de cooperación robusto a los errores son aquellas que cooperan tras la cooperación mutua y la deserción mutua, es decir, $p_{C,n-1} = 1$ y $p_{D,0} = 1$. Este tipo de estrategia se llama *Win-Stay Lose-Shift* (*WSLS*) [58] y conduce a un equilibrio de Nash solo si el dilema social respeta la condición $(b_{n-1} + b_0)/2 \leq a_{n-1}$. [51]

Por los criterios más restrictivos de las estrategias *memory-one* puras para lograr y sostener un equilibrio de cooperación estable, se propone que los mineros adopten una estrategia ZD justa que respete la siguiente forma, derivada de la ecuación (24) reemplazando $s = 1$:

$$\boldsymbol{p} = \boldsymbol{p}^{Rep} + \phi\left[\boldsymbol{g}^{i} - \boldsymbol{g}^{-i}\right] \tag{26}$$

Inversión Computaional Óptima – Cooperación y Deserción

Cuando un minero coopera y participa en un pool, su estrategia de equilibrio en cuanto a su inversión computacional es respetar el nivel de recursos para consumir asignado. En caso contrario, al desertar para minar en solitario, el minero se convierte en un jugador del subjuego de los pools. Si tiene suficientes recursos, adopta la estrategia de equilibrio y se considera como un jugador estratégico parte del conjunto S, pero si su capacidad computacional máxima no le permite adoptarla, invierte su capacidad máxima y esta se cuenta en la porción fija l.

Participación a la Minería

Un minero participa en la minería si cumple con la condición de la ecuación (15). El conjunto $\hat{S}$ de los mineros que invierten un poder computacional positivo se puede determinar de forma iterativa integrandolos gradualmente en el conjunto, en orden ascendente de ratio c_i/k_i, hasta que no se cumpla la condición de la ecuación (15) [38].

2.6 Prueba de Concepto

Esta sección presenta los resultados de las simulaciones realizadas para demostrar la viabilidad del modelo de juego de minería óptima propuesto. La elección de los valores de los parámetros se explica en el apéndice. Algunos fueron elegidos para simplificar las simulaciones, mientras que otros se establecieron para tratar de reflejar lo más fielmente posible el contexto de Bitcoin, aunque es difícil obtener datos confiables dada la falta de transparencia en este sentido. La simulación realizada demuestra que los mineros se encuentran efectivamente en un dilema social y que se puede lograr un equilibrio estable de cooperación.

2.6.1 Subjuego de los Pools

Establecemos los siguientes valores para los parámetros: $r = 6{,}25$; $\tau = 10\,000$; $\beta = 0{,}1$; $\theta = 0{,}000\,1$; $t_i = t_j = 2100$; $|U| = |S| = \widehat{|S|} = 10$; $c_i = c_j = 0{,}0007$; $\lambda_j = \mu_j = 0$; $k_i = k_j = k_l = 1$; $z_i = z_j = 0{,}005/60$ y $l = 700\,000$. La siguiente figura muestra las estrategias óptimas y las utilidades esperadas obtenidas según el número de pools estratégicos en el sistema.

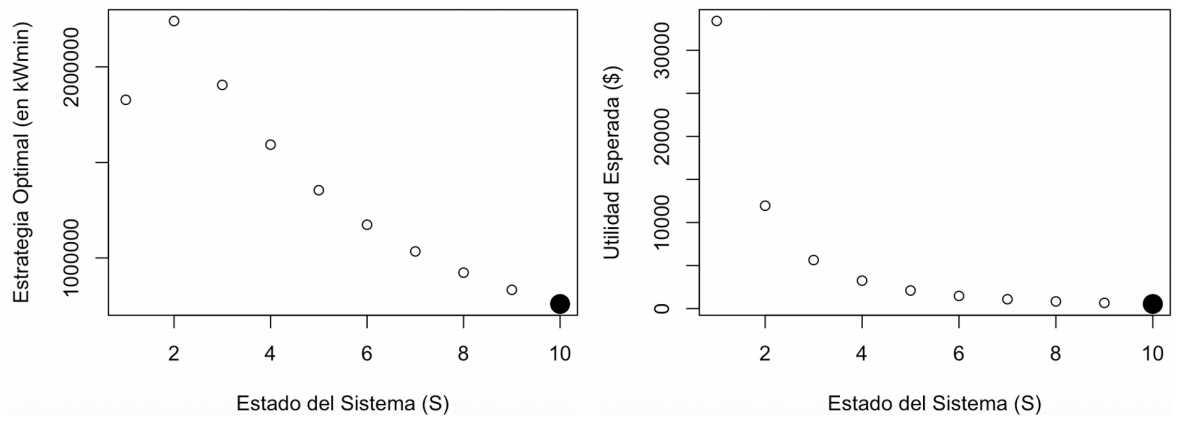


Figura 3 : PoC : Estrategias óptimas y utilidades esperadas de los pools en el subjuego de los pools.

Como $\lambda_j = \mu_j = 0$, el estado de la red se considera estático. Por lo tanto, la utilidad esperada en cada estado se evalúa por separado y coincide con la determinada por el modelo estático. Con diez pools estratégicos presentes en el sistema, la estrategia óptima es invertir 759 174,7 kWh/min y genera una utilidad esperada de 535,60$ por bloque para cada pool estratégico.

2.6.2 Protocolo de Pool

Para simplificar la simulación, el número de mineros registrados en el pool se limita a 1100 y se establece que 1050 de ellos están presentes en el sistema. Se supone que 500 tienen una capacidad computacional máxima que les impide jugar la estrategia óptima y, por lo tanto, su poder computacional se cuenta en la parte fija l. Se supone que 50 mineros estratégicos tienen un costo marginal más alto que los demás, por lo que no se cumple la condición de la ecuación (15) y entonces no invierten ningún poder computacional. Por lo tanto, establecemos los siguientes parámetros para el juego de protocolo entre los mineros, donde $E[r]_p^{x_p^*}$ es la recompensa esperada ganada por el pool al adoptar la estrategia óptima x_p^* determinada en el subjuego de los pools: $r = E[r]_p^{x_p^*} = 5848{,}82;\ \tau = 1;\ \beta = 0{,}1; |U| = 600; |S| = 550;\ |\widehat{S}| = 500; c_{i\in S/\hat{S}} = 0{,}000\,72;\quad c_{i\in\hat{S}} = 0{,}000\,70;\quad c_{i\notin S} = 0{,}000\,69;\quad l = 10\,000; \lambda_j = 1; \mu_j = 0{,}1; k_i = k_j = k_l = 1$ y los otros parámetros son nulos. Los valores de λ_j y μ_j están determinados para obtener una distribución de densidad de probabilidades del tiempo pasado en los distintos estados de acuerdo con los datos recopilados por Bitnodes [59] acerca del número de nodos conectados a la red Bitcoin[74].

Distribución del Trabajo Computacional

La estrategia de equilibrio del pool es invertir 759 174,7 kWh/min, distribuido entre los miembros según sus ratios c_i/k_i y sus capacidades máximas. Luego se calculan los costos por minero y sus índices de costos relativos. La siguiente tabla supone diferentes capacidades máximas y presenta los resultados obtenidos, eligiendo a los mineros no estratégicos como clase de referencia para el cálculo de los índices relativos.

[74] Ver el apéndice.

c_i	k_i	$\frac{c_i}{k_i}$	Número de mineros	Capacidad máxima (kW/min)	Tipo de minero	Recursos asignados por minero (kW/min)	Costo por minero ($/min)	Índices relativos de costo
0,00069	1	0,00069	500	20	No Estratégico	20	0,0138	1,00
0,00070	1	0,00070	300	100	Estratégico	100	0,0700	5,07
	1	0,00070	200	2000		2000	1,4000	101,45
	1	0,00070	50	50 000		6383	4,4684	323,80

Tabla 2 : PoC : Distribución del trabajo computacional entre los mineros..

Como se mencionó anteriormente en la sección 2.5.2, el costo marginal c_{p_i} de un pool i en el subjuego de los pools es un promedio de los costos marginales de sus mineros ponderados por sus niveles de contribución a la estrategia óptima y puede determinarse a partir de las columnas 1, 4 y 7 de la Tabla 2.

Juego de Protocolo

El siguiente gráfico muestra la utilidad esperada y el ROI obtenido de un minero que adopta la estrategia de equilibrio en el juego de protocolo, en función del estado del pool cuando ingresa al sistema.

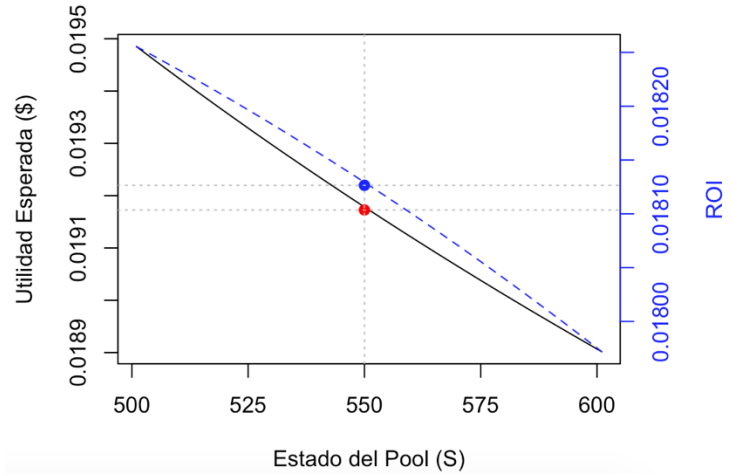


Figura 4 : PoC : Utilidades esperadas y ROI de los mineros estratégicos en el juego de protocolo.

Un minero estratégico que adopta la estrategia de equilibrio y se conecta al sistema al estado $S = 550$, tiene una utilidad esperada de $0{,}0192\$$ por bloque y un ROI de $1{,}81\%$.

Para un minero no estratégico, la utilidad esperada se determina con la siguiente fórmula:

$$R_{sim_i} = \frac{k_i x_i}{\sum_{j \in \hat{S}} k_j E\left[x_j^*\right] + k_l l} E[r]_p^{x_p^*} - \frac{c_i x_i}{\beta} \tag{27}$$

donde $E\left[x_j^*\right]$ es el poder computacional esperado que invierte un minero estratégico j. Tal participante adopta la estrategia óptima e invierte un poder computacional variable dependiendo del estado del pool. $E\left[x_j^*\right]$ es, por lo tanto, un promedio del poder invertido en cada estado, ponderado de acuerdo con la distribución del tiempo pasado en cada uno, la cual depende del estado del pool a la llegada del minero[75]. Para simplificar, hacemos el supuesto no realista pero sin impacto en la naturaleza de los resultados, que todos los mineros estratégicos llegan al estado $S = \hat{S} = 550$ y todos los no estratégicos invierten su capacidad máxima, que es la misma para todos, es decir $x_i^{max} = l/500$. Al integrar los valores en la ecuación (27) obtenemos una utilidad esperada de $0{,}002\,69\$$ por bloque para los mineros no estratégicos y un ROI es $1{,}95\%$ [76]:

La siguiente tabla resume las utilidades esperadas y los ROI de los mineros estratégicos y no estratégicos en el juego de protocolo, así como presenta los índices relativos de ROI calculados utilizando los no estratégicos como clase de referencia:

Tipo de minero	Número de mineros	Utilidad esperada del juego de protocolo ($)	ROI (%)	Índices relativos de ROI del juego de protocolo[1]
No Estratégico	500	0,002 69	1,95	1,00
Estratégico	550	0,0192	1,81	0,93

[1] El índice relativo de ROI de los mineros no estratégicos es más alto debido a su costo marginal inferior

Tabla 3 : PoC : Utilidades esperadas, ROI e índices relativos de ROI de los mineros estratégicos y no estratégicos en el juego de protocolo.

[75] En el apéndice, la sección sobre la elección de valores λ_j y μ_j presenta la distribución del tiempo pasado en los distintos estados para un minero que llega al estado $S = 550$.
[76] Cálculo en apéndice.

Repartición de la Recompensa

Los índices relativos de costo y de ROI de los mineros del pool se utilizan para determinar la tasa α_i de la recompensa ganada por el grupo que se otorgará a cada uno de ellos. A partir de la utilidad esperada del pool $R_p^{x_p^*} = 535{,}60\$$ determinada en el subjuego de los pools y de la recompensa esperada del pool $E[r]_p^{x_p^*} = 5848{,}82\$$ calculada previamente para determinar el valor de la recompensa en el juego de protocolo, se calculan las tasas α_i para cada minero según la ecuación (20). La siguiente tabla muestra los resultados obtenidos que permiten confirmar que los ROI relativos de los mineros son iguales a los del juego de protocolo:

c_i	Número de mineros	Capacidad máxima (kW/min)	Tipo de minero	Recursos asignados por minero (kW/min)	Costo por minero ($/min)	Índices relativos de costo	Índices relativos de ROI del juego de protocolo	$\mathbb{I}_i \cdot R_p^{x_p}$	α_i
0,00069	500	20	No Estratégico	20	0,0138	1,00	1,00	0,0150	2,62E-05
0,00070	300	100	Estratégico	100	0,0700	5,07	0,93	0,0705	1,32E-04
	200	2000		2000	1,4000	101,45	0,93	1,4099	2,63E-03
	50	50 000		6383	4,4684	323,80	0,93	4,4999	8,41E-03

Tabla 4 : PoC : Repartición de la recompensa entre los mineros del pool.

2.6.3 Dilema de los Mineros

Confirmación del Dilema Social

La siguiente tabla muestra las utilidades esperadas de los mineros según tres escenarios: cooperación mutua de todos (a_n), deserción de uno solo (b_{n-1}) y deserción mutua de todos (b_0). Cuando un minero invierte en más de un pool, se supone que son iguales. Los resultados obtenidos respetan las condiciones de la sección 2.5.4 sobre las utilidades de un dilema social y muestran que la cooperación aumenta significativamente las ganancias de todos los mineros.

Tipo de minero	c_i	Capacidad máxima (kW/min)	Recursos asignados pool (kW/min)	Utilidad esperada ($)			$\frac{b_{n-1}}{a_{n-1}}$	$\frac{a_{n-1}}{b_o}$
				a_{n-1}	b_{n-1}	b_0 [1]		
No Estratégico	0,00069	20	20	0,0150	0,0296	0,0002	1,98	74,86
Estratégico	0,00070	100	100	0,0705	0,1482	0,0012	2,10	58,74
		2000	2000	1,4099	2,9597	0,0212	2,10	66,50
		50 000	6383	35,2464*	71,3085	0,0477	2,02	738,92

[1] Para este escenario, solo los mineros con capacidad máxima de 50 000 son estratégicos (S=510, I=5 100 000)

* Se supone que los mineros pueden invertir en varios pools hasta llegar a su capacidad máxima

Tabla 5 : PoC : Utilidades esperadas de los mineros según distintas estrategias adoptadas en el dilema social de los mineros.

Logro de un Equilibrio Estable de Cooperación

El logro de un equilibrio de Nash estable de cooperación se verifica simulando una red paramétrica. Para simplificar la simulación, se asume un total de 10 000 mineros en la red que tienen el mismo perfil. El vector de las utilidades posibles al minar un bloque se define $\boldsymbol{g}^i = (a_{n-1}, \dots, a_0, b_{n-1}, \dots, b_0)$ y nos basamos en los resultados de la última línea de la Tabla 5 para estimar $a_{n-1} = 35\$$, $b_{n-1} = 70\$$ y $b_0 = 0{,}05\$$. Establecemos arbitrariamente $a_0 = 0{,}04\$$ y determinamos las utilidades a_j y b_j donde $j \in \{1, \dots, n-2\}$ con el fin de lograr una disminución lineal de las utilidades a_j y b_j. El vector $\boldsymbol{g}^i$ resultante respeta las propiedades de las utilidades de un dilema social determinadas en la sección 2.5.4 y se calcula $\boldsymbol{g}^{-i}$ de acuerdo con la fórmula establecida en dicha sección. En las simulaciones, se supone que todos los mineros de la red siguen la estrategia propuesta por la ecuación (26) para lograr un equilibrio estable de cooperación, es decir $\boldsymbol{p} = \boldsymbol{p}^{Rep} + \phi\left[\boldsymbol{g}^i - \boldsymbol{g}^{-i}\right]$.

El valor de ϕ se elige para que todas las probabilidades del vector $\boldsymbol{p}$ estén entre 0 y 1 inclusive. Como se mencionó anteriormente, el valor de ϕ determina la velocidad, en términos del número de iteraciones, en la que las utilidades de los mineros convergen hacia la relación lineal de la ecuación (23). En las simulaciones, ya que todos los mineros adoptan una estrategia *memory-one* justa, ϕ determina el número de iteraciones necesarias para lograr el equilibrio: cuanto mayor sea ϕ, más iteraciones se necesitan. Al contrario, si $\phi = 0$, entonces $\boldsymbol{p} = \boldsymbol{p}^{Rep}$ y el equilibrio se alcanza inmediatamente porque los mineros siempre repiten la misma acción con cada iteración. La siguiente figura muestra las estrategias $\boldsymbol{p} =$

$(p_{C,n-1}, \dots, p_{C,0}, p_{D,n-1}, \dots, p_{D,0})$ obtenidas con un valor de ϕ máximo ($\phi = 1/\max(\boldsymbol{g}^i - \boldsymbol{g}^{-i})$), mínimo ($\phi = 0$) e intermedio ($\phi = 0{,}5 \times 1/\max(\boldsymbol{g}^i - \boldsymbol{g}^{-i})$).

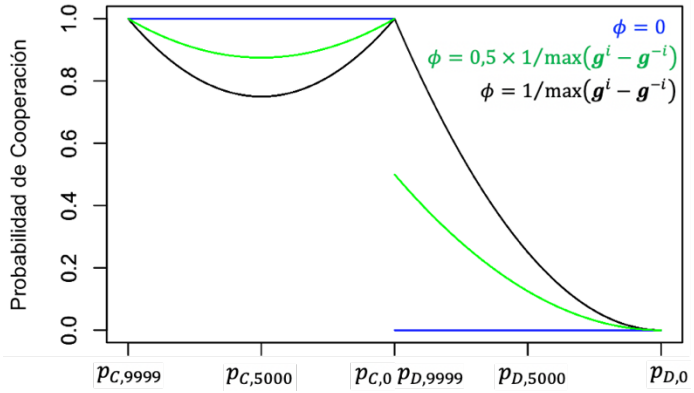
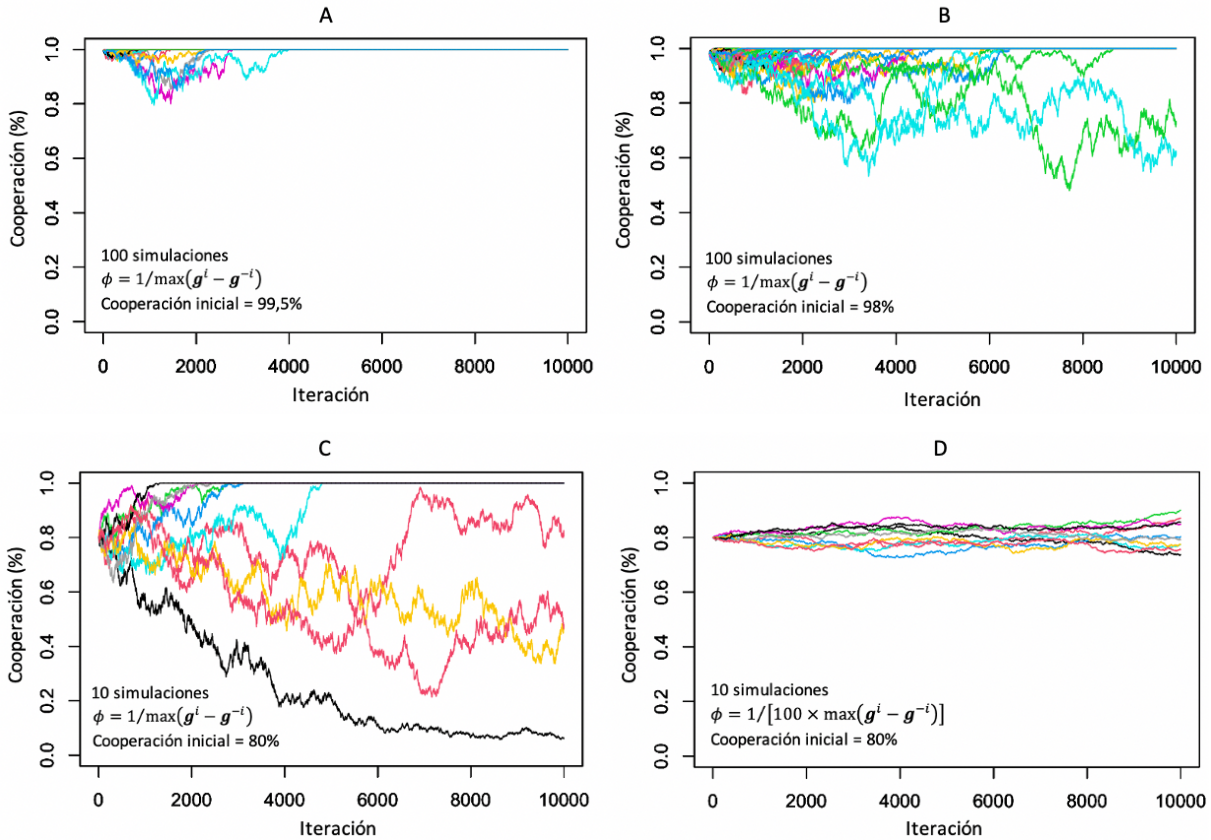


Figura 5 : Estrategias *memory-one* justas según distintos valores de ϕ.

Los siguientes gráficos muestran la evolución del nivel de cooperación de los mineros en la red según distinctos niveles de cooperación inicial y valores de ϕ. Se supone que todos siguen la misma estrategia justa $\boldsymbol{p}$.



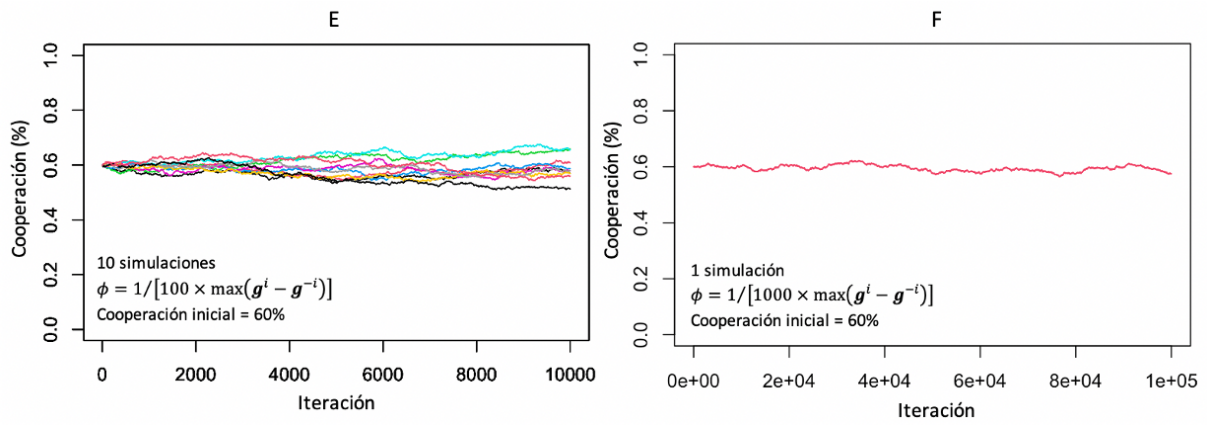


Figura 6 : Evolución de la cooperación en la red según distintos valores de ϕ y niveles de cooperación inicial.

Los gráficos A y B muestran que mientras todos los mineros cooperan al entrar en el sistema, una estrategia justa conduce a un equilibrio estable de cooperación y soporta hasta cierta medida las desviaciones de estrategia (accidentales o voluntarias). Sin embargo, los gráficos B y C muestran que para un ϕ grande, cuantos más mineros desertan en una iteración, más difícil será lograr un equilibrio estable de cooperación. Esto se debe a la mayor variabilidad en las probabilidades de cooperación cuando ϕ es grande (ver Figura 5): por un lado, la deserción de una minoría se castiga más severamente al generar más deserciones posteriores y, por otra parte, la probabilidad de volver a la cooperación tras una deserción disminuye significativamente cuando el nivel de cooperación disminuye. Como resultado, se necesitan más iteraciones para lograr un equilibrio estable y la probabilidad de que el mismo sea una deserción mutua aumenta cuando el nivel de cooperación disminuye.

Por otro lado, los gráficos D, E y F muestran que un ϕ pequeño, o incluso que tienda hacia 0, estabiliza el nivel actual de cooperación en la red. Por ejemplo, en los gráficos B y C en los que todos los mineros aplican una estrategia $\boldsymbol{p}$ con un ϕ grande, algunas curvas se están moviendo hacia la deserción y en algún momento alcanzan un nivel de cooperación de 60%; los mineros cooperativos podrían entonces formar una alianza[77] y acordarse para ajustar su ϕ a un valor muy bajo para garantizar un

[77] Los trabajos de Hible et al. [51], [57] también demuestran la influencia que pueden tener las alianzas sobre los otros jugadores. Según su tamaño y su estrategia, una alianza puede hasta incitar y traer de vuelta a la cooperación los desertores.

nivel mínimo de cooperación, independientemente de las estrategias de los desertores. El nivel de cooperación se estabilizará como en el gráfico F si los desertores siguen desertando y aumentará si vuelven a la cooperación.

2.7 Análisis y Observaciones

En esta última sección, presentamos algunos análisis, observaciones y consideraciones que surgen del trabajo realizado.

2.7.1 Prueba de Concepto y Aplicabilidad del Modelo

Para la prueba de concepto, los valores de los parámetros se eligieron tanto para tratar de reflejar el contexto actual de Bitcoin como para simplificar las simulaciones. Sin embargo, el consumo de energía global óptimo de la red obtenido de estas es del orden de 4000 TWh anualmente. Esto es significativamente superior a las estimaciones realizadas en [60], [61] y [62] acerca del consumo de energía de la red Bitcoin que sería más del orden de 35 a 70 TWh anualmente. Si el orden de magnitud de los resultados sigue siendo similar a partir de simulaciones más complejas que reflejan mejor la realidad de Bitcoin, esto implicaría que el modelo propuesto no es aplicable en el contexto actual, ya que los pools no podrían adoptar la estrategia de equilibrio. Por lo general, el modelo establece que la red consumirá el nivel de electricidad necesario para maximizar la utilidad de los mineros, que depende principalmente del monto de la recompensa (en bitcoins), del valor de la moneda Bitcoin y de los costos marginales para minar[78]. Variaciones en estos parámetros podrían eventualmente hacer que el modelo sea aplicable. En particular, se espera que el monto de la recompensa disminuya con el tiempo, hasta que solo esté compuesto por los costos de transacción en los alrededores de 2140 [63], lo que reducirá significativamente el nivel de inversión energética óptimo.

2.7.2 Estabilidad

Equilibrio Estable

En cada uno de los subjuegos del juego de minería óptimo, existe un equilibrio. En el caso del subjuego de los pools y del juego de protocolo, los equilibrios son únicos y, por lo tanto, necesariamente estables. En el dilema de los mineros, un equilibrio estable de cooperación es alcanzable. En este caso, el equilibrio no implica que todos

[78] Si se supone que los mineros tienen equipos con una eficiencia energética similar, solo aumenta la tasa de hash de la red, pero no tiene impacto en el nivel de consumo de energía [62].

los mineros cooperen en todo momento, sino que sus estrategias están definidas para promover la cooperación a expensas de la deserción mutua. Pueden establecer sus estrategias, por ejemplo, con una probabilidad positiva de desertar del pool bajo ciertas circunstancias, pero en última instancia, las mismas también los llevarán nuevamente a la cooperación cuando existe el riesgo de deserción mutua de todos.

El equilibrio estable de cooperación asegura que siempre haya un cierto nivel de cooperación en la red, de modo que los mineros que participan en un pool se beneficien de esta cooperación, incluso si hay una proporción de recalcitrantes que desertan y cuya utilidad esperada es mayor. El hecho de que los mineros tengan una preferencia individual por la deserción contribuye a la descentralización del sistema mediante la distribución del poder computacional de la red fuera de los pools. Sin embargo, el beneficio colectivo que se obtiene de la cooperación también los impulsa a cooperar cuando el riesgo de deserción mutua es demasiado alto. El incentivo para cooperar es esencial para la viabilidad del modelo de juego de minería óptima: dado que son los pools que implementan el modelo, deben obtener un beneficio al hacerlo y poder atraer mineros. Del mismo modo, la estabilidad de los ingresos ofrecida por un pool también constituye un incentivo para participar en él.

En resumen, existe un balance entre los incentivos para la cooperación y la deserción que conduce a un equilibrio de cooperación estable y descentralizado en cuanto a la distribución del poder computacional en la red. Sin embargo, es importante recordar que la existencia de equilibrios en las soluciones de los juegos no significa que se alcancen por seguro: para esto, los jugadores deben adoptar la estrategia de equilibrio. Especialmente en los dilemas sociales multijugadores que se repiten al infinito, estos a menudo definen sus estrategias basándose en los comportamientos pasados de sus oponentes y la evolución de las poblaciones puede ser difícil de predecir[79].

[79] La teoría de juegos evolutiva aplica la teoría de juegos al estudio de la evolución de las poblaciones [102].

Poder Predictivo

La implementación de un modelo de minería basado en el consumo óptimo de recursos computacionales ofrece la ventaja importante de dar un poder predictivo al modelo, fomentando así la estabilidad del sistema. Por ejemplo, la aplicación del modelo permite anticipar el impacto de un *halving* en el poder computacional total de la red. Un *halving* es una operación que forma parte del diseño de Bitcoin y que implica una reducción a la mitad del monto de la recompensa fija cada 210 000 bloques o aproximadamente cada cuatro años. Históricamente, estas operaciones han causado mucha incertidumbre y una gran variabilidad en el valor de la moneda, lo que a su vez influye en la minería [63]. Ser capaz de predecir el impacto de un *halving* en la minería reduce la incertidumbre para los mineros, los inversores y los usuarios, así como fomenta la estabilidad de la moneda y del sistema.

Se pueden hacer análisis similares a partir de otros parámetros del modelo y que sirven como una herramienta para las decisiones de diseño del sistema. Por ejemplo, el impacto en la minería de modificar el tamaño límite de bloque[80] se puede evaluar a partir de los parámetros z (factor de retraso de propagación) y t_i (número de transacciones en un bloque). También, el modelo puede ayudar a determinar el monto promedio de los cargos de transacción (θ) necesarios para mantener un incentivo para los mineros y un poder computacional total de la red suficiente para garantizar la seguridad del sistema.

Sistema de Bonos y Penalizaciones

Para alentar a los mineros a respetar el nivel de recursos para consumir que les ha asignado el pool, más allá del incentivo directo de maximizar su utilidad, se podría desarrollar un sistema de bonos y penalizaciones. Por ejemplo, el sistema podría aplicar ajustes retroactivos en los cuales las recompensas otorgadas se ajustarían para coincidir con el escenario de equilibrio. Si un minero invierte menos del nivel asignado, su recompensa se reduciría garantizando todavía que los otros mineros del pool mantengan el mismo rendimiento relativo óptimo que habrían

[80] El aumento del tamaño límite de bloque ha sido objeto de varios debates y ha llevado a la creación de Bitcoin XT [112].

alcanzado en el equilibrio. Si invierte más del nivel asignado, el pool podría simplemente ignorar sus intentos excesivos para resolver la PoW. Asimismo, se podría implementar un sistema similar entre los pools, lo cual confirmaría su compromiso mutuo de respetar la estrategia de equilibrio. Tal sistema agregaría un incentivo para que los mineros y los pools se adhieran a dicha estrategia y, por lo tanto, fortalecerían la estabilidad del sistema.

Transparencia de la Información

Dhamal et al. [38] proponen la creación de una interfaz donde los mineros podrían declarar públicamente su costo marginal, pero tengan en cuenta que tal solución podría no ser viable en la realidad ya que los mineros no tienen ningún incentivo para compartir su información y probablemente preferirían no hacerlo. Ante esta limitación, señalen que el diseño de incentivos para que los jugadores compartan su costo marginal representa una vía interesante para desarrollos futuros. La arquitectura del modelo de juego de minería óptima parece satisfacer esta necesidad y, además, contribuye a cumplir la premisa del conocimiento común[81] que está vinculado entre otras cosas a la conciencia de la información[82]. Al compartir su costo marginal, eficiencia energética y capacidad máxima, los mineros aumentan su utilidad esperada al poder determinar y adoptar estrategias de equilibrio que dependen del saber de esta información. La transparencia de la información resultante facilita los análisis y las predicciones, aumenta la confianza de los usuarios y fomenta la estabilidad del sistema.

2.7.3 Descentralización

En función principalmente del monto de la recompensa, de los cargos de transacción y de los costos marginales, el modelo permite determinar el poder computacional total de la red. Sin embargo, es difícil estimar el número de jugadores que serían estratégicos en el subjuego de los pools. Como se mencionó anteriormente, cuantos más hay, más aumenta la competencia y más disminuye la

[81] Una de las dos premisas principales de la teoría de juegos. Ver la sección 1.1.
[82] Información perfecta o imperfecta. Ver la sección 1.2.5.

utilidad esperada de cada uno. Por el contrario, cuantos menos hay, más aumenta la utilidad esperada de cada uno. El mejor escenario, que no parece improbable y que garantizaría la descentralización del poder computacional de la red, sería que la implementación del modelo creara un mercado competitivo entre los pools que estaría entre la competencia oligopolística y perfecta [64], con un gran número de pools que aplicarían sustancialmente el mismo protocolo. Dicha estructura de mercado podría ser viable y rentable para los pools incluso con la existencia de un gran número de ellos, dependiendo del modelo económico de cada uno. A este efecto, la sección 2.7.4 siguiente propone un modelo económico que podrían adoptar. Sin embargo, sería interesante analizar con más detalle el impacto de adoptar el modelo de minería óptima en el número de jugadores en el subjuego de los pools. En todos los casos, como se mencionó anteriormente, la descentralización de la red también se ve fomentada por el incentivo a la deserción en el dilema de los mineros, que se refuerza cuanto más el número de pools disminuye.

2.7.4 Modelo Económico y Cargos de Pool

El modelo de juego de minería óptima implica que un pool recopila la información sobre la eficiencia energética, el costo marginal y la capacidad máxima de los mineros. Luego explota esta información para maximizar la utilidad esperada de estos últimos y para este propósito, su tarea es asesorarlos sobre el nivel de inversión computacional al asignarles un nivel de recursos para consumir. En cierto modo, esta función es análoga a la de un asesor financiero que aconseja a los clientes sobre sus inversiones. Por lo tanto, el modelo económico de los pools también podría ser similar al de un asesor financiero que retiene una comisión correspondiente a una cierta proporción del rendimiento que genera para sus clientes. Así, los cargos de pool podrían corresponder a un porcentaje retenido de las ganancias de los mineros. Tal modelo estaría justificado dado que la gestión de la información y las decisiones estratégicas realizadas por el pool permiten directamente aumentar los beneficios de sus miembros. Como se demuestra en la prueba de concepto, la aplicación del modelo de juego de minería óptima aumenta significativamente la utilidad esperada de los mineros y entonces, es posible que las ganancias de los pools también aumentarían significativamente.

2.7.5 Protección contra Ataques

La aplicación de un modelo de minería que sea determinista y transparente en cuanto al nivel de recursos a ser consumidos podría constituir un modelo preventivo contra ciertos ataques conocidos contra la red Bitcoin, o al menos podría ser un medio para detectar estos ataques. Al conocer el nivel de recursos que cada uno debe consumir, se puede deducir la fracción de las recompensas que cada uno debería recoger y detectar los comportamientos deshonestos cuando un jugador recolecta más que su justa parte, como por ejemplo en casos de *selfish mining* [65], [66] o de retención de bloques [67]. Además, si se implementa un sistema de ajustes retroactivos (es decir, un sistema de bonos y penalizaciones) como el descrito en la sección 2.7.2, los mineros y los pools no tendrían ningún incentivo para actuar deshonestamente. En cierto modo, al adherirse al modelo y acordar colaborar entre sí, los pools se comprometerían indirectamente a actuar honestamente: de lo contrario, tendrían que pagar una multa que anularía los beneficios derivados de su comportamiento desviado. Sin embargo, este aspecto merecería ser analizado con más detalle para comprender completamente las implicaciones del modelo de minería óptima sobre posibles ataques contra Bitcoin.

Conclusión

La minería de Bitcoin es una competencia entre los mineros por una recompensa. Este proceso está en el corazón del mecanismo de consenso del sistema que mantiene la cadena de bloques y garantiza su seguridad sin la necesidad de una autoridad central. Por otro lado, el papel de la teoría de juegos es analizar las interacciones estratégicas entre jugadores y las consecuencias de sus decisiones estratégicas sobre el resultado de un juego. El objetivo de este trabajo fue primero aplicar la teoría de los juegos a la minería de Bitcoin para comprender su dinámica y luego proponer un modelo de minería óptima que refuerce la descentralización y la estabilidad del sistema, aspectos que no son suficientemente soportados por los mecanismos actuales de Bitcoin.

En la sección 1, se han resumido las nociones principales de la teoría de juegos. Las premisas de racionalidad y de conocimiento común constituyen los principios fundamentales en los que se basan el análisis de un juego y el desarrollo de su solución. Una situación puede modelarse como un juego y analizarse según su tipo, que está determinado por ciertas características del modo de juego (cronología, frecuencia, cooperación) y en relación con la información (simetría, conciencia, conocimiento). Luego, un concepto de solución que depende del tipo de juego aplica algunas reglas formales para predecir el resultado del mismo. El concepto de solución más importante es el equilibrio de Nash, que se logra cuando ningún jugador puede mejorar su estrategia unilateralmente.

En la segunda parte del trabajo, primero presentamos en las secciones 2.2 y 2.3 un modelo estático (Xiong et al. [43], Dimitri [42], Chiu et Koeppl [44]) y un modelo dinámico (Dhamal et al. [38]) que pueden aplicarse a la minería de Bitcoin y permiten determinar la inversión computacional óptima que maximiza la utilidad de un minero. En la sección 2.4, se propuso un modelo que resulta de la unificación y mejora (adición de un factor de eficiencia energética y de un parámetro de tasa de conversión de moneda) de los dos modelos presentados previamente. En la sección 2.5, se desarrolló un modelo de juego de minería óptima con el objetivo de mejorar la descentralización y la estabilidad de la red Bitcoin. El juego modelado es un juego Stackelberg con dos niveles: en el primero, los pools son los líderes que asignan un

nivel de recursos para consumir a los mineros y, en el segundo, los mineros deciden el nivel y la distribución (pools o minería solitaria) de sus recursos. Cada nivel está compuesto por un subjuego. En el primer nivel, un *subjuego de los pools* (sección 2.5.2) permite que estos determinen el poder computacional óptimo que necesitan generar para maximizar su utilidad. Esto es posible gracias al intercambio de información de los mineros (costo marginal, eficiencia energética y capacidad máxima) y a la colaboración entre los pools. En el segundo nivel, el *dilema de los mineros* (sección 2.5.4) es un dilema social en el que estos deben elegir entre sus preferencias individuales y el interés común de todos. También se desarrolló brevemente un protocolo de pool que establece las reglas del juego entre el pool y sus miembros en la sección 2.5.3. Se definieron tres componentes del protocolo: la distribución del trabajo computacional entre los mineros, un juego de protocolo que simula una competencia interna entre ellos y la repartición de la recompensa dentro del pool (basada en el juego de protocolo). Las soluciones del subjuego de los pools y del juego de protocolo son equilibrios de Nash únicos y estables determinados por el modelo propuesto en la sección 2.4, mientras que el dilema de los mineros conduce a un equilibrio estable de cooperación cuando eligen sus estrategias de acuerdo con ciertos criterios, según el trabajo de Hilbe et al. [51]. Los resultados de una prueba de concepto se presentaron luego en la sección 2.6 y parecen demostrar que el modelo el juego de minería óptima aumentaría significativamente las utilidades de los mineros mediante el alcance de un equilibrio estable de cooperación en el dilema social en el que se encuentran.

Finalmente, en la sección 2.7, se realizaron ciertos análisis y observaciones sobre el trabajo realizado. Esencialmente, se llega a la conclusión de que el modelo de juego de minería óptima desarrollado parece favorecer la descentralización y la estabilidad de la red Bitcoin. Principalmente, el dilema social de los mineros junto con el balance en los incentivos asegura una cierta distribución del poder computacional entre los pools y la minería solitaria. Asimismo, la existencia de equilibrios en las soluciones de los juegos proporciona una estabilidad tangible al sistema. Sin embargo, se debe realizar un trabajo adicional sobre la aplicabilidad de dicho modelo en el contexto actual de Bitcoin, los problemas de implementación y las implicaciones de seguridad más allá de la descentralización y de la estabilidad, como los ataques posibles contra el sistema.

Apéndice

Sección 2.2.3 – Corrección de la estrategia óptima de Xiong et al. [43].

Según lo especificado por Xiong et al. [43], tenemos la función de utilidad $u_i(x_i, x_{-i}, p_i) = (R + rt_i)\frac{x_i}{\sum_{j=1}^{N} x_j} e^{-\lambda z t_i} - p_i x_i$ y la condición de la primera derivada $\frac{\partial u_i}{\partial x_i} = (R + rt_i)e^{-\lambda z t_i}\frac{\partial \alpha_i}{\partial x_i} - p$ donde $\frac{\partial \alpha_i}{\partial x_i} = \frac{\sum_{j \neq i} x_j}{(\sum_{i \in N} x_i)^2}$. Al igualar a cero y aislar x_i para obtener la estrategia óptima, tenemos:

$$0 = (R + rt_i)e^{-\lambda z t_i}\frac{\sum_{j \neq i} x_j}{(\sum_{i \in N} x_i)^2} - p$$

$$\left(\sum_{i \in N} x_i\right)^2 = \frac{(R + rt_i)e^{-\lambda z t_i}}{p}\sum_{j \neq i} x_j$$

$$x_i{}^* = \sqrt{\frac{(R + rt_i)e^{-\lambda z t_i}}{p}\sum_{j \neq i} x_j} - \sum_{j \neq i} x_j$$

Sección 2.2.5 – Demostración 1: Equivalencia entre las estrategias de equilibrio de los modelos estáticos de Xiong et al. [43], Dimitri [42] y Chiu et Koeppl [44].

A partir de la estrategia de equilibrio (5) de Xiong et al. [43] :

$$x_i{}^* = \frac{N-1}{\sum_{j \in N}\frac{p}{(R + rt_j)e^{-\lambda z t_j}}} - \left(\frac{N-1}{\sum_{j \in N}\frac{p}{(R + rt_j)e^{-\lambda z t_j}}}\right)^2 \frac{p}{(R + rt_i)e^{-\lambda z t_i}} \quad , \forall i$$

y si generalizamos la recompensa de tal manera que $(R + rt_i) = R$, que asumimos que un bloque minado ciertamente está incluido en la cadena, es decir $e^{-\lambda z t_i} = 1$, y reformulamos $N = n$, $p = c_i$ y $\sum_i c_i = c_{(n)}$, obtenemos:

$$x_i{}^* = \frac{n-1}{\sum_{j\in N}\frac{c_j}{R}} - \left(\frac{n-1}{\sum_{j\in N}\frac{c_j}{R}}\right)^2 \frac{c_i}{R} = \frac{R(n-1)}{\sum_{j\in N} c_j} - \frac{R^2(n-1)^2}{\left(\sum_{j\in N} c_j\right)^2}\frac{c_i}{R} = \frac{Rc_{(n)}(n-1) - R(n-1)^2 c_i}{{c_{(n)}}^2}$$

$$= \frac{R(n-1)\left[c_{(n)} - (n-1)c_i\right]}{{c_{(n)}}^2}$$

que corresponde al equilibrio calculado por Dimitri [42]. Luego aplicando las sustituciones $n = M$ y asumiendo un costo unitario uniforme para todos los mineros tal que $c_i = \alpha$ et $c_{(n)} = M\alpha$, obtenemos:

$$x_i{}^* = \frac{R(M-1)[M\alpha - (M-1)\alpha]}{(M\alpha)^2} = \frac{R(M-1)[M\alpha - M\alpha + \alpha]}{(M\alpha)^2} = \frac{R\alpha(M-1)}{M^2\alpha^2} = \frac{M-1}{\alpha M^2}R$$

que corresponde a la estrategia de equilibrio de Chiu et Koeppl [44].

Sección 2.3.3 – Demostración 2: Equivalencia entre la función de mejor respuesta del modelo estático (según la forma de Xiong et al. [43]) y la del modelo dinámico.

A partir de la estrategia óptima de un minero i al estado S en el modelo dinámico (10), y sin considerar el espacio estratégico, calculamos:

$$x_i^{(S)^*} = \max\left\{\psi^{(S)}\left(1 - \frac{\psi^{(S)}}{r\beta}c_i\right), 0\right\} = \psi^{(S)}\left(1 - \frac{\psi^{(S)}}{r\beta}c_i\right)$$

$$= \sum_{j\in S} x_j^{(S)} + l - \frac{\left(\sum_{j\in S} x_j^{(S)} + l\right)^2}{r\beta}c_i$$

$$= \sum_{j\in S} x_{i\neq j}^{(S)} + x_i^{(S)^*} + l - \frac{\left(\sum_{j\in S} x_{i\neq j}^{(S)} + x_i^{(S)^*} + l\right)^2}{r\beta}c_i$$

$$\left(\sum_{j\in S} x_{i\neq j}^{(S)} + x_i^{(S)^*} + l\right)^2 = \frac{r\beta\sum_{j\in S} x_{i\neq j}^{(S)} + l}{c_i}$$

$$x_i^{(S)^*} = \sqrt{\frac{r\beta \sum_{j\in S} x_{i\neq j}^{(S)} + l}{c_i}} - \left(\sum_{j\in S} x_{i\neq j}^{(S)} + l\right)$$

Si establecemos $l = 0$, que cambiamos la notación de la recompensa tal que $r\beta = (R + rt_i)$, que establecemos el costo del poder computacional como $c_i = p$, y que consideramos la probabilidad $e^{-\lambda z t_i}$ que un bloque minado quede huérfano, obtenemos:

$$x_i{}^* = \sqrt{\frac{(R + rt_i)e^{-\lambda z t_i} \sum_{j\in S} x_{i\neq j}^{(S)}}{p}} - \sum_{j\in S} x_{i\neq j}^{(S)}$$

que corresponde a la estrategia óptima de un minero i en el modelo estático según la forma definida por Xiong et al. [43].

Sección 2.3.4 – Demostración 3: Equivalencia entre la estrategia de equilibrio del modelo estático (según la forma de Dimitri [42]) y la del modelo dinámico.

A partir de la estrategia de equilibrio del modelo dinámico (10):

$$x_i^{(S)^*} = \max\left\{\psi^{(S)}\left(1 - \frac{\psi^{(S)}}{r\beta} c_i\right), 0\right\} \quad , \forall i$$

donde $\psi^{(S)} = r\beta \frac{|\hat{S}| - 1 + \sqrt{(|\hat{S}|-1)^2 + \frac{4l}{r\beta}\sum_{j\in\hat{S}} c_j}}{2\sum_{j\in\hat{S}} c_j}$

Si establecemos $l = 0$, que definimos la recompensa como $r\beta = R$, que cambiamos la notación del número de mineros que invierten un poder computacional positivo tal que $|\hat{S}| = n$, y que definimos $\sum_{j\in\hat{S}} c_j = c_{(n)}$, obtenemos:

$$\psi^{(S)} = r\beta \frac{\left|\hat{S}\right| - 1 + \sqrt{\left(\left|\hat{S}\right| - 1\right)^2 + \frac{4l}{r\beta}\sum_{j\in\hat{S}} c_j}}{2\sum_{j\in\hat{S}} c_j} = R\frac{N - 1 + \sqrt{(N-1)^2 + 0}}{2c_n} = \frac{R(N-1)}{c_n}$$

Reemplazando $\psi^{(S)}$ en la función de estrategia de equilibrio, obtenemos:

$$x_i^{(S)^*} = \max\left\{\psi^{(S)}\left(1 - \frac{\psi^{(S)}}{r\beta}c_i\right), 0\right\} = \max\left\{\frac{R(n-1)}{c_{(n)}} - \frac{\left[\frac{R(n-1)}{c_{(n)}}\right]^2}{R}c_i, 0\right\}$$

$$= \max\left\{\frac{R(n-1)}{c_{(n)}} - \frac{R(n-1)^2}{{c_{(n)}}^2}c_i, 0\right\} = \max\left\{\frac{R(n-1)\left[c_{(n)} - (n-1)c_i\right]}{{c_{(n)}}^2}, 0\right\}$$

Que corresponde a la estrategia de equilibrio del modelo estático de Dimitri [42] en el espacio estratégico $[0, \infty[$.

Sección 2.4.2 – Demostración 4: Estrategia de equilibrio del modelo propuesto.

Tal que mencionado en la sección 2.3.3, optimizamos $Z_i^{(S,x)}$ a partir de la primera derivada:

$$Z_i^{(S,x)} = \frac{\beta}{D^{(S,x)}}\frac{k_i x_i^{(S)}}{\sum_{j\in S} k_j x_j^{(S)} + k_l l}\tau(r + \theta t_i)e^{-\beta z_i t_i} - \frac{c_i {x_i}^{(S)}}{D^{(S,x)}}$$

$$\frac{\partial Z_i^{(S,x)}}{\partial {x_i}^{(S)}} = \frac{\beta}{D^{(S,x)}}\tau(r + \theta t_i)e^{-\beta z_i t_i}\frac{\partial \alpha_i}{\partial {x_i}^{(S)}} - \frac{c_i}{D^{(S,x)}}$$

$$\frac{\partial \alpha_i}{\partial {x_i}^{(S)}} = \frac{\partial}{\partial {x_i}^{(S)}}\left(\frac{k_i x_i^{(S)}}{\sum_{j\in S} k_j x_j^{(S)} + k_l l}\right) = \frac{k_i}{\sum_{j\in S} k_j x_j^{(S)} + k_l l} - \frac{{k_i}^2 {x_i}^{(S)}}{\left(\sum_{j\in S} k_j x_j^{(S)} + k_l l\right)^2}$$

$$\frac{\partial Z_i^{(S,x)}}{\partial {x_i}^{(S)}} = \frac{\beta}{D^{(S,x)}}\tau(r + \theta t_i)e^{-\beta z_i t_i}\left(\frac{k_i}{\sum_{j\in S} k_j x_j^{(S)} + k_l l} - \frac{{k_i}^2 {x_i}^{(S)}}{\left(\sum_{j\in S} k_j x_j^{(S)} + k_l l\right)^2}\right) - \frac{c_i}{D^{(S,x)}} = 0$$

$$x_i{}^{(S)} = \frac{\left(\sum_{j\in S} k_j x_j^{(S)} + k_l l\right)^2}{k_i{}^2}\left(\frac{k_i}{\sum_{j\in S} k_j x_j^{(S)} + k_l l} - \frac{c_i}{\beta\tau(r+\theta t_i)e^{-\beta z_i t_i}}\right)$$

$$= \frac{\left(\sum_{j\in S} k_j x_j^{(S)} + k_l l\right)}{k_i} - \frac{c_i\left(\sum_{j\in S} k_j x_j^{(S)} + k_l l\right)^2}{k_i{}^2\beta\tau(r+\theta t_i)e^{-\beta z_i t_i}}$$

$$= \left(\sum_{j\in S} k_j x_j^{(S)} + k_l l\right)\left(\frac{1}{k_i} - \frac{c_i\left(\sum_{j\in S} k_j x_j^{(S)} + k_l l\right)}{k_i{}^2\beta\tau(r+\theta t_i)e^{-\beta z_i t_i}}\right)$$

Tenemos la siguiente función de mejor respuesta para un jugador:

$$x_i{}^{(S)^*} = \psi^{(S)}\left(\frac{1}{k_i} - \frac{\psi^{(S)}}{k_i{}^2\beta\tau(r+\theta t_i)e^{-\beta z_i t_i}}c_i\right)$$

donde $\psi^{(S)} = \sum_{j\in S} k_j x_j^{(S)} + k_l l$

Trayendo k_i a la izquierda de la igualdad, sumando para todos los jugadores y agregando $k_l l$, obtenemos:

$$\sum_{j\in S} k_j x_j + k_l l = \psi^{(S)}\left(|\hat{S}| - \frac{\psi^{(S)}}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j\left(r+\theta t_j\right)e^{-\beta z_j t_j}}\right) + k_l l$$

Reemplazando $\sum_{j\in S} k_i x_j + k_l l$ por $\psi^{(S)}$, obtenemos:

$$\psi^{(S)} = \psi^{(S)}\left(|\hat{S}| - \frac{\psi^{(S)}}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j\left(r+\theta t_j\right)e^{-\beta z_j t_j}}\right) + k_l l$$

$$\frac{1}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j\left(r+\theta t_j\right)e^{-\beta z_j t_j}}\left(\psi^{(S)}\right)^2 - \left(|\hat{S}| - 1\right)\psi^{(S)} - k_l l = 0$$

Al resolver la ecuación para los valores positivos de $\psi^{(S)}$, obtenemos:

$$\psi^{(S)} = \frac{|\hat{S}| - 1 + \sqrt{\left(|\hat{S}| - 1\right)^2 + \frac{4k_l l}{\beta\tau}\sum_{j\in\hat{S}} \frac{c_j}{k_j\left(r + \theta t_j\right)e^{-\beta z_j t_j}}}}{\frac{2}{\beta\tau}\sum_{j\in\hat{S}} \frac{c_j}{k_j\left(r + \theta t_j\right)e^{-\beta z_j t_j}}}$$

Obtenemos la siguiente estrategia de equilibrio:

$$x_i^{(S)^*} = \max\left\{ \psi^{(S)}\left(\frac{1}{k_i} - \frac{\psi^{(S)}}{{k_i}^2 \beta\tau(r + \theta t_i)e^{-\beta z_i t_i}} c_i\right), 0\right\} \quad , \forall i$$

donde $\psi^{(S)} = \frac{|\hat{S}|-1+\sqrt{(|\hat{S}|-1)^2+\frac{4k_l l}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j\left(r+\theta t_j\right)e^{-\beta z_j t_j}}}}{\frac{2}{\beta\tau}\sum_{j\in\hat{S}}\frac{c_j}{k_j\left(r+\theta t_j\right)e^{-\beta z_j t_j}}}$

Sección 2.6 – Valores de los parámetros

General

β : El nivel de dificultad de la PoW está configurado para generar un nuevo bloque en promedio cada diez minutos. Por lo tanto, la tasa constante de resolución de la PoW es $\beta = 0{,}1$ bloque por minuto.

Subjuego de los Pools

r : La recompensa por minar un bloque que se agrega a la cadena de Bitcoin es actualmente 6,25 bitcoins.

τ : El valor de un bitcoin se estima en alrededor de 10 000$ según el historial de Bitcoin.com [68].

c_i, c_j : El costo marginal de la electricidad se redondea a $c_i = c_j = 0{,}0007$$ kWh/min tomando como base el costo marginal promedio de la electricidad estimado a 0,04$ kWh en un análisis reciente de CoinShares Research [62].

t_i, t_j : El número promedio de transacciones en un bloque $t_i = t_j = 2100$ se estima a partir del historial de Bitcoin.com, y la cantidad de transacciones generalmente es entre 1500 y 2500 transacciones por bloque. [69]

θ : Los cargos promedios de transacción $\theta = 0{,}000\ 12$ $ por transacción se obtienen convirtiendo en bitcoins (1 bitcoin = 100M satoshis) el producto del tamaño promedio de transacción (600B) y de la tasa de cargos promedios por byte (20 satoshis / B). Asimismo, se establece que los cargos por transacción son generalmente entre $\theta = 0{,}000\ 04$ y $\theta = 0{,}0012$, valores estimados a partir de un tamaño mínimo de transacción de 400B y máximo de 1200B, y de una tasa de cargos mínima de 10 satoshis/B y máxima de 100 satoshis/B. Todos los valores se estiman a partir del historial de Bitcoin.com. [70], [71]

z : El valor del factor de propagación de un bloque en la red se obtiene del análisis de Xiong et al. [43] y se establece a $z = 0{,}005/60$ sobre la base de un tiempo en minutos. Esto corresponde a un tiempo de propagación de 10,5 segundos para un bloque de 2100 transacciones, durante el cual este se propaga y que existe el riesgo de una bifurcación en la cadena. Este resultado es consistente con el de [72] que estima este tiempo a 11,37 segundos.

$S, \hat{S}, U$: El número de pools grandes que tienen los recursos para jugar la estrategia de equilibrio se estima en 10 a partir de los datos de Blockchain.com sobre la distribución del poder computacional de la red Bitcoin. [73]

l : El valor se establece arbitrariamente para corresponder a la proporción del poder computacional de la red que no proviene de los pools grandes, o sea aproximadamente 1/11 de la potencia total, según los datos de Blockchain.com y Bitcoin.com. [73], [74]

Dilema de los Mineros

λ_i, μ_i : Según los datos recogidos de Bitnodes [59] para principios de julio de 2020, el número de nodos presentes en el sistema durante un período de 24 horas varía

aproximadamente entre 10 300 y 10 600 con un promedio de alrededor de 10 450 nodos conectados. Para reproducir dicha distribución a los mineros conectados en un pool, asumimos que hay 1100 nodos registrados en él, que 500 de ellos no son estratégicos y entonces que se consideran una constante invariable, y aplicamos a los 600 mineros estratégicos una tasa de llegada (es decir de conexión) en el pool de $\lambda_i = 1$ y una tasa de salida (es decir de desconexión) de $\mu_i = 0{,}1$. El siguiente gráfico presenta la distribución de densidad de probabilidades obtenida del tiempo pasado en los distintos estados para un minero que ingresa al sistema en el estado $S = 550$, y muestra que casi todo el tiempo (99,96978%) se gasta en los estados $S = 520$ a $S = 570$, lo que es consistente con los datos de Bitnodes [59]:

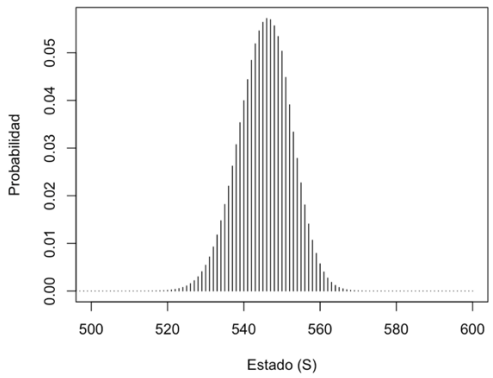


Figura 7: Apéndice: Distribución del tiempo pasado en los distintos estados con $\lambda_i = 1$ y $\mu_i = 0{,}1$ en el dilema de los mineros.

Sección 2.6.2 – Cálculo de la utilidad esperada y del ROI de los mineros no estratégicos en el juego de protocolo.

$$R_i^{(x_i^{max})} = \frac{k_i x_i^{max}}{\sum_{j \in \hat{S}} k_j E\left[x_j^*\right] + k_l l} E[r]_p^{(S, x_p{}^*)} - \frac{x_i^{max} c_i}{\beta}$$

$$= \frac{1 \cdot 10\,000/500}{550 \cdot 1 \cdot 1498{,}263 + 1 \cdot 10\,000} \cdot 5867{,}20 - \frac{10\,000/500 \cdot 0{,}000\,69}{0{,}1}$$

$$= 0{,}002\,69\$$$

$$ROI = \frac{R_i^{(x_i^{max})}}{\frac{x_i^{max} c_i}{\beta}} = \frac{0{,}002\,69}{0{,}138} = 1{,}95\%$$

Referencias

[1] J. von Neumann y O. Morgenstern, Theory of Games and Economic Behavior, Princeton: Princeton University Press, 1944.

[2] D. Ross, «Stanford Encyclopedia of Philosophy - Game Theory,» [En línea]. Available: https://plato.stanford.edu/entries/game-theory/. [Último acceso: 10 Abril 2020].

[3] «Wikipedia - Game Theory,» [En línea]. Available: https://en.wikipedia.org/wiki/Game_theory. [Último acceso: 10 Abril 2020].

[4] «Wikipedia - Distributed Ledger,» [En línea]. Available: https://en.wikipedia.org/wiki/Distributed_ledger. [Último acceso: 13 Abril 2020].

[5] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» [En línea]. Available: https://bitcoin.org/bitcoin.pdf. [Último acceso: 13 Abril 2020].

[6] «Wikipedia - Solution Concept,» [En ligne]. Available: https://en.wikipedia.org/wiki/Solution_concept. [Accès le 16 Abril 2020].

[7] A. Hayes, «Investopedia - Game Theory,» 25 Junio 2019. [En línea]. Available: https://www.investopedia.com/terms/g/gametheory.asp. [Último acceso: 20 Abril 2020].

[8] «Wikipedia - Strategy (Game Theory),» [En línea]. Available: https://en.wikipedia.org/wiki/Strategy_(game_theory). [Último acceso: 20 Abril 2020].

[9] «Wikipedia - Outcome (Game Theory),» [En línea]. Available: https://en.wikipedia.org/wiki/Outcome_(game_theory). [Último acceso: 20 Abril 2020].

[10] K. Leyton-Brown y Y. Shoham, Essentials of Game Theory, Oregon State: Morgan & Claypool, 2008.

[11] «Wikipedia - Complete Information,» [En línea]. Available: https://en.wikipedia.org/wiki/Complete_information. [Último acceso: 28 Abril 2020].

[12] L. Kockesen y E. A. Ok, «An Introduction to Game Theory,» 2007. [En línea]. Available: http://home.ku.edu.tr/~lkockesen/teaching/econ333/lectnotes/uggame.pdf. [Último acceso: 16 Abril 2020].

[13] M. J. Osborne y A. Rubinstein, A Course in Game Theory, London, England: The MIT Press, 1994.

[14] «Wikipedia - Normal-form game,» [En línea]. Available: https://en.wikipedia.org/wiki/Normal-form_game. [Último acceso: 21 Abril 2020].

[15] «Wikipedia - Extensive-form game,» [En línea]. Available: https://en.wikipedia.org/wiki/Extensive-form_game. [Último acceso: 21 Abril 2020].

[16] «Wikipedia - Simultaneous Game,» [En línea]. Available: https://en.wikipedia.org/wiki/Simultaneous_game. [Último acceso: 23 Abril 2020].

[17] M. Paul, D. Lepelley y H. Smaoui, «Introduction à la Théorie des Jeux : les jeux non coopératifs,» [En línea]. Available: https://cemoi.univ-reunion.fr/fileadmin/Fichiers/CEMOI/Publications/Documents_de_travail/2013/2013-08_-_TDJ_1_version_longue.pdf. [Último acceso: 5 Mayo 2020].

[18] L. Ziyao, C. L. Nguyen, W. Wenbo, N. Dusti, W. Ping, L. Ying-Chang y K. Dong In, «A Survey on Applications of Game Theory in Blockchain,» 2019. [En línea]. Available: https://arxiv.org/pdf/1902.10865.pdf. [Último acceso: 5 Mayo 2020].

[19] «Wikipedia - Stackelberg Competition,» [En línea]. Available: https://en.wikipedia.org/wiki/Stackelberg_competition. [Último acceso: 6 Mayo 2020].

[20] T. Pénard, «La Théorie des Jeux Répétés: Application à la Concurrence Oligopilistique (Partie1),» [En línea]. Available: https://perso.univ-rennes1.fr/thierry.penard/biblio/aix.pdf. [Último acceso: 5 Mayo 2020].

[21] L. C. Thomas, Games, Theory and Applications, Mineola, New York: Dover Publications Inc., 1984.

[22] «Game theory III: Repeated games,» [En línea]. Available: https://policonomics.com/lp-game-theory3-repeated-game/. [Último acceso: 5 Mayo 2020].

[23] «Wikipedia - Repeated Game,» [En ligne]. Available: https://en.wikipedia.org/wiki/Repeated_game. [Accès le 4 Mayo 2020].

[24] G. Riley, «Game Theory - Different Types of Games,» [En línea]. Available: https://www.tutor2u.net/economics/reference/game-theory-different-types-of-games. [Último acceso: 4 Mayo 2020].

[25] «Wikipedia - Markov Decision Process,» [En línea]. Available: https://en.wikipedia.org/wiki/Markov_decision_process. [Último acceso: 31 Mayo 2020].

[26] «Wikipedia - Théorie des Jeux,» [En línea]. Available: https://fr.wikipedia.org/wiki/Th%C3%A9orie_des_jeux. [Último acceso: 18 Abril 2020].

[27] «Wikipedia - Jeu Coopératif,» [En línea]. Available: https://fr.wikipedia.org/wiki/Jeu_coop%C3%A9ratif_(th%C3%A9orie). [Último acceso: 20 Abril 2020].

[28] «Wikipedia - Aggregatice Game,» [En línea]. Available: https://en.wikipedia.org/wiki/Aggregative_game. [Último acceso: 28 Junio 2020].

[29] Z. Cao y X. Yang, «Symmetric Games and Symmetry Group,» 2015. [En línea]. Available: https://www.researchgate.net/publication/280600867_Symmetric_Games_and_Symmetry_Groups. [Último acceso: 29 Julio 2020].

[30] «Wikipedia - Perfect Information,» [En línea]. Available: https://en.wikipedia.org/wiki/Perfect_information. [Último acceso: 28 Abril 2020].

[31] «Wikipedia - Jeu bayésien,» [En línea]. Available: https://fr.wikipedia.org/wiki/Jeu_bay%C3%A9sien. [Último acceso: 28 Abril 2020].

[32] A. M. Coleman, «Reasoning About Strategic Interaction - Solution Concepts in Game Theory,» [En línea]. Available: https://www2.le.ac.uk/departments/npb/people/amc/articles-pdfs/reasabou.pdf. [Último acceso: 7 Mayo 2020].

[33] L. Akos, «Scholar Havard - Section 11 - Nash Equilibrium,» [En línea]. Available: https://scholar.harvard.edu/files/alada/files/section11_1.pdf. [Último acceso: 7 Mayo 2020].

[34] «Nash Equilibrium-Proof of Existence,» [En línea]. Available: https://en.wikipedia.org/wiki/Nash_equilibrium#Proof_of_existence. [Último acceso: 29 Julio 2020].

[35] G. Bonanno, Game Theory, California: Giacomo Bonanno, 2018.

[36] «Wikipedia - Nash Equilibrium,» [En línea]. Available: https://en.wikipedia.org/wiki/Nash_equilibrium. [Último acceso: 10 Mayo 2020].

[37] «Wikipedia - Bellman Equation,» [En línea]. Available: https://en.wikipedia.org/wiki/Bellman_equation#cite_note-BellmanDP-6. [Último acceso: 1 Junio 2020].

[38] S. Dhamal, W. Ben-Ameur, T. Chahed, A. Eitan, A. Sunny y S. Poojary, «A Stochastic Game Framework for Analyzing Computational Investment Strategies in Distributed Computing,» 16 Noviembre 2019. [En línea]. Available: https://arxiv.org/pdf/1809.03143.pdf. [Último acceso: 28 Mayo 2020].

[39] A. M. Antonopoulos, Mastering Bitcoin, Sebastopol: O'Reilly Media, 2015.

[40] J. Gogo, «Bitcoin.com,» 7 Mayo 2020. [En línea]. Available: https://news.bitcoin.com/65-of-global-bitcoin-hashrate-concentrated-in-china/. [Último acceso: 4 Junio 2020].

[41] J. Frankenfield, «Investopedia-51% Attack,» 2019. [En línea]. Available: https://www.investopedia.com/terms/1/51-attack.asp. [Último acceso: 27 Julio 2020].

[42] N. Dimitri, «Bitcoin Mining as a Contest,» *Ledger,* vol. 2, pp. 31-37, 2017.

[43] Z. Xiong, S. Feng, D. Niyato, P. Wang y Z. Han, «Optimal Pricing-Based Edge Computing Resource Management in Mobile Blockchain,» 2017. [En línea]. Available: https://arxiv.org/pdf/1711.01049.pdf. [Último acceso: 18 Mayo 2020].

[44] J. Chiu y T. V. Koeppl, «Incentive Compatibility on the Blockchain,» 2018. [En línea]. Available: https://www.bankofcanada.ca/wp-content/uploads/2018/07/swp2018-34.pdf. [Último acceso: 25 Mayo 2020].

[45] P. J. Reny, «Non-Cooperative Games: Equilibrium Existence,» The New Palgrave Dictionary of Economics, Second Edition, 2005.

[46] M. Hall, «Investopedia,» 22 Mayo 2020. [En línea]. Available: https://www.investopedia.com/ask/answers/041315/how-marginal-revenue-related-marginal-cost-production.asp. [Último acceso: 26 Mayo 2020].

[47] R. D. Yates, «A Framework for Uplink Power Control in Cellular Radio Systems,» 13 Mayo 1996. [En ligne]. Available: https://www.researchgate.net/publication/3233585_A_Framework_for_Uplink_Power_Control_in_Cellular_Radio_Systems?enrichId=rgreq-bd0552ffbcec9d1e80cb149698798855-XXX&enrichSource=Y292ZXJQYWdlOzMyMzM1ODU7QVM6MTk1NDI5NTQ4NDY2MTgwQDE0MjM2MDU0NDM5MTU=&el=1_x_2&. [Accès le 24 Mayo 2020].

[48] N. V. Long y A. Soubeyran, «Existence and uniqueness of Cournot equilibrium: A contraction mapping approach,» 6 Enero 2000. [En línea]. Available: http://pareto.uab.cat/xmg/Docencia/IO-en/IOReadings/CournotEq/VLongSoub.pdf. [Último acceso: 25 Mayo 2020].

[49] A. Barone, «How to Choose a Cryptocurrency Mining Pool,» 2020. [En línea]. Available: https://www.investopedia.com/tech/how-choose-cryptocurrency-mining-pool/. [Último acceso: 20 Julio 2020].

[50] «Imputation,» [En línea]. Available: https://en.wikipedia.org/wiki/Imputation_(game_theory). [Último acceso: 23 Julio 2020].

[51] C. Hilbe, B. Wu, A. Traulsen y M. A. Nowak, «Cooperation and control in multiplayer social dilemmas,» 2014. [En línea]. Available: https://www.pnas.org/content/111/46/16425. [Último acceso: 23 Julio 2020].

[52] S. Kuhn, «Prisoner's Dilemma,» 2019. [En línea]. Available: https://plato.stanford.edu/entries/prisoner-dilemma/#SingPersInte. [Último acceso: 23 Julio 2020].

[53] L. Pan, D. Hao y Z. Z. T. Rong, «Zero-Determinant Strategies in Iterated Public Goods Game,» 2015. [En línea]. Available: https://www.nature.com/articles/srep13096. [Último acceso: 23 Julio 2020].

[54] M. W. Macy y A. Flache, «Learning dynamics in social dilemmas,» 2002. [En línea]. Available: https://www.pnas.org/content/99/suppl_3/7229. [Último acceso: 23 Julio 2020].

[55] L. Wardil, I. R. Silva y J. K. L. da Silva, «Positive interactions may decrease cooperation in social dilemma experiments,» 2019. [En línea]. Available: https://www.nature.com/articles/s41598-018-37674-5. [Último acceso: 23 Julio 2020].

[56] E. Akin, «The Iterated Prisoner's Dilemma:Good Strategies and Their Dynamics,» 2013. [En línea]. Available: https://arxiv.org/pdf/1211.0969v3.pdf. [Último acceso: 25 Julio 2020].

[57] C. Hilbe, B. Wu, A. Traulsen y M. A. Nowak, «Cooperation and Control in Multisocial Dilemas - SI Text,» 2014. [En línea]. Available: https://www.pnas.org/content/pnas/suppl/2014/10/23/1407887111.DCSupplemental/pnas.201407887SI.pdf?targetid=nameddest%3DSTXT. [Último acceso: 12 Septiembre 2020].

[58] «Win-Stay, Lose-Shift,» [En línea]. Available: https://en.wikipedia.org/wiki/Win%E2%80%93stay,_lose%E2%80%93switch. [Último acceso: 24 Julio 2020].

[59] «Bitnodes,» [En línea]. Available: https://bitnodes.io/dashboard/. [Último acceso: 8 Julio 2020].

[60] S. Haig, «Bitcoin.com,» 2018. [En línea]. Available: https://news.bitcoin.com/mining-consumes-half-as-much-power-as-beci-estimates-coinshares/. [Último acceso: 27 Julio 2020].

[61] «Digiconomist-Bitcoin Energy Consumption,» 2020. [En línea]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Último acceso: 27 Julio 2020].

[62] C. Bendiksen y S. Gibbons, «CoinShares Research-Network, The Bitcoin Mining,» 2019. [En línea]. Available: https://coinshares.com/assets/resources/Research/bitcoin-mining-network-december-2019.pdf. [Último acceso: 7 Julio 2020].

[63] L. Conway, «Bitcoin Halving,» [En línea]. Available: https://www.investopedia.com/bitcoin-halving-4843769. [Último acceso: 2 Agosto 2020].

[64] D. Taralla, «Les formes de concurrence/ de marché,» 2009-2010. [En línea]. Available: https://people.montefiore.uliege.be/dtaralla/files/marches.pdf. [Último acceso: 15 Septiembre 2020].

[65] A. Sapirshtein, Y. Sompolinsky y A. Zohar, «Optimal Selfish Mining Strategies in Bitcoin,» 2015. [En línea]. Available: https://arxiv.org/pdf/1507.06183.pdf. [Último acceso: 5 Junio 2020].

[66] I. Eyal y E. G. Sirer, «Majority is not Enough: Bitcoin Mining is Vulnerable,» 2014. [En línea]. Available: https://arxiv.org/pdf/1311.0243.pdf. [Último acceso: 5 Junio 2020].

[67] Eyal y Ittay, «The Miner's Dilemma,» 2014. [En línea]. Available: https://arxiv.org/pdf/1411.7099.pdf. [Último acceso: 5 Junio 2020].

[68] «Bitcoin.com - Bitcoin Core Price,» [En línea]. Available: https://charts.bitcoin.com/btc/chart/price#5moc. [Último acceso: 7 Julio 2020].

[69] «Bitcoin.com - Transactions per block,» [En línea]. Available: https://charts.bitcoin.com/btc/chart/transactions-per-block#5moc. [Último acceso: 7 Julio 2020].

[70] «Bitcoin.com - Transaction size,» [En línea]. Available: https://charts.bitcoin.com/btc/chart/transaction-size#5moc . [Último acceso: 7 Julio 2020].

[71] «Bitcoin.com - Fee rate,» [En línea]. Available: https://charts.bitcoin.com/btc/chart/fee-rate#5moc. [Último acceso: 7 Julio 2020].

[72] C. Decker y R. Wattenhofer, «Information Propagation in the Bitcoin Network,» 2013. [En línea]. Available: https://www.gsd.inesc-id.pt/~ler/docencia/rcs1314/papers/P2P2013_041.pdf. [Último acceso: 18 Julio 2020].

[73] «Blockchain.com - Distribución de tasas de hash,» [En línea]. Available: https://www.blockchain.com/pools. [Último acceso: 7 Julio 2020].

[74] «Bitcoin.com - Hash rate,» [En línea]. Available: https://charts.bitcoin.com/btc/chart/hash-rate#5moc. [Último acceso: 7 Julio 2020].

[75] J. Chappelow, «Investopedia - Utility,» 30 Enero 2020. [En línea]. Available: https://www.investopedia.com/terms/u/utility.asp. [Último acceso: 20 Abril 2020].

[76] «Wikipedia - Prisoner's Dilemma,» [En línea]. Available: https://en.wikipedia.org/wiki/Prisoner%27s_dilemma. [Último acceso: 21 Abril 2020].

[77] M. Plantevit, «Théorie des Jeux - Jeux Répétés,» [En línea]. Available: https://perso.liris.cnrs.fr/marc.plantevit/ENS/GameTheory/CM/5_jeux_repetes_Full.pdf. [Último acceso: 4 Mayo 2020].

[78] «Des Jeux Répétés et Dynamiques,» [En línea]. Available: https://www.lri.fr/~jcohen/documents/enseignement/chap6.pdf. [Último acceso: 4 Mayo 2020].

[79] «Définitions et Typologie des Jeux,» [En línea]. Available: https://theses.univ-lyon2.fr/documents/getpart.php?id=lyon2.2000.dieng_sa&part=20642. [Último acceso: 4 Mayo 2020].

[80] «Wikipedia - Grim Trigger,» [En línea]. Available: https://en.wikipedia.org/wiki/Grim_trigger. [Último acceso: 4 Mayo 2020].

[81] J. Rosenmuller, Game Theory: Stochastics, Information, Strategies and Cooperation, Boston: Kluwer Academic Publishers, 2000.

[82] «Wikipedia - Stratégie (théorie des jeux),» [En línea]. Available: https://fr.wikipedia.org/wiki/Strat%C3%A9gie_(th%C3%A9orie_des_jeux). [Último acceso: 7 Mayo 2020].

[83] «Mixed Strategies,» [En línea]. Available: https://saylordotorg.github.io/text_introduction-to-economic-analysis/s17-03-mixed-strategies.html. [Último acceso: 7 Mayo 2020].

[84] «Nash Equilibrium,» [En línea]. Available: https://fr.qwe.wiki/wiki/Nash_equilibrium. [Último acceso: 11 Mayo 2020].

[85] «Non-Zero-Sum Games,» [En línea]. Available: https://cs.stanford.edu/people/eroberts/courses/soco/projects/1998-99/game-theory/nonzero.html. [Último acceso: 17 Mayo 2020].

[86] J. A. Kroll, I. C. Davy et E. W. Felton, «The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries,» 2013. [En ligne]. Available: https://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf. [Accès le 18 Mayo 2020].

[87] Amin, «Stack Exchange,» 1 Noviembre 2017. [En línea]. Available: https://math.stackexchange.com/questions/2500035/whats-the-difference-between-quasi-concavity-and-concavity. [Último acceso: 21 Mayo 2020].

[88] R. Y. Maragheh, «Research Gate,» 16 Julio 2014. [En línea]. Available: https://www.researchgate.net/post/Application_of_Infinite_dimensional_strategy_space_for_game_theory. [Último acceso: 24 Mayo 2020].

[89] «Wikipedia,» [En línea]. Available: https://en.wikipedia.org/wiki/Kakutani_fixed-point_theorem. [Último acceso: 24 Mayo 2020].

[90] «Wikipedia - Kakutani Fixed-Point Theorem,» [En línea]. Available: https://en.wikipedia.org/wiki/Kakutani_fixed-point_theorem. [Último acceso: 24 Mayto 2020].

[91] I. Bashir, Mastering Blockchain, Birmingham: Packt Publishing Ltd, 2017.

[92] Z. Xiong, S. Feng, D. Niyato, P. Wang y Z. Han, «Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks,» 19 Mayo 2018. [En línea]. Available: https://arxiv.org/pdf/1710.01567.pdf. [Último acceso: 26 Mayo 2020].

[93] «Wikipedia - Memorylessness,» [En línea]. Available: https://en.wikipedia.org/wiki/Memorylessness. [Último acceso: 29 Mayo 2020].

[94] R. Bellman, Dynamic Programming, New York: Dover Publications Inc., 1957.

[95] «Wikipedia - Absorbing Markov Chain,» [En línea]. Available: https://en.wikipedia.org/wiki/Absorbing_Markov_chain. [Último acceso: 1 Junio 2020].

[96] A. Gervais, H. Ritzdorf, G. O. Karame y S. Capkun, «Tampering with the Delivery of Blocks and Transactions in Bitcoin,» 2015. [En línea]. Available: https://eprint.iacr.org/2015/578.pdf. [Último acceso: 5 Junio 2020].

[97] «Wikipedia - Identity Matrix,» [En línea]. Available: https://en.wikipedia.org/wiki/Identity_matrix. [Último acceso: 6 Junio 2020].

[98] «bitcoin.it - Block hashing algorithm,» [En línea]. Available: https://en.bitcoin.it/wiki/Block_hashing_algorithm. [Último acceso: 7 Junio 2020].

[99] «Bitmain - Antminer S17+,» [En línea]. Available: https://shop.bitmain.com/product/detail?pid=00020200428172147790jIY8bLfh06B8. [Último acceso: 13 Julio 2020].

[100] «Mining Pool,» [En línea]. Available: https://en.wikipedia.org/wiki/Mining_pool. [Último acceso: 20 Julio 2020].

[101] «The Prisoner's Dilemma,» 2019. [En línea]. Available: https://blog.methodsconsultants.com/posts/the-prisoners-dilemma/. [Último acceso: 23 Julio 2020].

[102] «Evolutionary Game Theory,» [En línea]. Available: https://en.wikipedia.org/wiki/Evolutionary_game_theory. [Último acceso: 23 Julio 2020].

[103] «Zero-Determinant Strategies,» [En línea]. Available: https://en.wikipedia.org/wiki/Prisoner%27s_dilemma#Zero-determinant_strategies. [Último acceso: 23 Julio 2020].

[104] W. H. Press y F. J. Dyson, «Iterated Prisoner's Dilemma contains strategies that dominate any evolutionary opponent,» 2012. [En línea]. Available: https://www.pnas.org/content/109/26/10409. [Último acceso: 24 Julio 2020].

[105] J. Frankenfield, «Tit for Tat,» 2019. [En línea]. Available: https://www.investopedia.com/terms/t/tit-for-tat.asp. [Último acceso: 24 Julio 2020].

[106] «ROI Formula (Return on Investment),» 2017. [En línea]. Available: https://corporatefinanceinstitute.com/resources/knowledge/finance/return-on-investment-roi-formula/. [Último acceso: 26 Julio 2020].

[107] W. Spaniel, «Symmetric , Zero-Sum Games,» [En línea]. Available: http://gametheory101.com/courses/game-theory-101/symmetric-zero-sum-games/. [Último acceso: 29 Julio 2020].

[108] «Compact Space,» [En línea]. Available: https://en.wikipedia.org/wiki/Compact_space. [Último acceso: 29 Julio 2020].

[109] R. Theorem. [En línea]. Available: https://en.wikipedia.org/wiki/Church%E2%80%93Rosser_theorem. [Último acceso: 29 Julio 2020].

[110] «Bayes' Theorem,» [En línea]. Available: https://en.wikipedia.org/wiki/Bayes%27_theorem. [Último acceso: 29 Julio 2020].

[111] «Volunteer Computing,» [En línea]. Available: https://en.wikipedia.org/wiki/Volunteer_computing. [Último acceso: 29 Julio 2020].

[112] M. Hearn, «The Resolution of the Bitcoin Experiment,» 2016. [En línea]. Available: https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7?gi=ea79cd719490. [Último acceso: 3 Agosto 2020].